THE UNIVERSITY of EDINBURGH

Edinburgh Research Explorer

Advances in Quantum Cryptography

Citation for published version:
Pirandola, S, Andersen, UL, Banchi, L, Berta, M, Bunandar, D, Colbeck, R, Englund, D, Gehring, T, Lupo, C, Ottaviani, C, Pereira, J, Razavi, M, Shaari, JS, Tomamiche, M, Usenko, VC, Vallone, G, Villoresi, P & Wallden, P 2020, 'Advances in Quantum Cryptography', *Advances in Optics and Photonics*, vol. 12, no. 4, pp. 1012-1236. https://doi.org/10.1364/AOP.361502

Digital Object Identifier (DOI):
https://doi.org/10.1364/AOP.361502

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Peer reviewed version

Published In:
Advances in Optics and Photonics

Publisher Rights Statement:
© 2020 Optical Society of America. One print or electronic copy may be made for personal use only. Systematic reproduction and distribution, duplication of any material in this paper for a fee or for commercial purposes, or modifications of the content of this paper are prohibited.

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

OPEN ACCESS

Download date: 27. Jul. 2024

Advances in Quantum Cryptography

S. Pirandola[1,2], U. L. Andersen[3], L. Banchi[4], M. Berta[5], D. Bunandar[2], R. Colbeck[6], D. Englund[2], T. Gehring[3], C. Lupo[7], C. Ottaviani[1], J. L. Pereira[1], M. Razavi[8], J. S. Shaari[9,10], M. Tomamichel[11,12], V. C. Usenko[13], G. Vallone[14], P. Villoresi[14], P. Wallden[15]

[1] *Department of Computer Science and York Centre for Quantum Technologies, University of York, York YO10 5GH, UK*
[2] *Research Laboratory of Electronics, Massachusetts Institute of Technology (MIT), Cambridge, Massachusetts 02139, USA*
[3] *Center for Macroscopic Quantum States (bigQ), Department of Physics, Technical University of Denmark, Fysikvej, 2800 Kgs. Lyngby, Denmark*
[4] *Department of Physics and Astronomy, University of Florence, via G. Sansone 1, I-50019 Sesto Fiorentino (FI), Italy*
[5] *Department of Computing, Imperial College, Kensington, London SW7 2AZ, UK*
[6] *Department of Mathematics, University of York, York YO10 5DD, UK*
[7] *Department of Physics and Astronomy, University of Sheffield, Sheffield S3 7RH, UK*
[8] *School of Electronic and Electrical Engineering, University of Leeds, Leeds, LS2 9JT, UK*
[9] *Faculty of Science, International Islamic University Malaysia (IIUM), Jalan Sultan Ahmad Shah, 25200 Kuantan, Pahang, Malaysia*
[10] *Institute of Mathematical Research (INSPEM), University Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia*
[11] *Centre for Quantum Software and Information, School of Software, University of Technology Sydney, Sydney NSW 2007, Australia*
[12] *Department of Electrical and Computer Engineering and Centre for Quantum Technologies, National University of Singapore, Singapore*
[13] *Department of Optics, Palacky University, 17. listopadu 50, 772 07 Olomouc, Czech Republic*
[14] *Dipartimento di Ingegneria dell'Informazione, Universitá degli Studi di Padova, via Gradenigo 6B, 35131 Padova, Italy and*
[15] *School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, UK*

Quantum cryptography is arguably the fastest growing area in quantum information science. Novel theoretical protocols are designed on a regular basis, security proofs are constantly improving, and experiments are gradually moving from proof-of-principle lab demonstrations to in-field implementations and technological prototypes. In this review, we provide both a general introduction and a state of the art description of the recent advances in the field, both theoretically and experimentally. We start by reviewing protocols of quantum key distribution based on discrete variable systems. Next we consider aspects of device independence, satellite challenges, and protocols based on continuous variable systems. We will then discuss the ultimate limits of point-to-point private communications and how quantum repeaters and networks may overcome these restrictions. Finally, we will discuss some aspects of quantum cryptography beyond standard quantum key distribution, including quantum random number generators and quantum digital signatures.

CONTENTS

I. Introduction 6

II. Basic notions in quantum key distribution 7
- A. Generic aspects of a QKD protocol 7
- B. Asymptotic security and eavesdropping strategies 8
- C. Finite-size effects 8
- D. Composable security of QKD 8

III. Overview of DV-QKD 10
- A. Preliminary notions 10
- B. Prepare and measure protocols 11
  - 1. BB84 protocol 11
  - 2. Intercept-resend against the BB84 protocol 12
  - 3. Intercept-resend with an intermediate basis 13
  - 4. Optimal eavesdropping strategy of the BB84 protocol 13
  - 5. Unconditional security of the BB84 protocol 15
  - 6. Six-state protocol 15
  - 7. B92 protocol 16
- C. Practical imperfections and countermeasures 17
  - 1. Realistic devices and photon number splitting attacks 17
  - 2. From GLLP to decoy states 17
  - 3. SARG04 protocol 19
- D. Entanglement-based QKD 19
  - 1. E91 protocol 19
  - 2. BBM92 protocol 20
- E. Two-way quantum communication 20
  - 1. Ping pong protocol 20
  - 2. Two-way QKD protocols 21
  - 3. Intercept-resend strategy 21
  - 4. Non-orthogonal attack strategies 22
  - 5. Further considerations 22

IV. Device-independent QKD 22
- A. Introduction 22
- B. The link between Bell violation and unpredictability 23
- C. Quantitative bounds 24
- D. Protocols for DI-QKD 25
  - 1. The setup for DI-QKD 25
  - 2. The spot-checking CHSH QKD protocol 25
- E. Historical remarks 26
- F. Putting DI-QKD protocols into practice 27
- G. Measurement device independence 27
- H. Twin-field QKD 29

V. Experimental DV-QKD protocols 31
- A. Detector technology 31
- B. Decoy state BB84 31
- C. Differential phase shift QKD 32
- D. Coherent one-way 33
- E. DV MDI-QKD 33
- F. Twin-Field QKD 35
- G. High-dimensional QKD 35
- H. Photonic integrated circuits 37

VI. Satellite quantum communications 39
- A. Introduction 39

B. The satellite opportunity 40
C. Type of orbits and applications 40
1. Space-link losses 40
2. LEO satellites 41
3. Higher Earth orbits (MEO and GEO) 42
4. Night and day use of the link 42
D. Beyond satellite QKD 42
1. Other protocols 42
2. Tests of quantum mechanics in space 43
E. Concluding remarks 44

VII. Continuous-variable QKD 44
A. Brief introduction to CV systems 44
B. Historical outline 44
C. One-way CV-QKD protocols 45
D. Computation of the key rate 46
E. Ideal performances in a thermal-loss channel 47
F. Finite-size aspects 47
G. Two-way CV-QKD protocols 48
1. Asymptotic security of two-way CV-QKD 48
2. Asymptotic key rates 49
3. Further considerations 49
H. Thermal-state QKD 50
1. One-way thermal communication 50
2. Two-way thermal communication 50
I. Unidimensional protocol 51
J. CV-QKD with discrete modulation 51
K. CV MDI-QKD 52
1. Basic concepts and protocol 52
2. Asymptotic security 52
3. Composable security 53
4. Variants of CV MDI-QKD 54
5. Multipartite CV MDI-QKD 54

VIII. Experimental CV-QKD 54
A. Introduction 54
B. Point-to-point CV-QKD 54
1. Coherent state encoding 55
2. Detection 55
3. Post-processing 58
C. Implementation of advanced CV-QKD 58
1. Squeezed-state protocols 59
2. CV MDI-QKD 59

IX. Theoretical security aspects 59
A. Finite-size analysis in QKD 59
B. Finite-size statistical analysis 60
1. Privacy amplification (PA) 60
2. Guaranteeing large smooth min-entropy 60
C. Uncertainty principle versus entanglement: an intuitive approach to QKD security 61
D. Composable security of CV-QKD protocols 61
1. Entropic uncertainty relations 62
2. Gaussian de Finetti reduction 62
E. Extensions and Outlook 62

X. Quantum hacking 63
A. Hacking DV-QKD protocols 63
1. PNS and intensity-based attacks 64
2. Trojan horse attacks 64

3. Backflash attacks 65
4. Faked states and detector efficiency mismatch 66
B. Hacking CV-QKD protocols 67
1. Attacks on the local oscillator 67
2. Saturation attacks on detectors 68
3. Trojan horse attacks 68
C. General considerations 68
D. Device-independence as a solution? 69

XI. Limits of point-to-point QKD 69
A. Overview of the main contributions 69
B. Adaptive protocols and two-way assisted capacities 71
C. General weak-converse upper bound 73
D. LOCC simulation of quantum channels 73
E. Teleportation covariance and simulability 74
F. Strong and uniform convergence in teleportation simulation 74
G. Stretching of an adaptive protocol 75
H. Single-letter upper bound for two-way assisted capacities 76
I. Bounds for teleportation-covariant channels 76
J. Capacities for distillable channels 77
K. Open problems 78

XII. Repeater chains and quantum networks 78
A. What is a quantum repeater? 78
B. Information-theoretic limits for repeater-assisted quantum communications 79
1. Ideal chains of quantum repeaters 79
2. Quantum communication networks 80
C. Quantum repeaters based on ED and QEC 82
1. Probabilistic ED repeaters 83
2. Deterministic ED repeaters 83
3. Memory-less QEC repeaters 84
4. Other studies on quantum repeaters 85

XIII. QKD against a bounded quantum memory 85
A. Introduction 85
B. Entropic uncertainty relations for multiple observables 85
C. QKD in the bounded quantum storage model 86
D. Quantum data locking 86
E. Quantum data locking for communication: the quantum enigma machine 87
F. Practical quantum data locking 88
G. Experimental demonstrations 88

XIV. Quantum random number generation 89
A. Introduction 89
B. Protocols for DI-QRE 90
1. The setup for DI-QRE 90
2. The spot-checking CHSH QRE protocol 90
C. Historical remarks and further reading 91
D. Implementations 91
E. Randomness amplification 91

XV. Quantum digital signatures 92
A. Introduction 92
B. Definitions and security properties 92
C. What is a *quantum* digital signature scheme and why it is useful? 93
D. The Lamport one-time signature scheme 94
E. The Gottesman-Chuang QDS 94
1. The protocol 94
2. Security intuition 95

3. Remarks 95
4. Practical limitations of GC-QDS 96
F. Practical QDS: Lifting the limitations 96
1. Simplifying state comparison 96
2. No quantum memory requirement 97
3. QDS from QKD technology 98
4. Insecure quantum channels 98
G. A generic modern QDS protocol 98
1. Description 98
2. Security intuition and performance 99
H. Extending QDS: Multiple parties, longer messages, and MDI 99
I. Experimental QDS realizations 100
1. Proof-of-principle 100
2. Kilometer-range and fully-secure QDS 100
J. Classical unconditional secure signatures 101
K. Summary and outlook 101

XVI. Post-quantum cryptography 102
A. Overview 102
B. Lattice-based protocols 102
C. Code-based protocols 102
D. Hash-based protocols 102
E. Other categories of protocols 103
F. Can quantum cryptography fully replace classical (public-key) cryptography? 103
G. Further issues and essential quantum research 103

XVII. Further topics in quantum cryptography 103
A. Basic cryptographic primitives 104
B. Cyptographic functionalities 104
C. Secure quantum computing 104

XVIII. Conclusions 105

Acknowledgments 105

A. Formulas for Gaussian states 106
1. Symplectic action and its computation 106
2. Fidelity between arbitrary Gaussian states 107
3. Entropic quantities 108

B. Composable secret key rate of a CV-QKD protocol 109
1. ϵ-security under collective attacks 109
2. Parameter estimation 111
3. Extension to coherent attacks 112

C. List of commonly-used symbols and some acronyms 113

References 115

I. INTRODUCTION

Quantum information [1–21] is the core science behind the so-called second quantum revolution or quantum 2.0 [22]. This is the rapid development of new disrupting technologies based on the most powerful features and resources of quantum mechanics, such as quantum entanglement [23], teleportation [24–27], and the no-cloning theorem [28, 29], just to name a few. In this context, quantum computing [1] has recently gained a lot of momentum, also thanks to the involvement of multinational corporations competing to develop large quantum computers. Superconducting chips based on Josephson junctions [30] are rapidly scaling up their number of qubits and soon may start to factorize non-trivial integers by using Shor's algorithm [31, 32]. The threat for the Rivest-Shamir-Adleman (RSA) protocol [33] and the other public key cryptosystems not only comes from quantum computing but also from potential advances in number theory, where an efficient factorization algorithm might be found for classical Turing machines (e.g., already in 2004 the test of primality has become polynomial, thanks to the Agrawal-Kayal-Saxena algorithm [34]).

An important point to understand is that the fragility of current classical cryptosystems not only is a potential threat for the present, but a more serious and realistic threat for the future. Today, eavesdroppers may intercept cryptograms that they are not able to decrypt. However, they may store these encrypted communications and wait for their decryption once a sufficiently large quantum computer is technologically available (or a new classical algorithm is discovered). This means that the confidentiality of messages may have a very limited lifespan. Following Ref. [35], consider the length of time x (in years) we need the classical cryptographic keys to be secure (*security shelf-life*). Then, consider the time y needed to adapt the current classical infrastructure with quantum-secure encryption (*migration time*). Finally, call z the *collapse time*, which is the time for a large quantum computer to be built. If $x + y > z$ then "worry" [35]. In fact, because z might be small while x is fixed, we want y to be small, i.e., start the migration to quantum-secure encryption as soon as possible.

In order to move to quantum-safe cryptography, two approaches are currently considered: quantum key distribution (QKD) and post-quantum cryptography. Let us start from the latter, which is an area of classical cryptography. It exploits cryptosystems whose security relies on classical computationally-hard problems different from those that quantum computers are known to efficiently solve (such as factoring or discrete log). This is certainly one option but it does not completely solve the problem: security may be suddenly broken by the discovery of new quantum (or even classical) algorithms.

By contrast, QKD promises the ultimate security solution by resorting to quantum systems to generate secret correlations. In this case, security relies on unbreakable principles of nature, such as the uncertainty principle or the monogamy of entanglement [36–40]. Even though an ideal realization of QKD offers a complete encryption of a communication channel, realistic implementations of QKD protocols open loopholes and practical problems at the level of the devices locally used by the remote parties (e.g., modulators, detectors etc.). These may be subject to all sorts of hacking and side-channel attacks. In this scenario, fully-device independent QKD protocols [41, 42] represent the safest possible implementation, but their high level of security is achieved at the expense of very low secret key rates. On the other hand, more practical QKD protocols assume some level of trust in their devices. In this way, they can achieve reasonable key rates, but at the cost of a lower level of security.

Besides the discussed trade-off between security and rate, there is also another one which is between rate and distance. Today, we know that there is a fundamental limit which restricts any point to point implementation of QKD. Given a lossy link with transmissivity η, two parties cannot distribute more than the secret key capacity of the channel, which is $-\log_2(1-\eta)$ [43]. This is also known as the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound which gives the exact linear scaling of 1.44η secret bits per channel use at long distances. Ideal implementations of QKD protocols based on continuous-variable (CV) systems [8] and Gaussian states [7] may approach this capacity [44], while those based on discrete variable (DV) systems may fall below by additional factors. In order to overcome this limit and enable long-distance high-rate implementations of QKD, one needs to introduce quantum repeaters (also known as quantum relays) in the lossy communication channel.

The most practical and effective way to achieve this goal is to introduce a chain of trusted repeaters between the remote parties and, more generally, a network of trusted nodes. A number of trusted-node QKD networks have been or are being constructed, from metropolitan to wider scales. In this regard, let us mention the DARPA Quantum Network [45, 46], the Vienna QKD network [47], the Chinese hierarchical metropolitan network [48], the Tokyo QKD network [49], the Beijing-Shanghai 2000km quantum line [50], and the UK quantum network [51]. A better option would be the development of QKD chains and networks that are based on untrusted repeaters/nodes. These would be "end-to-end" in the sense that their security would only rely on the successful authentication of the remote end-users, but not on that of the middle nodes. In a basic single-repeater scenario, this idea can be realized without the distribution of entanglement as originally proposed in the protocol of measurement-device independent (MDI) QKD [52, 53] and, more recently and efficiently, in the protocol of twin-field QKD [54]. A stronger but more challenging approach would be the use of quantum repeaters for entanglement distillation [55–57]. The remote and certified distillation of entanglement bits (ebits) would exclude the intromission of any eavesdropper, so that the repeaters may be untrusted and could be used to implement device-

independent (DI) QKD. Today there are a number of studies on chains and QKD networks based on trusted-, untrusted-, and entanglement-distillation nodes [58–78].

In all this panorama, the present review aims at providing an overview of the most important results and the most recent advances in the field of quantum cryptography, both theoretically and experimentally. After a brief introduction of the general notions, we will review the main QKD protocols based on discrete- and continuous-variable systems. We will consider standard QKD, device-independent and measurement-device independent QKD. We will discuss the various levels of security for the main communication channel, from asymptotic security proofs to finite-size effects and composability aspects. We will also review quantum hacking and side-channel attacks. Then, we will present the most recent progress in the exploration of the ultimate limits of QKD. In particular, we will discuss the secret key capacities associated with the most important models of quantum channels over which we may implement point-to-point QKD protocols, and their extension to quantum repeaters and networks. Practical aspects of quantum repeaters will then be thoroughly discussed. Finally, we will treat topics beyond traditional QKD, including quantum data locking, quantum random number generators, and quantum digital signatures, with also some discussion on post-quantum cryptography.

While it is certainly reductive for the field to highlight just a few of the many excellent contributions produced in the last years, it is also true that two recent breakthroughs need a particular mention. The first mention is the rapid development of satellite quantum communications, including the experimental realization of the first intercontinental QKD network between cities in China and Austria [79, 80]. The second mention is the introduction of twin-field QKD [54]. This protocol achieved what MDI QKD [52, 53] somehow missed to achieve, i.e., beating the secret key capacity of point-to-point lossy communications (PLOB bound [43]) by means of an untrusted measurement-based QKD repeater. Twin-field QKD paved the way for a completely new family of long-distance end-to-end QKD protocols, whose state of the art is summarized in this review.

II. BASIC NOTIONS IN QUANTUM KEY DISTRIBUTION

A. Generic aspects of a QKD protocol

In our review we consider both discrete-variable systems, such as qubits or other quantum systems with finite-dimensional Hilbert space, and CV systems, such as bosonic modes of the electromagnetic field which are described by an infinite-dimensional Hilbert space. There a number of reviews and books on these two general areas (e.g., see Refs. [1, 7]). Some of the concepts are repeated in this review but we generally assume basic knowledge of these systems. Here we mention some general aspects that apply to both types of systems.

A generic "prepare and measure" QKD protocol can be divided in two main steps: quantum communication followed by classical postprocessing. During quantum communication the sender (Alice) encodes instances of a random classical variable α into non-orthogonal quantum states. These states are sent over a quantum channel (optical fiber, free-space link) controlled by the eavesdropper (Eve), who tries to steal the encoded information. The linearity of quantum mechanics forbids to perform perfect cloning [28, 29], so that Eve can only get partial information while disturbing the quantum signals. At the output of the communication channel, the receiver (Bob) measures the incoming signals and obtains a random classical variable β. After a number of uses of the channel, Alice and Bob share raw data described by two correlated variables α and β.

The remote parties use part of the raw data to estimate the parameters of the channel, such as its transmissivity and noise. This stage of parameter estimation is important in order to evaluate the amount of post-processing to extract a private shared key from the remaining data. Depending on this information, they in fact perform a stage of error correction (EC), which allows them to detect and eliminate errors, followed by a stage of privacy amplification (PA) that allows them to reduce Eve's stolen information to a negligible amount. The final result is the secret key.

Depending on which variable is guessed, we have direct or reverse reconciliation. In direct reconciliation (DR), it is Bob that post-process its outcomes in order to infer Alice's encodings. This procedure is usually assisted by means of forward classical communication (CC) from Alice to Bob. By contrast, in reverse reconciliation (RR), it is Alice who post-process her encoding variable in order to infer Bob's outcomes. This procedure is usually assisted by a final round of backward CC from Bob to Alice. Of course, one may more generally consider two-way procedures where the extraction of the key is helped by forward and feedback CCs, which may be even interleaved with the various communication rounds of the protocol.

Let us remark that there may also be an additional post-processing routine, called sifting, where the remote parties communicate in order to agree instances while discard others, depending on the measurement bases they have independently chosen. For instance this happens in typical DV protocols, where the Z-basis is randomly switched with the X-basis, or in CV protocols where the homodyne detection is switched between the q and the p quadrature.

Sometimes QKD protocols are formulated in entanglement-based representation. This means that Alice' preparation of the input ensemble of states is replaced by an entangled state Ψ_{AB} part of which is measured by Alice. The measurement on part A has the effect to conditionally prepare a state on part B.

The outcome of the measurement is one-to-one with the classical variable encoded in the prepared states. This representation is particularly useful for the study of QKD protocols, so that their prepare and measure formulation is replaced by an entanglement-based formulation for assessing the security and deriving the secret key rate.

B. Asymptotic security and eavesdropping strategies

The asymptotic security analysis is based on the assumption that the parties exchange a number $n \gg 1$ (ideally infinite) of signals. The attacks can then be divided in three classes of increasing power: Individual, collective, and general-coherent. If the attack is individual, Eve uses a fresh ancilla to interact with each transmitted signal and she performs individual measurements on each output ancillary systems. The individual measurements can be done run-by-run or delayed at the end of the protocol, so that Eve may optimize over Alice and Bob's CC (also known as delayed-choice strategy). In the presence of an individual attacks, we have three classical variables for Alice, Bob and Eve, say α, β and γ. The asymptotic key rate is then given by the difference of the mutual information [81] I among the various parties according to Csiszar and Korner's classical theorem [82]. In DR ($\blacktriangleright$), we have the key rate

$$R^{\blacktriangleright} := I(\alpha : \beta) - I(\alpha : \gamma), \tag{1}$$

where $I(\alpha : \beta) := H(\alpha) - H(\alpha|\beta)$, with H being the Shannon entropy, and $H(|)$ its conditional version [81]. In RR ($\blacktriangleleft$), we have instead

$$R^{\blacktriangleleft} := I(\alpha : \beta) - I(\beta : \gamma), \tag{2}$$

If the attack is collective then Eve still uses a fresh ancilla for each signal sent but now her output ancillary systems are all stored in a quantum memory which is collectively measured at the end of the protocol after Alice and Bob's CCs. In this case, we may compute a lower bound to the key rate by replacing Eve's mutual information with Eve's Holevo information [83] on the relevant variable. In DR, one considers Eve's ensemble of output states conditioned to Alice's variable α, i.e., $\{\rho_{\mathrm{E}|\alpha}, P(\alpha)\}$ where $P(\alpha)$ is the probability of the encoding α. Consider then Eve's average state $\rho_{\mathrm{E}} := \int d\alpha P(\alpha)\rho_{\mathrm{E}|\alpha}$. Eve's Holevo information on α is equal to

$$I(\alpha : E) := S(\rho_{\mathrm{E}}) - \int d\alpha P(\alpha) S(\rho_{\mathrm{E}|\alpha}), \tag{3}$$

where $S(\rho) := -\mathrm{Tr}(\rho \log_2 \rho)$ is the von Neumann entropy. In RR, Eve's Holevo information on β is given by

$$I(\beta : E) := S(\rho_{\mathrm{E}}) - \int d\beta P(\beta) S(\rho_{\mathrm{E}|\beta}), \tag{4}$$

where $\rho_{\mathrm{E}|\beta}$ is Eve's output state conditioned to the outcome β with probability $P(\beta)$. Thus, we may write the two key rates [84]

$$R^{\blacktriangleright} := I(\alpha : \beta) - I(\alpha : E), \tag{5}$$

$$R^{\blacktriangleleft} := I(\alpha : \beta) - I(\beta : E). \tag{6}$$

In a general-coherent attack, Eve's ancillae and the signal systems are collectively subject to a joint unitary interaction. The ancillary output is then stored in Eve's quantum memory for later detection after the parties' CCs. In the asymptotic scenario, it has been proved [85] that this attack can be reduced to a collective one by running a random symmetrization routine which exploits the quantum de Finetti theorem [85–87]. By means of random permutations, one can in fact transform a general quantum state of n systems into a tensor product $\rho^{\otimes n}$, which is the structure coming from the identical and independent interactions of a collective attack.

C. Finite-size effects

Finite-size effects come into place when the number of signal exchanged n is not so large to be considered to be infinite (see Sec. IX for more details). If we assume that the parties can only exchange a finite number of signals, them the key rate must be suitably modified and takes the form

$$R := \xi I(\alpha : \beta) - \chi_{\mathrm{E}} - \Delta(n, \epsilon). \tag{7}$$

Here ξ accounts for non-ideal reconciliation efficiency of classical protocols of EC and PA, while $\Delta(n, \epsilon)$ represents the penalty to pay for using the Holevo quantity $\chi_{\mathrm{E}} = I(\alpha : \mathrm{E})$ or $I(\beta : \mathrm{E})$ in the non-asymptotic context. An important point is the computation of $\Delta(n, \epsilon)$ which is function of the number of signals exchanged n, and of composite ϵ-parameter that contains contributions from the probability that the protocol aborts, the probability of success of EC, PA etc. This is related to the concept of composability that we briefly explain in the next section. Composable security proofs are today known for both discrete- and continuous-variable QKD protocols [88–95].

D. Composable security of QKD

Cryptographic tasks often form parts of larger protocols. Indeed the main reason for our interest in QKD is that secure communication can be built by combining key distribution with the one-time pad protocol. If two protocols are proven secure according to a composable security definition, then the security of their combination can be argued based on their individual functionalities and *without* the need to give a separate security proof for the combined protocol. Since individual cryptographic tasks are often used in a variety of applications, composability is highly desirable. Furthermore, the early

security proofs for QKD [96, 97] did not use a composable definition and were consequently shown to be inadequate (even when combined with the one-time pad) [98].

The concept of composability was first introduced in classical cryptography [99–102] before being generalized to the quantum setting [103–105]. A new security definition was developed [106, 107] that is composable in the required sense and is the basis of the accepted definition, which we discuss here. The main idea behind a composable security definition is to define an ideal protocol, which is secure by construction, and then show that the real implementation is virtually indistinguishable from the ideal in *any* situation. Therefore, in effect it takes into account the worst possible combined protocol for the task in question. To think about this concretely, it is often phrased in terms of a game played by a distinguisher whose task it is to guess whether Alice and Bob are implementing the real protocol or the ideal. The distinguisher is permitted to do anything that an eavesdropper could in a real implementation of the protocol. They are also given access to the outputs of the protocol, but not to any data private to Alice and Bob during the protocol (e.g., parts of any raw strings that are not publicly announced).

Coming up with a reasonable ideal for a general cryptographic task is not usually straightforward because the ideal and real protocols have to be virtually indistinguishable even after accounting for all possible attacks of an adversary. However, in the case of key distribution it is relatively straightforward. The ideal can be phrased in terms of a hypothetical device that outputs string S_A to Alice and S_B to Bob (each having n possible values) such that

$$\rho^{\mathrm{id}}_{S_A S_B E} = \frac{1}{n}\sum_{x=0}^{n-1} |x\rangle\langle x| \otimes |x\rangle\langle x| \otimes \rho_E \,. \tag{8}$$

This captures that Alice's and Bob's strings are identical and uncorrelated with E (which represents all of the systems held by Eve). These conditions are often spelled out separately:

1. $P(S_A \neq S_B)_{\rho^{\mathrm{id}}} = 0$ (correctness, i.e., Alice and Bob have identical outputs).

2. $\rho^{\mathrm{id}}_{S_A E} = n^{-1}\mathbb{1}_n \otimes \rho_E$, where $\mathbb{1}_n$ is the identity operator (the output string is secret).

The ideal protocol then says perform the real protocol and if it does not abort, replace the output with one from this hypothetical device with the same length. It may seem strange that the ideal involves running the real. However, if the ideal protocol just said use the hypothetical device, a distinguisher could readily distinguish it from the real protocol by blocking the quantum channel between Alice and Bob. This would force the real protocol to abort, while the ideal would not. By defining the ideal using the real protocol, both protocols abort with the same probability for any action of the distinguisher.

From the point of view of the distinguisher, the aim is to distinguish two quantum states: those that the protocol outputs in the real and ideal case. The complete output of the real protocol (taking into account the possibility of abort) can be written

$$\sigma^{\mathrm{re}}_{S_A S_B E} = p(\perp)|\perp\rangle\langle\perp| \otimes |\perp\rangle\langle\perp| \otimes \rho^{\perp}_E + p(\bar{\perp})\rho^{\mathrm{re}}_{S_A S_B E} \,, \tag{9}$$

where

$$\rho^{\mathrm{re}}_{S_A S_B E} = \sum_{xy} P_{XY}(x,y)|x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \rho^{x,y}_E \tag{10}$$

is the state conditioned on the real protocol not aborting, $|\perp\rangle$ as a special symbol representing abort (this is orthogonal to all the $|x\rangle$ or $|y\rangle$ terms in the sum), $p(\perp)$ and $p(\bar{\perp}) = 1 - p(\perp)$ are the probabilities of abort and not abort respectively. (Note that any information sent over the authenticated public channel that Eve could listen in on during the implementation is included in E.) The output of the ideal is instead

$$\sigma^{\mathrm{id}}_{S_A S_B E} = p(\perp)|\perp\rangle\langle\perp| \otimes |\perp\rangle\langle\perp| \otimes \rho^{\perp}_E + p(\bar{\perp})\rho^{\mathrm{id}}_{S_A S_B E} \,, \tag{11}$$

with $\rho^{\mathrm{id}}_{S_A S_B E}$ defined in Eq. (8).

The measure of distinguishability for these is the trace distance D [1]. This has the operational meaning that, given either $\sigma^{\mathrm{re}}_{S_A S_B E}$ or $\sigma^{\mathrm{id}}_{S_A S_B E}$ with 50% chance of each, the optimal probability of guessing which is

$$p_{\mathrm{guess}} = \frac{1}{2}[1 + D(\sigma^{\mathrm{re}}_{S_A S_B E}, \sigma^{\mathrm{id}}_{S_A S_B E})], \tag{12}$$

which accounts for any possible quantum strategy to distinguish them. If the distance is close to zero, then the real protocol is virtually indistinguishable from the real. Quantitatively, if $D(\sigma^{\mathrm{re}}_{S_A S_B E}, \sigma^{\mathrm{id}}_{S_A S_B E}) \leq \varepsilon$ for all possible strategies an eavesdropper could use, then the protocol is said to be ε-secure. The analogue of this definition for probability distributions was used in Ref. [108] to prove security of a QKD protocol against an adversary limited only by the no-signalling principle. However, it is more common to express security in another way as described below.

By using properties of the trace distance it can be shown that the probability of successfully distinguishing can be bounded by the sum of contributions from the two conditions stated previously [109]. These are usually called the *correctness error*

$$\varepsilon_{\mathrm{corr}} = p(\bar{\perp})P(S_A \neq S_B)_{\rho^{\mathrm{re}}} \,, \tag{13}$$

and the *secrecy error*,

$$\varepsilon_{\mathrm{secr}} = p(\bar{\perp})D(\rho^{\mathrm{re}}_{S_A E}, n^{-1}\mathbb{1}_n \otimes \rho_E) \,. \tag{14}$$

The correctness error is the probability that the protocol outputs different keys to Alice and Bob. The secrecy error is the probability that the key output to Alice can be distinguished from uniform given the system E. In security proofs it is often $\varepsilon_{\mathrm{corr}}$ and $\varepsilon_{\mathrm{secr}}$ that are computed.

III. OVERVIEW OF DV-QKD

DV protocols can be seen as the earliest (and possibly the simplest) form of QKD. Despite the development of the famous BB84 protocol with its name accorded based on a 1984 paper [110], the first ideas for the use of quantum physics in the service of security can be traced as far back as the early 70s. Wiesner was then exploring the idea of making bank notes that would resist counterfeit [111]. The first paper published on quantum cryptography was in 1982 [112]. (A detailed history on the beginnings of quantum cryptography can be found in Ref. [111].) In this section we give a brief description of DV protocols for QKD. It is instructive to introduce some preliminary notation which will be useful in the subsequent sections. The reader expert in quantum information may skip most of the following notions.

A. Preliminary notions

Recall that a qubit is represented as a vector in a bidimensional Hilbert space, which is drawn by the following basis vectors

$$|0\rangle \equiv \begin{pmatrix}1\\0\end{pmatrix}, \quad |1\rangle \equiv \begin{pmatrix}0\\1\end{pmatrix}. \tag{15}$$

Any pure qubit state can thus be expressed as a linear superposition of these basis states,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle, \tag{16}$$

with $\theta \in (0,\pi)$, $\phi \in (0,2\pi)$ and i the imaginary unit. This state can be pictorially represented as a vector in the so-called "Bloch sphere". When $\theta = 0$ or $\theta = \pi$, we recover the basis states $|0\rangle$ and $|1\rangle$, respectively, which are placed at the poles of the sphere. When $\theta = \pi/2$, the qubit pure state is a vector lying on the equator of the sphere. Here we can identify the four vectors aligned along the $\hat{x}$ and $\hat{y}$ axes, which are obtained in correspondence of four specific values of ϕ, i.e., we have

$$\phi = 0: \qquad |+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \tag{17}$$

$$\phi = \pi: \qquad |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}, \tag{18}$$

$$\phi = \pi/2: \quad |+i\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}, \tag{19}$$

$$\phi = 3\pi/2: |-i\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}. \tag{20}$$

The basis vectors in Eq. (15) are eigenstates of the Pauli operator (matrix)

$$\sigma_z = Z = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}. \tag{21}$$

We call them the "Z basis", as it is customary in QKD. Similarly, the states in Eqs. (17) and (18) are eigenstates of the Pauli operator (matrix)

$$\sigma_x = X = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}, \tag{22}$$

and are known as the X basis. Finally, the states in Eqs. (19) and (20) are eigenstates of the Pauli operator (matrix)

$$\sigma_y = Y = \begin{pmatrix}0 & -i\\i & 0\end{pmatrix}, \tag{23}$$

and are known as the Y basis. These pairs of eigenstates form two mutually unbiased bases (MUB). Formally, two orthogonal basis of a d-dimensional Hilbert space, say $\{|\psi_1\rangle, ..., |\psi_d\rangle\}$ and $\{|\phi_1\rangle, ..., |\phi_d\rangle\}$, are mutually unbiased if $|\langle\psi_i|\phi_j\rangle|^2 = 1/d$ for any i and j. Measuring a state of one MUB using the other basis would produce a completely random result.

Using the three Pauli matrices and the bidimensional identity operator (matrix)

$$\mathbb{1} = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, \tag{24}$$

it is possible to write the most generic state of a qubit in the form of a density operator,

$$\rho = \frac{1}{2}\mathbb{1} + \vec{n}\cdot\vec{\sigma}, \tag{25}$$

with $\vec{n}$ the Bloch vector and $\vec{\sigma} = \{\sigma_x, \sigma_y, \sigma_z\}$. This notation comes handy when the qubit states are mixed, which can be described with a vector $\vec{n}$ whose modulo is less than 1, as opposed to pure states, for which $|\vec{n}| = 1$.

To give a physical meaning to the representation of a qubit, we can interpret the qubit state in Eq. (16) as the polarization state of a photon. This is also known as "polarization qubit". In this case, the Bloch sphere is conventionally called the Poincaré sphere, but its meaning is unchanged. The basis vectors on the poles of the Poincaré sphere are usually associated with the linear polarization states $|H\rangle = |0\rangle$ and $|V\rangle = |1\rangle$, where H and V refer to the horizontal or vertical direction of oscillation of the electromagnetic field, respectively, with respect to a given reference system. The X basis states are also associated with linear polarization but along diagonal ($|D\rangle = |+\rangle$) and anti-diagonal ($|A\rangle = |-\rangle$) directions. Finally, the Y basis states are associated with right-circular ($|R\rangle = |+i\rangle$) and left-circular ($|L\rangle = |-i\rangle$) polarization states. Any other state is an elliptical polarization state and can be represented by suitably choosing the parameters θ and ϕ.

It is worth noting that polarization can be cast in one-to-one correspondence with another degree of freedom of the photon which is particularly relevant from an experimental point of view. This is illustrated in Fig. 1. The light source emits a photon that is split into two arms

by the first beam-splitter (BS). The transmission of this BS represents the angle θ of the Bloch sphere. More precisely, if r and t are the reflection and transmission coefficients of the BS, respectively, such that $|r|^2+|t|^2=1$, we can write $r=\cos(\theta/2)$ and $t=e^{i\phi}\sin(\theta/2)$ so to recover Eq. (16). If the BS is 50:50, then $\theta=\pi/2$ and the state after the BS becomes

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\phi}|1\rangle\right). \tag{26}$$

The phase ϕ now has a clear physical meaning, i.e., it represents the relative electromagnetic phase between the upper and lower arms of the interferometer in Fig. 1. This phase can be modified by acting on the phase shifters in Fig. 1 and this is one of the most prominent methods to encode and decode information in QKD. In fact, it is fair to say that the vast majority of QKD experiments were performed using either the polarization or the relative phase to encode information.

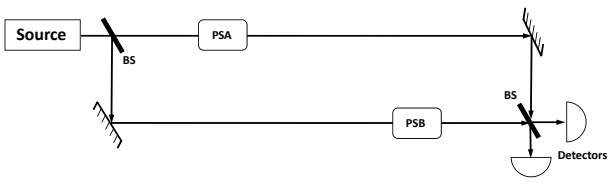

FIG. 1. Fundamental phase-based interferometer. BS: beam-splitter; PSA: phase shift Alice; PSB: phase shift Bob. Adapted with permission from Ref. [113] ©APS (1992).

As we well know, from a historical perspective, the first QKD protocols were introduced using DVs, especially polarization. This remains even today one of the simplest ways to describe an otherwise complex subject. The seminal BB84 protocol [110] was described using polarization. In 1991 Ekert suggested a scheme, the "E91" [114], that for the first time exploits entanglement for cryptographic purposes. The conceptual equivalence of this scheme with the BB84 protocol was demonstrated in 1992 by Bennett, Brassard and Mermin [115], who also proposed a simplified version of the E91 later called BBM92 or more simply Einstein-Podolsky-Rosen (EPR) scheme. However, this supposed equivalence cannot be taken strictly as it can be shown that the entangled based protocol of E91 can provide device independent security, which is impossible for the BB84 using separable states even in a noise free scenario [116].

A few years later, Lo and Chau [117] and Shor and Preskill [97] exploited this equivalence between the prepare-and-measure BB84 and the entanglement-based BBM92 to demonstrate the unconditional security of the BB84 protocol. Another important protocol, the "B92" [113], was proposed in 1992 by Bennett, showing that QKD can be performed with even only two non-orthogonal states [28, 29]. The idea of exploiting non-orthogonality was later extended to more sophisticated bipartite schemes by Goldenberg and Vaidman [118], Koashi and Imoto [119] and Noh [120]. Even though these protocols are based on bipartite states that are orthogonal, their security relies on the fact the eavesdropper cannot simultaneously access both the systems prepared by the sender, but only one of them which is instead described by non-orthogonal states [121]. Finally, note that non-orthogonality also has a bipartite formulation in terms of quantum discord [122, 123], so that the presence of the latter can be shown to be a necessary (but not sufficient) condition for security [124].

B. Prepare and measure protocols

In this section, we outline the most intuitive and practical DV-QKD protocols, called "prepare-and-measure" protocols. The transmitting user, Alice, prepares the signals by encoding a discrete random variable (typically a binary variable) in a quantum system with finite degrees of freedom, typically the polarization of an optical photon (polarization qubit). These signals are then sent to the receiving user, Bob, who measures them in order to retrieve the encoded information. In order to describe the modus operandi of the various protocols, here we assume the ideal case of single-photon sources.

1. BB84 protocol

In the BB84 protocol with polarization qubits, Alice prepares a random sequence of four states in two MUBs. These are usually chosen as $|0\rangle$, $|1\rangle$ (Z basis), and $|+\rangle$, $|-\rangle$ (X basis). However, other choices are possible, including the four states in Eqs. (17)-(20). The users associate the binary digit 0 with the non-orthogonal states $|0\rangle$ and $|+\rangle$, and the binary digit 1 with the other non-orthogonal states $|1\rangle$ and $|-\rangle$. The non-orthogonality condition guarantees that Eve (an eavesdropper) cannot clone the states with perfect fidelity [28, 29]. This implies that: (i) Eve cannot perfectly retrieve the information encoded by Alice; and (ii) Eve's action causes a disturbance on the quantum states that can be detected by the legitimate users.

The states prepared by Alice are sent to Bob, who then measures them in one of the two bases Z or X, selected at random. See Table I. Note that, if Bob chooses the same basis as Alice, then Bob should exactly decode Alice's input. By contrast, If Bob chooses the wrong basis, his result, and thus the bit he reads, will be random. For this reason, when the quantum communication is over, Bob exploits a classical public channel to inform Alice about what basis he used to measure each photon. Alice reports back her bases and they discard all the events corresponding to the use of different bases. After this sifting operation, the two parties should have two identical strings of bits, forming the so-called "sifted key".

In practice, however, the communication line is noisy and this noise has to be fully ascribed to Eve in the worst-

Alice's encoding			Bob's decoding	
basis	bit	state	Z	X
Z	0	$\|0\rangle$	0	?
	1	$\|1\rangle$	1	?
X	0	$\|+\rangle$	?	0
	1	$\|-\rangle$	?	1

TABLE I. Summary of Alice's encoding (left) and Bob's decoding (right) in BB84. Here "?" means that the output is completely random, i.e., 0 or 1 with the same probability.

case scenario. Because of the noise, Alice's and Bob's local strings will differ by an amount that can be quantified in terms of "quantum bit error rate" (QBER). This is defined as the probability that a generic bit in Bob's sifted string is different from the corresponding bit in Alice's sifted string. In order to compute the QBER, Alice and Bob perform a session of parameter estimation, where they agree to disclose a random subset of their data. Comparing these bits (later discarded), they can quantify the QBER and check if this is lower or higher than a certain security threshold of the protocol. If it is higher, it means that Eve has gain too much information. If it is lower, it means that the parties have more shared information than Eve, and they can use the classical procedures of EC and PA to derive a secret key. As a first step, they implement EC so that their strings are transformed into shorter but identical strings. Then, they implement PA, so that their common string is further shortened into a final form which is completely decoupled from Eve.

2. *Intercept-resend against the BB84 protocol*

We now describe a basic eavesdropping strategy, where Eve measures Alice's signal states and, from the outcomes, she re-prepares states to be sent to Bob. This strategy is here discussed to give an idea of how eavesdropping information automatically generates a non-trivial QBER for the parties. Assume that Alice prepares her states in the Z basis and assume that this is an instance where Bob picks the same basis for his measurement, so that the instance survives the sifting stage of the protocol. For the same instance, Eve will implement randomly either the Z or the X basis. With 50% probability, she applies the right basis Z, eavesdropping all the input information without causing any noise. With 50% probability, she applies the wrong basis X, therefore projecting Alice's input into $|+\rangle$ or $|-\rangle$ with the same probability. In this case, Eve does not retrieve any information and will randomize the system, so that Bob will also get a random output which coincides with Alice's input 50% of the times. The reasoning is similar if we start from the other basis X. See Table II for the complete scenario.

Encoding				Decoding
basis	bit	state	Eve	after sifting
Z	0	$\|0\rangle$	$\nearrow Z\left\{\begin{array}{l}\|0\rangle\\ \|1\rangle\end{array}\right. \longrightarrow Z\left\{\begin{array}{l}0\\ 1\end{array}\right.$	
	1	$\|1\rangle$		
			$\searrow X\left\{\begin{array}{l}\|+,-\rangle\\ \|+,-\rangle\end{array}\right. \longrightarrow Z\left\{\begin{array}{l}?\\ ?\end{array}\right.$	
X	0	$\|+\rangle$	$\nearrow Z\left\{\begin{array}{l}\|0,1\rangle\\ \|0,1\rangle\end{array}\right. \longrightarrow X\left\{\begin{array}{l}?\\ ?\end{array}\right.$	
	1	$\|-\rangle$		
			$\searrow X\left\{\begin{array}{l}\|+\rangle\\ \|-\rangle\end{array}\right. \longrightarrow X\left\{\begin{array}{l}0\\ 1\end{array}\right.$	

TABLE II. BB84 scenario after sifting in the presence of an intercept-resend attack (where Eve randomly switches between Z and X bases). Here "?" means that the output value decoded by Bob is completely random, i.e., 0 or 1 with the same probability. When Eve's basis matches Alice's, then no error is introduced. When Eve's basis is different from Alice's, Eve re-sends states from the other MUB and Bob gets a random output, coinciding with Alice's input 50% of the times. As a result, we have a QBER of 25%. It is clear that Eve retrieves at least the same information as Bob. As a matter of fact, she steals half of the sifted bits. On the other hand Bob, can only reconstruct $\simeq 19\%$ of the sifted bits due to the fact that, in correcting his data, he does not know which instances were perfectly eavesdropped and which ones were completely randomized by Eve.

The noise induced by this attack is quite high, corresponding to a QBER of 25% (above the security threshold of the protocol, equal to $\simeq 11\%$ as discussed afterwards). It is also clear that Eve gets at least the same information as Bob (so that the key rate is zero). More exactly, Eve is able to steal half of the sifted bits, while Alice and Bob's mutual information is given by $1 - H_2(\text{QBER}) \simeq 0.19$ key bits per sifted bit, where

$$H_2(p) := -p \log_2 p - (1-p) \log_2 (1-p) \qquad (27)$$

is binary Shannon entropy. By accounting of the sifting process, we may add a factor 1/2 and consider the information per use of the protocol or channel use. We have then $[1 - H_2(\text{QBER})]/2 < 0.1$ per channel use, compared to 0.25 bits per channel use stolen by Eve. Note also that the formula of the mutual information does not change if we use the probability of success $1 - \text{QBER}$, since the binary entropy is invariant under the exchange $p \to 1-p$.

3. Intercept-resend with an intermediate basis

The performance of the intercept-resend attack does not substantially change if Eve, instead of randomizing her measurement between the two MUBs Z and X, always applies an intermediate basis. Consider the orthogonal basis $\{|\theta\rangle, |\theta^\perp\rangle\}$, where

$$|\theta\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle, \tag{28}$$

$$|\theta^\perp\rangle = \sin(\theta/2)|0\rangle - e^{-i\phi}\cos(\theta/2)|1\rangle. \tag{29}$$

Here the choice of parameters is not limited to $\theta = 0$ (Z basis) or $\theta = \pi/2$ and $\phi = 0$ (X basis). Another possible choice is for instance $\theta = \pi/4$ and $\phi = 0$, i.e., the so-called "Breidbart basis". In general, Eve associates Alice's bit-value 0 (i.e., her states $|0\rangle$ and $|+\rangle$) to the outcome θ, and Alice's bit-value 1 (i.e., her states $|1\rangle$ and $|-\rangle$) to the other outcome θ. It is easy to compute the conditional probabilities

$$P(\theta|0) = P(\theta^\perp|1) = \cos^2(\theta/2), \tag{30}$$

$$P(\theta|+) = P(\theta^\perp|-) = \frac{1+\sin\theta\cos\phi}{2}. \tag{31}$$

and their complementary quantities ($p \to 1-p$)

$$P(\theta^\perp|0) = P(\theta|1) = \sin^2(\theta/2), \tag{32}$$

$$P(\theta^\perp|+) = P(\theta|-) = \frac{1-\sin\theta\cos\phi}{2}. \tag{33}$$

Assuming the sifted scenario where the basis Z or X is known to Eve, then we can easily compute the success probability of Eve guessing Alice's input, starting from the probabilities above and using Bayes' theorem with identical priors. For instance, assume that Alice is using the Z basis and sending the state $|0\rangle$. The probability for Eve to guess the input 0 given her outcome θ is given by $\mathrm{P}(0|\theta) = \mathrm{P}(\theta|0) = \cos^2(\theta/2)$. In fact, from Bayes' theorem, we may write

$$P(0|\theta) = \frac{P(\theta|0)P(0)}{P(\theta)}, \tag{34}$$

$$P(\theta) = P(\theta|0)P(0) + P(\theta|1)P(1). \tag{35}$$

Then, using the conditional probabilities in Eqs. (30)-(33) and the equal priors $P(0) = P(1) = 1/2$ (due to Alice's random input), we get the result above. We find similar results for the other cases, so that we may write

$$P(0|\theta) = P(1|\theta^\perp) = \cos^2(\theta/2) := P_E^Z, \tag{36}$$

$$P(+|\theta) = P(-|\theta^\perp) = \frac{1+\sin\theta\cos\phi}{2} := P_E^X. \tag{37}$$

Given Eve's probabilities of success, P_E^Z and P_E^X, of decoding Alice's sifted bit in the two bases, Z and X, we can compute the corresponding expressions for Alice and Eve's mutual information. These are given by $I_E^Z = 1 - H_2(P_E^Z)$ and $I_E^X = 1 - H_2(P_E^X)$. Considering that Alice randomly switches between bases Z and X, Eve's information is therefore given by the average $I_E = (I_E^Z + I_E^X)/2$. We can now see that, for the specific case of the Breidbart basis ($\theta = \pi/4$, $\phi = 0$), we have the symmetric scenario $P_E^Z = P_E^X := P_E$, where Eve's overall probability of guessing Alice's sifted bit is given by $P_E = (1 + 1/\sqrt{2})/2 \simeq 0.854$ (which is higher than the 75% value of the previous intercept-resend attack with switching bases). In the present attack, Eve is able to eavesdrop $I_E = 1 - H_2(P_E) \simeq 0.4$ bits per sifted bit, which is less than the 50% value of the previous intercept-resend attack with switching bases (the apparent discrepancy of the performance between guessing probability and mutual information can be understood in terms of the concavity of the Shannon entropy).

Let us now compute the QBER, first assuming the general basis in Eqs. (28) and (29), and then specifying the result for the Breidbart basis. Let us start by considering the Z basis, with Alice sending $|0\rangle$. When Eve projects the incoming polarization qubit onto the state $|\theta\rangle$, with probability $P(\theta|0) = \cos^2(\theta/2)$, Bob gets an erroneous result with probability $P(1|\theta) = \sin^2(\theta/2)$. If Eve projects onto $|\theta^\perp\rangle$, with probability $P(\theta^\perp|0) = \sin^2(\theta/2)$, Bob has an error with probability $P(1|\theta^\perp) = \cos^2(\theta/2)$. Therefore, we find the error probability

$$\begin{aligned} P(1|0) &= P(1|\theta)P(\theta|0) + P(1|\theta^\perp)P(\theta^\perp|0) \\ &= 2\cos^2(\theta/2)\sin^2(\theta/2) = (\sin^2\theta)/2. \end{aligned} \tag{38}$$

It is easy to check that the error probability has the same expression when Alice sends $|1\rangle$, so that we may write $P_{\rm err}^Z = P(0|1) = P(1|0)$ for the Z basis.

A similar calculation can be done when Alice uses the X basis sending $|+\rangle$ or $|-\rangle$. One finds $P_{\rm err}^X = P(-|+) = P(+|-) = (1 - \sin^2\theta\cos^2\phi)/2$. As a result, the average error probability (QBER) is equal to

$$P_{\rm err} = (P_{\rm err}^Z + P_{\rm err}^X)/2 = [1 + (1-\cos^2\phi)\sin^2\theta]/4. \tag{39}$$

For the Breidbart basis, a simple replacement in Eq. (39) provides a QBER of 25%, exactly as in the previous attack with switching bases. Alice and Bob's mutual information is again $\simeq 0.19$ key bits per sifted bit, lower than Eve's stolen information ($\simeq 0.4$), so that no secret key can be generated.

4. Optimal eavesdropping strategy of the BB84 protocol

A more powerful strategy that Eve can consider is to attach an ancilla E (i.e., a quantum system with possibly higher dimension than a qubit) to the incoming Alice's qubit. Let its state $|E\rangle$ unitarily interact with Alice's qubit state in the hope of gleaning some information. With respect to Alice computational Z basis $\{|0\rangle, |1\rangle\}$, this unitary interaction can be written as

$$U|0\rangle|E\rangle = |0\rangle|F_0\rangle + |1\rangle|D_0\rangle, \tag{40}$$

$$U|1\rangle|E\rangle = |1\rangle|F_1\rangle + |0\rangle|D_1\rangle, \tag{41}$$

with $|F_{0,1}\rangle$ and $|D_{0,1}\rangle$ being Eve's ancillary states after the interaction; these are generally non-orthogonal and un-normalized. There are two points worth noting here; firstly, the Stinespring dilation theorem allows us to limit our consideration of Eve's ancillae to a four dimensional quantum system or two qubits. Secondly, the interaction with respect to Alice's X basis $\{|+\rangle, |-\rangle\}$ is automatically determined using linearity. In both bases, the attack can compactly be expressed by

$$U|a\rangle|E\rangle = |a\rangle|F_a\rangle + |a^\perp\rangle|D_a\rangle, \tag{42}$$

where $|a\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and $\langle a|a^\perp\rangle = 0$. In particular, the relation between Eve's states in the two bases is given by

$$\begin{aligned} 2\,|F_\pm\rangle &= |F_0\rangle + |F_1\rangle \pm |D_0\rangle \pm |D_1\rangle \\ 2\,|D_\pm\rangle &= |F_0\rangle - |F_1\rangle \mp |D_0\rangle \pm |D_1\rangle\,. \end{aligned} \tag{43}$$

In this formalism it is easy to write an optimal collective attack which is able to saturate the minimum QBER associated with the security of the BB84 protocol. This collective attack was shown in Ref. [125], building on the individual symmetric attack described in Ref. [126, 127]. Assume that the unitary U is such that Eve's un-normalized states are orthogonal of the following form (in Eve's two-qubit computational basis)

$$\begin{aligned} |F_0\rangle &= \left(\ \sqrt{F},\ 0,\ 0,\ 0\ \right)^T \\ |F_1\rangle &= \left(\ \sqrt{F}\cos x,\ 0,\ 0,\ \sqrt{F}\sin x\ \right)^T \\ |D_0\rangle &= \left(\ 0,\ \sqrt{D},\ 0,\ 0\ \right)^T \\ |D_1\rangle &= \left(\ 0,\ \sqrt{D}\cos y,\ \sqrt{D}\sin y,\ 0\ \right)^T. \end{aligned} \tag{44}$$

where x, y are two arbitrary angles, $F = 1 - D$ and

$$D = \frac{1-\cos x}{2-\cos x+\cos y}. \tag{45}$$

This choice is such that $\langle F_a\,|F_a\rangle = F$, $\langle D_a\,|D_a\rangle = D$, $\langle F_a\,|F_{a^\perp}\rangle = F\cos x$, $\langle D_a\,|D_{a^\perp}\rangle = D\cos y$ and all the other inner products are zero, i.e., we have $\langle F_a\,|D_a\rangle = 0$ and $\langle F_a\,|D_{a^\perp}\rangle = 0$. We can see that the attack acts symmetrically in the two bases. Combining this choice with Eq. (42), it is easy to see that the term F represents the fidelity (probability of Bob getting the same state $|a\rangle$ sent by Alice), while D is the QBER, i.e., the probability that Bob finds the state $\left|a^\perp\right\rangle$ instead of $|a\rangle$. In fact, from the conditional total output state $\rho_{BE|a} := U\,|a\rangle\,\langle a|\otimes|E\rangle\,\langle E|\,U^\dagger$ one can check that Bob's conditional state

$$\begin{aligned} \rho_{B|a} &:= \mathrm{Tr}_E\left(\rho_{BE|a}\right) \\ &= F^{-1}\,\langle F_a|\,\rho_{BE|a}\,|F_a\rangle + D^{-1}\,\langle D_a|\,\rho_{BE|a}\,|D_a\rangle \end{aligned} \tag{46}$$

is given by

$$\rho_{B|a} = F\,|a\rangle\,\langle a| + D\left|a^\perp\right\rangle\left\langle a^\perp\right|, \tag{47}$$

while Eve's conditional output state is given by

$$\rho_{E|a} = |F_a\rangle\,\langle F_a| + |D_a\rangle\,\langle D_a|\,. \tag{48}$$

From Eq. (47) we can easily see that Alice and Bob's mutual information is equal to $I_{AB} = [1 - H_2(D)]/2$ where the factor $1/2$ accounts for the basis reconciliation (sifting) and H_2 is the binary Shannon entropy.

Let us compute the performance of this attack assuming it is an individual (delayed-choice) attack [126, 127]. Eve can store the ancilla in a memory in order to wait for the basis reconciliation. She can then keep the same instances of Alice and Bob and make individual measurements on her ancillas. Eve can first measure $\rho_{E|a}$ to distinguish between the orthogonal sets $\{|F_a\rangle\}$ and $\{|D_a\rangle\}$ and then she can perform a further measurement to distinguish between the non-orthogonal states $|F_a\rangle$ and $|F_{a^\perp}\rangle$ or between the other non-orthogonal states $|D_a\rangle$ and $|D_{a^\perp}\rangle$. Because two states with overlap $\cos x$ can be distinguish with probability $(1+\sin x)/2$ [128], we have that Eve guesses the correct state up to an error

$$p_{\mathrm{Eve}} = F\left(\frac{1+\sin x}{2}\right) + D\left(\frac{1+\sin y}{2}\right)\ . \tag{49}$$

At fixed QBER D, this probability is minimized by the choice $x = y$, so that Eve's attack is reduced to just one parameter x. In this case, we can write $D = (1-\cos x)/2$ and the following expression of Alice and Eve's mutual information

$$I_{AE} = \left[1 - H_2\left(\tfrac{1+\sin x}{2}\right)\right]/2\ . \tag{50}$$

By imposing the condition $I_{AB} = I_{AE}$, one finds the following threshold value for the QBER [126, 127]

$$D = \frac{1-1/\sqrt{2}}{2} \simeq 14.6\%\ . \tag{51}$$

Let us now consider a collective version of this attack [125], where Eve is not limited to individual measurements on her ancillas, but she is allowed to perform an optimal coherent measurement on all of them. Her accessible information is therefore upper bounded by her Holevo information χ_{AE} on Alice's variable. Due to the symmetry of the attack in the two bases, without losing generality we can assume that the sifted instances are all coming from the Z basis, i.e., $a \in \{0, 1\}$. With respect to the sifted data, Eve's Holevo bound is given by

$$\chi_{AE} = S(\rho_E) - \frac{S(\rho_{E|a}) + S(\rho_{E|a^\perp})}{2}\ , \tag{52}$$

where S is the von Neumann entropy, and $\rho_E := (\rho_{E|a} + \rho_{E|a^\perp})/2$ is Eve's average output state. Setting $x = y$, one can compute $\chi_{AE} = H_2(D)$. Including the sifting $1/2$ factor and computing the rate $R = I_{AB} - \chi_{AE}$ (bits per use), we get [125]

$$R_{\mathrm{BB84}} = [1 - 2H_2(D)]/2\ , \tag{53}$$

which corresponds to the unconditionally-secure key-rate of the BB84 protocol [97] with a threshold QBER of $D \simeq 11\%$. Thus, the collective symmetric attack is an optimal eavesdropping strategy against the BB84 protocol. It is optimal in the sense that it provides the lowest security threshold for the protocol.

5. *Unconditional security of the BB84 protocol*

This security threshold value of 11% is the same as the one that is found by assuming the most general 'coherent attack' against the protocol, where all the signal states undergo a joint unitary interaction together with Eve's ancillae, and the latter are jointly measured at the end of protocol. In this general case, the unconditional security of the BB84 protocol was provided by Shor and Preskill [97]. The main idea was based on the reduction of a QKD protocol into an entanglement distillation protocol (EDP). Given a set of non-maximally entangled pairs, the EDP is a procedure to *distill* a smaller number of entangled pairs with a higher degree of entanglement using only local operations and classical communication (LOCC). In some ways, employing this for a security proof for QKD actually makes perfect sense as it involves the two parties ending with a number of maximally entangled pairs. Given the monogamous nature of entanglement, no third party can be privy to any results of subsequent measurements the two make.

In particular, Shor and Preskill [97] showed that EDP can be done using quantum error correction codes, namely the Calderbank-Shor-Steane (CSS) code [129–131] which has the interesting property which decouples phase errors from bit errors. This allows for corrections to be made independently. In this way, one can show that the key generation rate becomes

$$R_{\mathrm{BB84}} = \left[1 - H_2(e_b) - H_2(e_p)\right]/2, \tag{54}$$

where e_b and e_p are bit and phase error rates. For $e_b = e_p = D$, this results in the same formula of Eq. (53) and it is simple to see that $R = 0$ for QBER $D \approx 11\%$.

It is important to say that a more refined analysis of the secret key rate of the BB84 protocol should account for other imperfections, such as the finite efficiency of EC and the probability Q that Alice's (single-photon) pulses are effectively detected by Bob. Thus, one has the rate

$$R_{\mathrm{BB84}} = \frac{Q}{2}\left[1 - H_2(D) - \mathrm{leak}_{\mathrm{EC}}(D)\right], \tag{55}$$

where $\mathrm{leak}_{\mathrm{EC}}(D) = f(D)H_2(D)$ is the leakage of information due to EC, with $f(D) \geq 1$ being the EC efficiency. It is interesting to derive the optimal scaling of the BB84 protocol, by setting $E = 0$ in Eq. (55) and noticing that $Q = \eta$, so that we get

$$R^{\mathrm{ideal}}_{\mathrm{BB84}} = \frac{\eta}{2}. \tag{56}$$

In conclusion, it is worth to mention the 'efficient' version of the BB84 protocol, where the sifting factor 1/2 can be eliminated from the rate [132]. The idea is to make a bias used of the bases so that, e.g., the Z basis is chosen with probability p and the X basis with probability $1-p$. Instead of the standard choice of $p = 1/2$, one can adopt a very asymmetric choice, so that $p \to 1^-$, meaning that the parties almost always use the Z basis. In the limit of large number of uses $n \to \infty$, the scheme turns out to be unconditionally secure, even though the exact choice $p = 0$ would make it completely insecure at any n. Therefore, the secret key rate of the efficient BB84 protocol is given by

$$R_{\text{eff-BB84}} = 1 - 2H_2(D). \tag{57}$$

Accounting for imperfections, it becomes the double of Eq. (55), and it leads to the ideal scaling $R^{\mathrm{ideal}}_{\text{eff-BB84}} = \eta$.

6. *Six-state protocol*

The BB84 protocol has also been extended to use six states in three bases to enhance the key generation rate and the tolerance to noise [133]. The 6-state protocol is identical to BB84 except, as its name implies, rather than using two or four states, it uses six states on three bases X, Y and Z. This creates an obstacle to the eavesdropper who has to guess the right basis from among three possibilities rather than just two of the BB84. This extra choice causes the eavesdropper to produce a higher rate of error, for example, 1/3 when attacking all qubits with a simple intercept-resend strategy, thus becoming easier to detect. The unconditional key rate against coherent attacks has the following expression in terms of the QBER D (including the sifting factor 1/3)

$$R_{\mathrm{6state}} = \frac{1}{3}\left[1 + \frac{3D}{2}\log_2\frac{D}{2} + \left(1 - \frac{3D}{2}\right)\log_2\left(1 - \frac{3D}{2}\right)\right], \tag{58}$$

which gives a security threshold value of about 12.6%, slightly improving that of the BB84 protocol [133–135]. An optimal attack achieving this rate is again provided by a symmetric collective attack [125].

Before moving on, it is worth noting that the symmetric attacks described in both the BB84 protocol as well as the 6-state protocol are equivalent to the action of quantum cloning machines (QCMs) [136]. Notwithstanding the no-cloning theorem, QCMs imperfectly clone a quantum state, producing a number of copies, not necessarily of equal fidelity. QCMs which result in copies that have the same fidelity are referred to as symmetric. In the case of the BB84, the states of interest come from only 2 MUBs, hence the relevant QCM would be the *phase covariant* QCM which clones all the states of the equator defined by two MUBs (the term 'phase covariant' comes

from the original formulation of the QCM cloning states of the form $(|0\rangle + e^{i\phi}|1\rangle)/\sqrt{2}$ independently of ϕ [137]; this QCM thus copies equally well the states from the X and Y bases). As for the 6-state protocol, the relevant QCM is universal, meaning that it imperfectly clones all states from 3 MUBs with the same fidelity.

7. *B92 protocol*

In 1992, Charles Bennett proposed what is arguably the simplest protocol of QKD, the "B92" [113]. It uses only two states to distribute a secret key between the remote parties. This is the bare minimum required to transmit one bit of a cryptographic key. More precisely, in the B92 protocol, Alice prepares a qubit in one of two quantum states, $|\psi_0\rangle$ and $|\psi_1\rangle$, to which she associates the bit values 0 and 1, respectively. The state is sent to Bob, who measures it in a suitable basis, to retrieve Alice's bit. If the states $|\psi_0\rangle$, $|\psi_1\rangle$ were orthogonal, it is always possible for Bob to deterministically recover the bit. For instance, if $|\psi_0\rangle = |0\rangle$ and $|\psi_1\rangle = |1\rangle$, Bob can measure the incoming states in the Z basis and recover the information with 100% probability.

However, Bob's ability to retrieve the information without any ambiguity also implies that Eve can do it too. She will measure the states midway between Alice and Bob, deterministically retrieve the information, prepare new states identical to the measured ones, and forward them to Bob, who will never notice any difference from the states sent by Alice. Orthogonal states are much alike classical ones, that can be deterministically measured, copied and cloned. Technically, the orthogonal states are eigenstates of some common observable, thus measurements made using that observable would not be subjected to any uncertainty. The no-cloning theorem [28, 29] does not apply to this case.

By contrast, measurements will be bounded by inherent uncertainties if Alice encodes the information in two non-orthogonal states, for example the following ones:

$$|\psi_0\rangle = |0\rangle, \quad |\psi_1\rangle = |+\rangle, \quad \langle\psi_0|\psi_1\rangle = s \neq 0. \tag{59}$$

As Bennett showed in his seminal paper [113], any two non-orthogonal states, even mixed, spanning disjoint subspaces of the Hilbert space can be used. In the actual case, the scalar product s is optimized to give the best performance of the protocol. For the states in Eq. (59), this parameter is fixed and amounts to $1/\sqrt{2}$; i.e. the states are derived from bases which are mutually unbiased one to the other. Given the complementary nature of the observables involved in distinguishing between these states, neither Bob nor Eve can measure or copy the states sent by Alice with a 100% success probability. However, while Alice and Bob can easily overcome this problem (as described in the following) and distil a common bit from the data, Eve is left with an unsurmountable obstacle, upon which the whole security of the B92 protocol is based.

In B92, Bob's decoding is peculiar and worth describing. It is a simple example of "unambiguous state discrimination" (USD) [138, 139]. To explain it, it is useful to remember that the state $|0\rangle$ ($|+\rangle$) is a Z (X) eigenstate and that $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, as it is easy to verify from Eqs. (15), (17) and (18). Suppose first that Alice prepares the input state $|\psi_0\rangle = |0\rangle$. When Bob measures it in the Z basis, he will obtain $|0\rangle$ with probability 100% whereas when he measures it in the X basis, he will obtain either $|+\rangle$ or $|-\rangle$ with probability 50%. In particular, there is one state that Bob will never obtain, which is $|1\rangle$. Now suppose that Alice prepares the other state of B92, i.e., $|\psi_1\rangle = |+\rangle$. Bob will still measure in the same bases as before but in this case, if we repeat the previous argument, we conclude that Bob can never obtain the state $|-\rangle$ as a result. See Table III for a schematic representation of Bob's outcomes and their probabilities (P) depending on Alice's encoding state and Bob's chosen basis for measurement:

Alice	Bob (Z)	Bob (X)
$\|0\rangle$	$\|0\rangle$, P = 1	$\|+\rangle$, P = 1/2
	$\|1\rangle$, P = 0	$\|-\rangle$, P = 1/2
$\|+\rangle$	$\|0\rangle$, P = 1/2	$\|+\rangle$, P = 1
	$\|1\rangle$, P = 1/2	$\|-\rangle$, P = 0

TABLE III.

From Table III it is clear that, for the conditional probability $P(a|b)$ of guessing Alice's encoding a given Bob's outcome b, we may write

$$\mathrm{P}(+|1) = \mathrm{P}(0|-) = 1. \tag{60}$$

In other words, Bob can logically infer that when he detects $|1\rangle$, Alice must have prepared the state $|+\rangle$, so he decodes the bit as '1', whereas when he detects $|-\rangle$, Alice must have prepared the state $|0\rangle$ so he decodes the bit as '0'. Whenever he detects any other state, Bob is unsure of Alice's preparation and the users decide to simply discard these "inconclusive" events from their records.

This way, using this sort of "reversed decoding", which is typical of USD, and his collaboration with Alice, Bob manages to decode the information encoded by Alice. Despite the fact that USD can also be used by Eve, the unconditional security of the B92 protocol was rigorously proven in [140] for a lossless scenario and then extended to a lossy, more realistic, case in [141], under the assumption of single photons prepared by Alice. This assumption is not necessary in the B92 version with a strong reference pulse, which has been proven secure in [142]. Remarkably, this particular scheme has been shown to scale linearly with the channel transmission at long distance, a desirable feature in QKD. Two interesting variants of this scheme appeared in [143] and [144], which allow for a much simpler implementation.

The performance of the B92 protocol is not as good as that of BB84. The presence of non-orthogonal but lin-

early independent states makes it possible for the eavesdropper to execute a good USD measurement on the quantum states prepared by Alice. This makes the B92 very loss dependent and reduces its tolerance to noise from a depolarizing channel [1] to about 3.34% [140]. This value is much smaller than the one pertaining to the BB84 protocol, which is 16.5% [97] (it should be stressed here that these values refer to the depolarizing parameter p of a depolarizing channel acting on a state ρ as $(1-p)\rho + p/3\sum_{i=x,y,z}\sigma_i\rho\sigma_i$ with Pauli operators σ_i).

However, it was recently shown that the B92 protocol can be made loss-tolerant if Alice prepares a pair of uninformative states in addition to the usual B92 states, while leaving Bob's setup unchanged [145]. This is due to the fact that the two extra states make the B92 states linearly dependent, thus preventing the possibility of a USD measurement by Eve. The existence of the uninformative states paved the way to a device-independent entanglement-based description of the B92 protocol [146], which was not previously available. In this description, Eve herself can prepare a non-maximally entangled state and distribute it to Alice and Bob. By measuring in suitable bases, Alice and Bob can test the violation of the Clauser-Horne inequality [147], a special form of Bell inequality, thus guaranteeing the security of the protocol from any attack allowed by quantum mechanics, irrespective of the detailed description of the hardware. Despite the radically different security proof used [148], the tolerance to the noise from a depolarizing channel was found to be 3.36%, remarkably close to the value of the standard prepare-and-measure B92 protocol.

Before concluding, it is worth mentioning that both the prepare-and-measure B92 [113] and the entanglement-based B92 [146] have a clear advantage in the implementation, as experimentally shown in [149]. The asymmetry of the B92 states allows for an automatic feedback that can keep distant systems aligned without employing ad-hoc resources at no extra cost for the key length.

C. Practical imperfections and countermeasures

1. *Realistic devices and photon number splitting attacks*

DV-QKD protocols are ideally defined on qubits (or qudits) for which the basic security proofs apply. Even though current technology is able to produce very good single-photon sources [150–153] encoding a single qubit per run, these sources are not widely available yet. Cheaper and more practical sources have some probability to emit multiple photons with identical encodings in a given run of the QKD protocol. As a matter of fact, the most typical QKD source is an attenuated laser which generates a coherent state $\left||\alpha|e^{i\theta}\right\rangle$ with mean photon number $\mu = |\alpha|^2$ and randomized phase θ. Each emitted pulse is therefore described by the state

$$\rho_\mu = \sum_{n=0}^{\infty} P_\mu(n)\left|n\right\rangle, \quad P_\mu(n) = \frac{\mu^n e^{-\mu}}{n!}, \tag{61}$$

where $|n\rangle$ is a number state and $P_\mu(n)$ is the Poisson distribution. On Bob's side the receiver is typically a threshold detector making a click or not, but unable to distinguish the number of photons in the incoming signal.

In this scenario, the eavesdropper may perform a photon number splitting (PNS) attack [154–156]. The essential idea is that Eve can perform a quantum non-demolition measurement (QND) to determine the number of photons in each pulse and, when this is greater than 1, she could steal one (or more) of the excess photons while forwarding the others to Bob. More precisely, the (ideal) QND measurement projects the state onto subspaces described by the total photon number without perturbing the polarization of the photons (where the encoding is typically performed).

Indeed the process of extracting photons from a pulse may preserve the polarization of the photons if this achieved by a suitable Jaynes-Cummings interaction [155, 156]. In this way, Bob's detector would not be able to detect Eve's presence while she waits for Alice's basis revelation to make sharp measurements of the stolen photons and obtain perfect information on the encoding from the multi-photon runs. The single-photon pulse can still be attacked using the ancillary assisted attack strategy described earlier. While the PNS attack may decrease the secure key generation rate drastically, the decoy state method and the SARG04 protocol are possible approaches to solve these issues.

2. *From GLLP to decoy states*

As we have seen in the previous section, practical implementations of DV-QKD include multi-photon pulses which are particularly detrimental to security, especially when Bob's detector cannot resolve the number of photons in the incoming pulses. In the presence of realistic devices (weak coherent state source as in Eq. (61) and a threshold detector), Alice and Bob can still extract a secret key if they are able to extrapolate some information on the fraction of single-photon pulses. From parameter estimation, the parties can certainly extract the "gain" of the protocol Q_μ, which is the success probability that Bob's detector clicks when triggered by Alice's pulse, and the QBER E_μ, which is the overall error affecting this detection. From the Poisson distribution $P_\mu(n)$ of Eq. (61), they can also estimate the fraction Ω of Bob's detection events corresponding to single-photon pulses emitted by Alice. In fact, they can use

$$1 - \Omega = Q_\mu^{-1} \sum_{n>1} P_\mu(n), \tag{62}$$

which implicitly assumes the worst-case scenario that all the multi-photon pulses generated by Alice's source will be detected by Bob's detector. Note that ΩQ_μ represents a lower bound for the probability Q_1 that Bob's detector clicks when Alice sends a single-photon state, and $E_\mu\Omega^{-1}$

represents an upper bound for the QBER e_1 associated to the detection of the single-photon pulses.

With this information in hand, the parties can apply EC to their entire output data (generated from both single- and multi-photon pulses) sacrificing $Q_\mu f(E_\mu)H_2(E_\mu)$ bits per use, where $f(x) \geq 1$ is the EC efficiency (with ideal value 1). Then, they can perform PA over the corrected data but at the rate which corresponds to the fraction Ω of the single-photon pulses. In fact, because PA is a linear operation, the resulting key K coming from the entire corrected data is a bitwise XOR of two keys, the one K_1 coming from single-photon pulses and the one $K_{>1}$ deriving from multi-photon pulses. At the rate considered, K_1 becomes private and random, so that $K_1 \oplus K_{>1}$ is still private and random, no matter if $K_{>1}$ remains unsecure. This gives a contribution $\Omega Q_\mu[1 - H_2(E_\mu \Omega^{-1})]$ to the rate. Thus, including the sifting factor 1/2 we can write the following unconditionally-secure rate for the realistic BB84 protocol

$$R^{\text{re}}_{\text{BB84}} = \frac{Q_\mu}{2}\left\{\Omega[1 - H_2(E_\mu \Omega^{-1})] - f(E_\mu)H_2(E_\mu)\right\}, \tag{63}$$

due to Gottesman-Lo-Lütkenhaus-Preskill (GLLP) [157]. The GLLP approach is also known as 'tagging' argument.

This rate can be improved if we can improve the bound on Ω with respect to Eq. (62). Let us start by assuming the extra condition (later removed) that Alice measures the photon numbers generated by her weak coherent state source, so that she can distinguish between single- and multi-photon pulses. Thanks to this extra assumption and the step of parameter estimation, the parties would exactly know the probability Q_1 that Alice's single-photon pulse are detected by Bob, and also the specific QBER e_1 associated to their detection. Correspondingly, the PA would be performed at the exact rate of the single-photon pulses and would give a contribution equal to $Q_1[1 - H_2(e_1)]$. As a result, we would have the improved rate [158]

$$R^{\text{re}}_{\text{BB84}} = \frac{1}{2}\left\{Q_1[1 - H_2(e_1)] - Q_\mu f(E_\mu)H_2(E_\mu)\right\}. \tag{64}$$

The rate in Eq. (64) is still achievable if we remove the extra measurement on Alice's source but we allow Alice to use decoy states. In principle these states allow the parties to estimate Q_1 and e_1 with arbitrary precision and therefore repeat the process above. Before describing this method, it is better to rigorously define some of the quantities involved. Let us start by defining the yield Y_n of an n-photon state $|n\rangle$ as the conditional probability that Bob's detector clicks given that Alice sends $|n\rangle$. Then, we define the gain Q_n of an n-photon state as $Q_n = Y_n P_\mu(n)$, which is the joint probability that Alice sends $|n\rangle$ [according to the Poisson distribution of Eq. (61)] and Bob's detector clicks. Let us also define the QBER e_n of an n-photon state as a detection error in Bob's detector given that Alice sends $|n\rangle$. With these basic definitions in hand, we can then rigorously define the overall gain (probability of a click) as

$$Q_\mu := \sum_{n=0}^{\infty} Q_n = \sum_{n=0}^{\infty} Y_n \frac{\mu^n e^{-\mu}}{n!}, \tag{65}$$

and the overall QBER as

$$E_\mu := \frac{1}{Q_\mu}\sum_{n=0}^{\infty} e_n Q_n = \frac{1}{Q_\mu}\sum_{n=0}^{\infty} e_n Y_n \frac{\mu^n e^{-\mu}}{n!}. \tag{66}$$

In a realistic QKD setup (based on weak coherent state source and a threshold detector) only the overall quantities Q_μ and E_μ can be estimated, not the individual terms Y_n and e_n in Eqs. (65) and (66). Therefore Y_1 (Q_1) and e_1 would not be directly accessible. However, if Alice uses different values of the light intensity μ, then Eq. (65) becomes a system of linear equations with the solution set $\{Y_0, Y_1, ...\}$, and Eq. (66) becomes another system of linear equations providing the solution set $\{e_0, e_1, ...\}$. Therefore, Alice could send pulses to Bob from a weak coherent state source whose intensity is randomly changed between different values. Only one intensity μ is preferred for the key bits while the other intensities $\{\nu, \nu', \ldots\}$ would be used to generate the decoy states needed for the estimation of the parameters Y_1 (Q_1) and e_1. As these would be done randomly, Eve would not know which photons would be used for key purposes and which were the decoys. As a matter of fact, the underlying assumption of the decoy state technique is that $Y_n(\text{decoy}) = Y_n(\text{signal})$ and $e_n(\text{decoy}) = e_n(\text{signal})$.

All seems well except for the fact that the value of n in Eqs. (65) and (66) runs from 0 to infinity. This literally means that to have an exact value for Y_1 (Q_1) and e_1, Alice should in principle use an infinite number of intensities for the decoy states. For the infinite decoy state case, the computation of these parameters is perfect and the rate is given by Eq. (64), i.e., we may write [159]

$$R^{\infty\text{-dec}}_{\text{BB84}} = \frac{1}{2}\left\{Q_1[1 - H_2(e_1)] - Q_\mu f(E_\mu)H_2(E_\mu)\right\}. \tag{67}$$

However, it is easy to see that the higher order terms in Eqs. (65) and (66) converge quickly to zero due to the factorial $n!$ at denominator. For this reason, just a few intensities are already sufficient to provide a good estimation of the parameters, so that Alice and Bob can find good bounds $e_1 \leq e_1^{\text{UB}}$ and $Y_1 \geq Y_1^{\text{LB}}$ ($Q_1 \geq Q_1^{\text{LB}}$) to be used in Eq. (64), so that we may write

$$R^{\text{dec}}_{\text{BB84}} = \frac{1}{2}\left\{Q_1^{\text{LB}}[1 - H_2(e_1^{\text{UB}})] - Q_\mu f(E_\mu)H_2(E_\mu)\right\}, \tag{68}$$

which becomes

$$R^{\text{dec}}_{\text{eff-BB84}} = 2R^{\text{dec}}_{\text{BB84}} \tag{69}$$

in the case of the efficient BB84 protocol [132].

It is important to note that the use of decoy states has also an impact in terms of rescaling the effective rate

expressed as secret bits per channel use (or pulse). Let us call $p_{\rm sig}$ ($p_{\rm dec}$) the probability to choose a signal (decoy) state. For large number of uses n, the key rate should be rescaled as $R \to p_{\rm sig}R/(p_{\rm sig}+p_{\rm dec})$. If we use a finite number of decoy intensities $\{\nu_1, \nu_2, \ldots, \nu_N\}$, it is easy to set $p_{\rm dec} \ll p_{\rm sig}$, so that the rate is not affected by any rescaling. However, in the case of an infinite number of decoy intensities, the situation is less clear. Call $p(\nu_i)$ the probability of selecting the decoy intensity ν_i. In order to have a non-zero effective rate, one should impose the joint limit $N \to \infty$ and $p(\nu_i) \to 0$ such that $p_{\rm dec} = N\sum_i p(\nu_i)$ is finite and small with respect to $p_{\rm sig}$. For this reason, it is clear that the infinite decoy state case is only a theoretical extrapolation which only serves to clarify the optimal achievable rate.

The ultimate ideal rate (bits per channel use) achievable by decoy-state BB84 can be easily derived from Eq. (67). Assuming zero QBER $E_\mu = e_1 = 0$, we get $R_{\rm BB84}^{\rm dec\text{-}opt} = Q_1/2$, where $Q_1 = Y_1\mu e^{-\mu}$ and $Y_1 = \eta + (1-\eta)Y_0$. Here Y_0 is the dark count rate and η is the transmissivity of the channel coupled with a unit-efficiency threshold detector, so that it corresponds to the probability of successfully detecting a single-photon pulse. Assuming zero dark counts ($Y_0 = 0$) and adopting the optimal choice $\mu = 1$, one finds

$$R_{\rm BB84}^{\rm dec\text{-}opt} = \eta/(2e). \tag{70}$$

Of course this rate can be further improved if one considers the efficient BB84 protocol [132] with infinite decoy intensities, which doubles the rate, so that

$$R_{\rm eff\text{-}BB84}^{\rm dec\text{-}opt} = 2R_{\rm BB84}^{\rm dec\text{-}opt} = \eta/e. \tag{71}$$

Historically, the technique of decoy states was first introduced in Ref. [160]. It was shown to be practically useful in Ref. [161], where the method was studied assuming three different intensities under finite-size effects (see also Ref. [162]) and also developed in Refs. [159, 163], which studied both the performance with infinite decoys and the practical case of two-decoy states. The important security aspect of the statistical fluctuation/estimation of the decoy intensities has been also addressed in the literature [164, 165]. The technique of decoy states has enabled DV-QKD to be executed over distances beyond a hundred kilometers despite the imperfections in implementation. For other reviews on decoy states, the reader may take a look at Ref. [158] and Ref. [166, Sec. 4.3].

3. SARG04 protocol

While the decoy state technique mitigates the problem of PNS attacks by introducing new elements to the BB84 protocol, a different approach was introduced in 2004 by Scarani, Acin, Ribordy, and Gisin, "SARG04" [167], a variant of the BB84 protocol at the classical communication stage. The PNS attack thrives on the information revealed regarding the basis. Thus, a natural way against such an attack would be to discount such an element from the protocol. The SARG04 protocol shares the first step of photon transmission with BB84: Alice sends one of four states selected randomly from 2 MUBs, Z or X, and Bob performs a measurement with the two bases. In the second step however, when Alice and Bob determine for which bits their bases matched, Alice does not directly announce her bases but a pair of non-orthogonal states, one of which being used to encode her bit.

The decoding is similar to that of the B92 protocol; it is a procedure of USD between states in the announced pair. For example, assume Alice transmits $|0\rangle$ and Bob measures it with the basis X. Alice would announce the set $\{|0\rangle, |+\rangle\}$. If Bob's measurement results in $|+\rangle$, then Bob cannot infer Alice's state conclusively as the output $|+\rangle$ could have resulted from either $|0\rangle$ or $|+\rangle$ as input. In such a case, the particular run would be discarded. If the result was $|-\rangle$ instead, then it is stored for post processing because it could have only resulted from the measurement of the $|0\rangle$ state. Since the two states in a set are non-orthogonal, the PNS attack cannot provide Eve with perfect information on the encoded bit.

The SARG04 protocol has been shown to be secure up to QBER values of 9.68% and 2.71% for single photon and double photon pulses respectively [168] using the EDP type proof. It is worth noting that similar modification to the classical phase of the six state protocol can be done to give a 'six-state SARG04' where key bits can be derived from even 4 photon pulse. This is secure for QBER values of $11.2\%, 5.60\%, 2.37\%$ and 0.788% for $1, 2, 3$ and 4 photon pulses respectively. See also the recent analysis in Ref. [169].

D. Entanglement-based QKD

1. E91 protocol

In 1991, Artur Ekert developed a new approach to QKD by introducing the E91 protocol [114]. The security of the protocol is guaranteed by a Bell-like test to rule out Eve. The E91 considers a scenario where there is a single source that emits pairs of entangled particles, each described by a Bell state, in particular the singlet state $|\Psi\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. The twin particles could be polarized photons, which are then separated and sent to Alice and Bob, each getting one half of each pair. The received particles are measured by Alice and Bob by choosing a random basis, out of three possible bases. These bases are chosen in accordance to a Clauser, Horne, Shimony and Holt (CHSH) test [170]. Explicitly, the angles chosen by Alice are

$$a_1 = 0, \quad a_2 = \pi/4, \quad a_3 = \pi/2, \tag{72}$$

corresponding to the bases Z, $(X+Z)/\sqrt{2}$ and X, respectively. Bob's on the other hand chooses

$$b_1 = \pi/4, \quad b_2 = \pi/2, \quad b_3 = 3\pi/4, \tag{73}$$

corresponding to $(X+Z)/\sqrt{2}$, X and $(X-Z)/\sqrt{2}$.

As in BB84, they would discuss in the clear which bases they used for their measurements. Alice and Bob use the instances where they chose different basis to check the presence of Eve. By disclosing the data related to these instances they check the violation of the CHSH quantity

$$E = \langle a_1 b_1 \rangle - \langle a_1 b_3 \rangle + \langle a_3 b_1 \rangle + \langle a_3 b_3 \rangle \tag{74}$$

where $\langle a_i b_j \rangle$ represents the expectation value when Alice measures using a_i and Bob uses b_j. If the inequality $-2 \leq E \leq 2$ holds, it would indicate either that the received photons are not truly entangled (which could be due to an attempt to eavesdrop) or that there is some problem with the measurement device. By contrast, if everything works perfectly and there is no eavesdropper, Alice and Bob expected value of E is the maximal violation $-2\sqrt{2}$. One way of looking at it is by writing the state of entangled photons subjected to a depolarizing channel [1], resulting into the isotropic mixed state

$$\rho_\Psi = p|\Psi\rangle\langle\Psi| + (1-p)\mathbb{1}_4/4, \tag{75}$$

with probability p. It can be shown that the CHSH test has maximal violation $-2\sqrt{2}$ provided that $p = 1$, i.e., for an unperturbed 'Eve-less' channel.

In the case of maximal violation of the CHSH test, Alice and Bob are sure that their data is totally decoupled from any potential eavesdropper. From the instances where they chose the same bases, they therefore process their perfectly anti-correlated results into a shared private key. While QKD generally capitalizes on the no-cloning theorem and the inability of perfectly distinguishing between two non-orthogonal states, the essential feature of the E91 protocol is its use of the nonlocal feature of entangled states in quantum physics. Eve's intervention can be seen as inducing elements of physical reality which affects the non-locality of quantum mechanics.

2. *BBM92 protocol*

The BBM92 protocol [115] was, in some sense, aimed as a critic to E91's reliance on entanglement for security. Building upon E91 with a source providing each legitimate party with halves of entangled pairs, BBM92 works more efficiently by having both the legitimate parties each measure in only two differing MUBs instead of the three bases of E91. The two MUBs can be chosen to be the same as that of BB84. By publicly declaring the bases, Alice and Bob select the instances where they chose the same basis to obtain correlated measurement results, from which a secret key can be distilled. A sample is then disclosed publicly to check for errors and evaluate the amount of eavesdropped information.

The idea is that Eve cannot become entangled to Alice's and Bob's qubits while not causing any error in their measurements. This points out to the claim that there is no need for the legitimate parties to commit to a Bell test. The similarity between BBM92 and BB84 is obvious. If Alice possesses the source, her measurement (in a random basis) would prepare the state to be sent to Bob in one of the 4 possible BB84 states. Hence, without a Bell test, we are essentially left with BB84. There is no way of telling whether Alice started off by measuring part of a Bell state or by preparing a qubit state using a random number generator. This observation is at the basis of the entanglement-based representation of prepare and measure protocols, which is a powerful theoretical tool in order to prove the security of QKD protocols.

Using or not entangled pairs in a QKD protocol is non-consequential in the context of standard eavesdropping on the main communication channel. However, it is also important to note that a protocol with a Bell test provides a higher level of security in the sense that it reduces the number of assumptions to be made on the local devices. This makes way for the most pessimistic security definition, i.e., device-independent security, a topic to be delved into later. The security analysis of entanglement-based QKD protocols is still the subject of very active research, with recent investigations and simplified proofs based on entanglement distillation protocols [171, 172].

E. Two-way quantum communication

Quantum cryptographic protocols making a bidirectional use of quantum channels started with the introduction of deterministic protocols for the purpose of secure direct communication [173–175] and later evolved into more mature schemes of two-way QKD [176, 177]. A defining feature of these protocols is that encodings are not based on preparing a quantum state but rather applying a unitary transformation, by one party (often Alice) on the traveling qubit sent by another party (Bob) in a bidirectional communication channel. The initial idea of direct communication aimed at allowing two parties to communicate a message secretly, without the need of first establishing a secret key. However the reality of noisy channels would render any such direct communication between parties invalid or very limited. For this reason, two-way protocols for direct communication were soon replaced by QKD versions, with appropriate security proofs [178].

1. *Ping pong protocol*

The ping pong direct communication protocol [173] derives its name from the to and from nature of the traveling qubits between the communicating parties in the protocol. The *ping* comes from Bob submitting to Alice half of a Bell pair he had prepared, $|\Psi_+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$,

and the *pong* is Alice's submitting of the qubit back to Bob. With probability c, Alice would measure the received qubit in the Z basis; otherwise, she would operate on it with either the identity $\mathbb{1}$ with probability p_0 or the σ_z Pauli operator with probability $1-p_0$, re-sending the qubit back to Bob. The former is the case where she could check for disturbance in the channel and is referred to as the 'control mode' (CM), while the latter is the essential encoding feature of the protocol and referred to as the 'encoding mode' (EM).

The operations in EM flip between two orthogonal Bell states as $\mathbb{1}$ retains $|\Psi_+\rangle$, while σ_z provides

$$\mathbb{1}\otimes\sigma_z|\Psi_+\rangle = |\Phi_-\rangle := (|00\rangle - |11\rangle)/\sqrt{2}. \tag{76}$$

This allows Bob to distinguish between them and infer Alice's encoding perfectly. The details of the CM is as follows: Alice measures the received qubit in the Z basis and announces her result over a public channel. Bob then measures his half of the (now disentangled) Bell pair and can determine if Eve had interacted with the traveling qubit. It should be noted that, in this protocol, Alice is not expected to resend anything to Bob in CM. See Fig. 2 for a schematic representation.

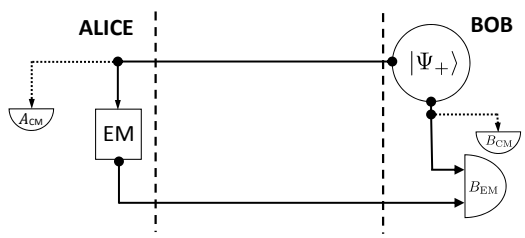

FIG. 2. A schematic of the ping pong protocol. Part of a Bell pair $|\Psi_+\rangle$ is sent by Bob to Alice, while the other part is kept. If Alice chooses the EM (solid lines), she performs either $\mathbb{1}$ or σ_z on the received qubit, which is then sent back to Bob. Finally, Bob performs a Bell detection ($B_{\rm EM}$) on the received and kept qubits. If Alice chooses the CM (dotted lines), she measures the incoming qubit in the Z basis ($A_{\rm CM}$), and informs Bob who also measures its kept qubit in the same basis ($B_{\rm CM}$).

By using the instances in CM, the parties may check the presence or not of Eve. In particular, Eve's action goes undetected only with an exponentially decreasing probability in the number of bits gained. Therefore for long enough communication, its presence is almost certainly discovered and the protocol aborted. If not present, then Alice's message is privately delivered to Bob via the EM instances with a sufficient degree of privacy. The message that Alice transmits to Bob is not subject to any form of further processing. Note that the protocol can be easily extended [179] to include all the Pauli operators plus the identity.

Unfortunately, direct private communication is very fragile and easily fails in realistic conditions where noise on the line is inevitable and, therefore, the presence of Eve must always be assumed as worst-case scenario. In particular, the ping pong protocol is also subject to a powerful denial-of-service attack [180] which can be partially mitigated if Alice returns the qubit to Bob in CM. Limitations also affect schemes of quantum direct communication in CV systems [181, 182]. Despite these difficulties, research activity is still active in this area, with some recent development [183].

2. *Two-way QKD protocols*

Two-way protocols for QKD do not need to use entanglement as in the ping pong protocol. According to Refs. [176, 177], Bob prepares a state $|a\rangle$ randomly selected from the two MUBs X and Z to be sent to Alice. In EM, Alice encodes a bit using either the identity $\mathbb{1}$ (corresponding to bit value '0') or $i\sigma_y$ (corresponding to bit value '1'), i.e.,

$$\mathbb{1}|a\rangle = |a\rangle\ ,\ i\sigma_y|a\rangle = |a^\perp\rangle \tag{77}$$

where $|a^\perp\rangle$ is the state orthogonal to $|a\rangle$. The qubit is then sent back to Bob who measures it in the same preparation basis. With some probability, Alice chooses the CM where the incoming qubit is instead measured, and another qubit is prepared and sent back to Bob for his measurement. This 'double check' was specifically introduced in Ref. [177] known as the LM05 protocol. This clearly increases the detection performance of the protocol. For instance, given an attack scenario where Eve measures the traveling qubits in either of the two MUBs Z and X, the probability of detecting her is 37.5%.

Security proofs are based on the fact that Eve is forced to attack both the forward and backward paths [184]. In general, from the CM, Alice and Bob derive the amount of noise in the channels, which determines how much PA has to be performed in the post-processing. By disclosing part of the data in EM, they can also estimate the amount of EC to be performed. Practical implementations of the protocol were already carried out as early as 2006 in Ref. [185] as well as Refs. [186–188]. We now discuss basic eavesdropping strategies.

3. *Intercept-resend strategy*

The simplest attack scheme is intercept-resend where Eve measures the traveling qubit in both channels with a basis of her choice (randomly selected between the same bases used by Bob). As she would effectively prepare the traveling qubit into her basis of choice by virtue of a projective measurement, she plays the role of Bob and would be able to ascertain Alice's encoding perfectly. In LM05, she would introduce errors 1/4 of the time in each path. This strategy leads to a security threshold of 11.9%, in terms of maximal error (detected in CM) before no key is distillable.

It is worth noting that this attack results in an asymmetry between Alice-Eve's and Bob-Eve's mutual information. While Eve attempts to estimate Alice's encoding by inferring the evolution of the state of the traveling qubit, her estimation of the result of Bob's final measurement is another matter entirely. This leads to the idea that Alice and Bob could actually consider doing a RR procedure for distilling a key, where Alice would correct her bits to guess Bob's string. In RR, the security threshold is increased to 25%.

4. Non-orthogonal attack strategies

Here Eve would attach an ancilla to the traveling qubit in the forward path and another in the backward path with the most optimal possible interaction between them to glean the maximal amount of information while minimizing the disturbance on the channel. In this way, the security threshold for LM05 is about 10% in DR, while remaining 25% in RR. A specific sub-optimal version of this attack is the DCNOT attack strategy, where Eve's ancilla is a qubit, used in the forward as well as the backward path. The unitary transformation used by Eve in both paths would be the same CNOT gate (hence the name *double CNOT attack* or DCNOT).

Let us write Alice's encoding as U which acts on a qubit in the computational basis as $U|i\rangle \to |i \oplus j\rangle$ where $\oplus$ is the addition modulo 2 operation and $i, j = 0, 1$. The action of the CNOT gates together with Alice's encoding U_A can be written as follows:

$$\mathrm{CNOT}(U_A \otimes \mathbb{1})\mathrm{CNOT}|i\rangle|0\rangle_E = |j\rangle|j \oplus i\rangle_E \tag{78}$$

where qubits with subscript E refers to Eve's ancillae. We see that Eve's qubit would record the evolution of Bob's qubit. This is not at all surprising as the CNOT gate allows for the perfect copying of states of the Z basis.

The case where Bob uses the X basis is no hindrance either to Eve. Despite the fact that a CNOT between a qubit in the X basis (as control qubit) and one in Z (for target) would entangle the qubits, a subsequent CNOT would serve to disentangle them.

$$\begin{aligned}&\mathrm{CNOT}(U_A \otimes \mathbb{1})\mathrm{CNOT}\ \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}|0\rangle_E \\ &= U_A\left(\frac{|0\rangle \pm |1\rangle}{\sqrt{2}}\right) \otimes |j\rangle_E.\end{aligned} \tag{79}$$

The attack would leave no trace of an eavesdropper in EM while she gains all the information. The attack is however very noisy and easily detectable in CM with an error rate of 25%. If Eve attacks a fraction f of the runs, then her information gain is f with an error rate of $f/4$.

5. Further considerations

A general security proof for two-way DV-QKD was reported in Ref. [178] but methods employed led to an over-pessimistic estimation of the key rate (1.7% for LM05). On the other hand, the approach of Ref. [189] based on entropic bounds does not directly apply to two-way QKD protocols based on unitary encodings. A tight security proof is therefore still very much an open problem. A number of eavesdropping strategies and technical issues have been also described in Refs. [190, 191], and the performance against lossy channels have been thoroughly studied in Refs. [192–194], where the key rate of the LM05 has been compared with that of the BB84 at the same distances.

Two-way QKD protocols were also extended to considering non-orthogonal unitaries [195–198]. For instance, the encoding unitaries $\mathbb{1}$ and the $(\mathbb{1} - i\sigma_y)/\sqrt{2}$ were considered by Ref. [199], while Ref. [197] exploited the notion of mutually unbiased unitary-operator bases [200]. Another development has been the extension of the LM05 from two to three MUBs (similar to the extension of BB84 to the six-state protocol). The improvement in security provided by the protocol known as 6DP [201] by making use of three MUBs instead of only two is expected. However the extension to include the third MUB is non-trivial given the no-go theorem which forbids the flipping of an arbitrary state selected from 3 MUBs (see also Ref. [202]). This can be seen as follows. Assume the existence of a unitary transformation U_f that flips between the orthogonal states of the Z basis, i.e., $U_f|0\rangle = -|1\rangle$ and $U_f|1\rangle = |0\rangle$. The negative phase factor in the first equation is necessary to ensure U_f also flips between the states in the X basis. However, U_f would not flip between the states in the Y basis,

$$\begin{aligned}U_f(|0\rangle + i|1\rangle)/\sqrt{2} &= (-|1\rangle + i|0\rangle)/\sqrt{2} \\ &:= (|0\rangle + i|1\rangle)/\sqrt{2}.\end{aligned} \tag{80}$$

IV. DEVICE-INDEPENDENT QKD

A. Introduction

A security proof for a QKD protocol is a mathematical theorem based on particular assumptions. These assumptions might encode that the devices work in a particular way, e.g., that Alice generates a $|0\rangle$ state and sends it to Bob, who measures in the $\{|0\rangle, |1\rangle\}$ basis. Although we have rigorous security proofs for QKD protocols, finding devices satisfying the assumptions of these proofs is difficult. Any features of the real devices not modeled in the security proof could compromise security, and there are cases where this has happened in actual implementations (e.g. [203–206]). Attacks that exploit features not modeled in the security proof are known as *side-channel attacks*.

Identified side-channel attacks can be patched sending the hacker back to the drawing board. This leads to a technological arms race between the hackers and protocol designers and a sequence of (hopefully) increasingly secure protocols. Device-independent protocols provide

a way to break out of this hack-and-patch cycle with respect to side-channel attacks on the devices. They are able to do so because they make no assumptions about how the devices used in the protocols operate in their security proofs—instead, security follows from the classical input-output behavior, which is tested in the protocol. In this way, a device independent protocol checks that the devices are functioning sufficiently well *during the protocol*. This has a second advantage: in standard QKD protocols with trusted devices, in principle a user should check the functionality of their devices regularly to ensure their behavior is still in line with the assumptions of the security proof. This is a technically challenging task and not one that can be expected of an average user. By contrast, in a device-independent protocol, no sophisticated testing is needed to detect devices that are not functioning sufficiently well (although, technical know-how is needed to fix them).

At first it may seem intuitive that this is an impossible task: how can we put any constraints on the workings of a device without probing its internal behavior? In particular, is it possible to test the input-output behavior and ensure that the outputs of a device could not have been pre-determined by its manufacturer? In fact, the intuition that this is impossible is correct if there is only one device. However, with two or more devices, this can be done, thanks to Bell's theorem. The basic idea is that if two devices are unable to communicate, are given random inputs and their input-output behavior gives rise to a distribution that violates a Bell inequality, then their outputs could not have been pre-determined and hence are a suitable starting point to generate a key. Because this idea is central to device-independence we will elaborate on it first before discussing DI-QKD protocols.

B. The link between Bell violation and unpredictability

Consider two parties, Alice and Bob, each of whom have a device. Alice and Bob are each able to make one of two inputs to their device and obtain one of two outputs. Quantum mechanically, these devices may be set up to measure halves of a pair of entangled qubits, with the inputs corresponding to the choice of basis. Crucially, although this may be what honest parties should do to set up their devices, for the security argument, no details of the setup are required. In order to describe the behavior of such devices we will use the following notation. Alice's input is modeled by a binary random variable A and Bob's by B and their respective outputs are binary random variables X and Y. It is convenient to use the following Table IV to represent the conditional distribution $P_{XY|AB}$ as a 4×4 matrix.

Suppose now that Alice and Bob's devices behave according to a particular distribution $P_{XY|AB}$ and imagine an eavesdropper holding some additional information about the devices and for ease of this exposition, let us

$P_{XY\|AB}$	B	0		1	
	Y	0	1	0	1
A	X				
0	0	$P_{00\|00}$	$P_{01\|00}$	$P_{00\|01}$	$P_{01\|01}$
	1	$P_{10\|00}$	$P_{11\|00}$	$P_{10\|01}$	$P_{10\|01}$
1	0	$P_{00\|10}$	$P_{01\|10}$	$P_{00\|11}$	$P_{01\|11}$
	1	$P_{10\|10}$	$P_{11\|10}$	$P_{10\|11}$	$P_{11\|11}$

TABLE IV.

assume that this information is classical and use the random variable Z to describe it. This classical information tells Eve additional information about what is happening. One can think of this in the following way: Eve supplies devices that behave according to $P^z_{XY|AB}$, but picks z with probability p_z such that from Alice and Bob's point of view the device behavior is the same, i.e.,

$$P_{XY|AB} = \sum_z p_z P^z_{XY|AB} \,. \tag{81}$$

If the devices are used in such a way that each device cannot access the input of the other then they must act in a local manner ($P^z_{X|AB} = P^z_{X|A}$ and $P^z_{Y|AB} = P^z_{Y|B}$). The question of interest is then whether Eve could have supplied deterministic devices giving rise to the observed distribution. This can be stated mathematically as the question whether $P_{XY|AB}$ can be written in the form (81) with $P^z_{XY|AB} = P^z_{X|A} P^z_{Y|B}$ and $P^z_{X|A=a}(x), P^z_{Y|B=b}(y) \in \{0,1\}$ for all $x, y, a, b \in \{0,1\}$. In other words, is $P_{XY|AB}$ a convex combination of the 16 local deterministic distributions

$$\left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right), \left(\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right), \ldots, \left(\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right)? \tag{82}$$

If not, then at least some of the time Eve must be sending a distribution $P^z_{XY|AB}$ to which she doesn't know either Alice's or Bob's outcome after later learning their inputs.

A Bell inequality is a relation satisfied by all local correlations (i.e., all $P_{XY|AB}$ that can be written as a convex combination of local deterministic distributions). The CHSH inequality can be expressed in this notation as $\langle C, P\rangle \leq 2$, where $P = P^z_{XY|AB}$,

$$C = \left(\begin{array}{cc|cc} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ \hline 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \end{array}\right) \tag{83}$$

and $\langle C, P\rangle = \mathrm{Tr}(C^T P)$ is the Hilbert-Schmidt inner product. Bell's theorem states that there are quantum correlations that violate this inequality. To describe these

we introduce a class of distributions parameterized in terms of $\varepsilon \in [0, 1/2]$ as follows

$$P_\varepsilon := \left(\begin{array}{cc|cc} \frac{1}{2}-\varepsilon & \varepsilon & \frac{1}{2}-\varepsilon & \varepsilon \\ \varepsilon & \frac{1}{2}-\varepsilon & \varepsilon & \frac{1}{2}-\varepsilon \\ \hline \frac{1}{2}-\varepsilon & \varepsilon & \varepsilon & \frac{1}{2}-\varepsilon \\ \varepsilon & \frac{1}{2}-\varepsilon & \frac{1}{2}-\varepsilon & \varepsilon \end{array}\right). \tag{84}$$

Define the state $|\psi_\theta\rangle := \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle$. Then assume that Alice and Bob measure the two halves of the maximally-entangled state $(|00\rangle + |11\rangle)/\sqrt{2}$ in the following bases:

$$\begin{aligned} \{|\psi_0\rangle, |\psi_\pi\rangle\} &\text{ for } A = 0, \\ \{|\psi_{\pi/2}\rangle, |\psi_{3\pi/2}\rangle\} &\text{ for } A = 1, \\ \{|\psi_{\pi/4}\rangle, |\psi_{5\pi/4}\rangle &\text{ for } B = 0, \\ \{|\psi_{3\pi/4}\rangle, |\psi_{7\pi/4}\rangle\} &\text{ for } B = 1. \end{aligned} \tag{85}$$

This gives rise to a distribution of the form P_ε as in Eq. (84) where

$$\varepsilon = \frac{1}{2}\sin^2\frac{\pi}{8} = \frac{1}{8}(2-\sqrt{2}) =: \varepsilon_{\mathrm{QM}}, \tag{86}$$

which leads to $\langle C, P_{\varepsilon_{\mathrm{QM}}}\rangle = 2\sqrt{2}$, i.e., the maximal violation of the CHSH inequality. Recall that the Tsirelson's bound [207] states that if P is quantum-correlated then $\langle C, P\rangle \leq 2\sqrt{2}$.

One way to think about how random the outcomes are is to try to decompose this distribution in such a way as to maximize the local part. For $0 \leq \varepsilon \leq 1/8$, this is achieved using the following decomposition whose optimality can be verified using a linear program

$$\begin{aligned} P_\varepsilon :=& \varepsilon \Bigg[\left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right) + \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{array}\right) + \left(\begin{array}{cc|cc} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{array}\right) \\ &+ \left(\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right) + \left(\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{array}\right) + \left(\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right) \\ &+ \left(\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right) + \left(\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right) \Bigg] \\ &+ (1-8\varepsilon) \left(\begin{array}{cc|cc} \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \hline \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \end{array}\right). \end{aligned} \tag{87}$$

If Eve used this decomposition she would be able to guess Alice's outcome with probability $8\varepsilon + \frac{1}{2}(1-8\varepsilon) = \frac{1}{2} + 4\varepsilon$. Thus, Alice's outcome would have some randomness with respect to Eve.

We note however that while the first eight terms in this decomposition are local, the last is a maximally non-local distribution [208, 209], often called a Popescu-Rohrlich (PR) box [210]. This is well-known not to be realizable in quantum theory. The stated strategy is hence not available to an eavesdropper limited by quantum mechanics. To analyze the case of a quantum-limited eavesdropper, we also have to ensure that $P^z_{XY|AB}$ is quantum-realizable for all z. It is not easy to do this in general, but in the case where A, B, X and Y are binary it can be shown that it is sufficient to consider qubits [208]. For other cases, there is a series of increasingly tight outer approximations to the quantum set that can be tested for using semidefinite programs [211].

Considering a quantum-limited eavesdropper reduces Eve's power and hence leads to more randomness in the outcomes. For a distribution of the form P_ε for $\varepsilon_{\mathrm{QM}} \leq \varepsilon \leq 1/8$, for instance, Eve can do a quantum decomposition as follows:

$$\begin{aligned} P_\varepsilon :=& \frac{\varepsilon - \varepsilon_{\mathrm{QM}}}{1-8\varepsilon_{\mathrm{QM}}} \Bigg[\left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right) + \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{array}\right) \\ &+ \left(\begin{array}{cc|cc} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{array}\right) + \left(\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right) + \left(\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{array}\right) \\ &+ \left(\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right) + \left(\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right) + \left(\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right) \Bigg] \\ &+ \frac{1-8\varepsilon}{1-8\varepsilon_{\mathrm{QM}}} P_{\varepsilon_{\mathrm{QM}}}, \end{aligned} \tag{88}$$

allowing her to predict the outcome correctly with probability $8\frac{\varepsilon-\varepsilon_{\mathrm{QM}}}{1-8\varepsilon_{\mathrm{QM}}} + \frac{1-8\varepsilon}{2(1-8\varepsilon_{\mathrm{QM}})}$.

The argument just given is intended to give an intuition to the idea of why violating a Bell inequality means that there is some randomness in the outcomes. However, knowing that there is some randomness is not enough; we also need to know how much key can be extracted from the raw data.

C. Quantitative bounds

Given a pair of uncharacterized devices we would like to know how much secure key we can extract from their outputs. Because the devices are uncharacterized, we need to test their behavior. Such a test involves repeatedly making random inputs to the devices and checking some function of the chosen inputs and the device outputs. For convenience, in this section we will mostly consider the average CHSH value. Conditioned on this test passing, the protocol will go on to extract key.

We would like a statement that says that for any strategy of Eve the probability that both the average CHSH value is high and the key extraction fails is very small. For this to be the case we need to connect the CHSH value with the amount of extractable key. Since key is shared randomness, before considering sharing we can ask how much randomness can Alice extract from her outcomes for a given CHSH value. For a cq-state (i.e., a state of the form $\rho_{AE} = \sum_{\mathbf{x}} P_{\mathbf{X}}(\mathbf{x})|\mathbf{x}\rangle\langle\mathbf{x}| \otimes \rho_E^{\mathbf{x}}$, where $\mathbf{X}$ denotes a string of many values), this can be quantified by the (smooth) min-entropy [107] $S_{\min}(\mathbf{X}|E)$ of Alice's string $\mathbf{X}$ conditioned on E.

This is a difficult quantity to evaluate, in part because of the lack of structure. In fact, Eve's behavior need not be identical on every round and she need not make measurements round by round, but can keep her information quantum. However, a simpler round-by-round analysis in which the conditional von Neumann entropy is evaluated can be elevated to give bounds against the most general adversaries via the entropy accumulation theorem (EAT) [212, 213]. The basic idea is that, provided the protocol proceeds in a sequential way, then the total min-entropy of the complete output of n rounds conditioned on E is (up to correction factors of order $\sqrt{n}$) at least n times the conditional von Neumann entropy of one round evaluated over the average CHSH value.

The evaluation of the conditional von Neumann entropy as a function of the CHSH value was done in [214]. There it was shown that for any density operator ρ_{ABE}, if the observed distribution $P_{XY|AB}$ has CHSH value $\langle C, P\rangle = \beta \in [2, 2\sqrt{2}]$, then the conditional von Neumann entropy satisfies the bound

$$S(X|E) \geq 1 - H_2\left[\frac{1}{2}\left(1 + \sqrt{(\beta/2)^2 - 1}\right)\right], \qquad (89)$$

where $H_2(...)$ is the binary Shannon entropy. Combining this with the EAT, we obtain a quantitative bound on the amount of uniform randomness that can be extracted from Alice's outcomes of roughly n times this.

The bound (89) is obtained by using various technical tricks specific to the CHSH scenario. For general non-local games/device measurements we do not know of good ways to obtain tight bounds on the conditional von Neumann entropy. Instead, a typical way to obtain a bound is to note that $S(X|E) \geq S_{\min}(X|E)$, and that $S_{\min}(X|E)$ can be bounded via a hierarchy of semidefinite programs [211, 215], as discussed in [216, 217]. However, the bounds obtained in this way are fairly loose and it is an open problem to find good ways to improve them. See also Refs. [218, 219] for some recent studies on the extractable key derived from i.i.d. device behaviors.

D. Protocols for DI-QKD

1. *The setup for DI-QKD*

As mentioned in Section IV A, use of device-independence eliminate security flaws due to inadequate modeling of devices. There are nevertheless, a number of other assumptions we make in this scenario (note that these assumptions are also made in the trusted-devices case):

1. Alice and Bob have secure laboratories and control over all channels connecting their laboratory with the outside world. (Without this assumption, the untrusted devices could simply broadcast their outputs to the adversary outside the laboratory, or Eve could send a probe into the laboratory to inspect any secret data.) For any devices in their labs, Alice and Bob can prevent unwanted information flow between it and any other devices.

2. Each party has a reliable way to perform classical information processing.

3. Alice and Bob can generate perfectly random (and private) bits within their own laboratories.

4. Alice and Bob are connected by an authenticated classical channel on which an adversary could listen without detection.

5. Alice and Bob are also connected by an insecure quantum channel on which an adversary can intercept and modify signals in any way allowed by quantum mechanics.

Security is proven in a composable way (cf. Section II D) allowing a key output by the protocol to be used in an arbitrary application. Note that because the protocol is device-independent, the prolonged security of any output relies on the devices not being reused [220] in subsequent protocols (note that the same devices can be used many times within a run of the protocol), although modified protocols to mitigate this problem have been proposed [220].

2. *The spot-checking CHSH QKD protocol*

A protocol acts as a filter. It is a procedure that can be fed by a set of devices such that bad devices lead to an "abort" with high probability, and good devices lead to success with high probability. There are many possible types of protocol; we will describe a specific protocol here, based on the CHSH game with spot-checking.

The protocol has parameters $\alpha \in (0, 1)$, $n \in \mathbb{N}$, $\beta \in (2, 2\sqrt{2}]$, $\delta \in (0, 2(\sqrt{2} - 1))$, which are to be chosen by the users before it commences. Here are the steps:

1. Alice uses a preparation device to generate an entangled pair. She keeps one half and sends the other to Bob. This step and the subsequent one refer to the generation, sending and storage of an entangled state, but for security Alice and Bob do not rely on this taking place correctly (if the state created is not of high enough quality the protocol should abort).

2. Bob stores it and reports its receipt to Alice.

3. Alice picks a random bit T_i, where $T_i = 0$ with probability $1 - \alpha$ and $T_i = 1$ with probability α. She sends T_i to Bob over the authenticated classical channel.

4. If $T_i = 0$ (corresponding to no test) then Alice and Bob each make some fixed inputs (choices of bases) into their devices, $A_i = 0$ and $B_i = 2$ and record the outcomes, X_i and Y_i. If $T_i = 1$ (corresponding to a test) then Alice and Bob each independently pick uniformly random inputs $A_i \in \{0, 1\}$ and $B_i \in \{0, 1\}$ to their devices and record the outcomes, X_i and Y_i.

5. Steps 1–4 are repeated n times, increasing i each time.

6. For all the rounds with $T_i = 1$, Bob sends his inputs and outputs to Alice who computes the average CHSH value (assigning $+1$ or -1 in accordance with the entries of matrix C). If this value is below $\beta - \delta$, Alice announces that the protocol aborts.

7. If the protocol does not abort, Alice and Bob use the rounds with $T_i = 0$ to generate a key using EC and PA over the authenticated classical channel. The EAT tells them how much key can be extracted, subject to adjustments for the communicated EC information.

To explain the structure of the protocol it is helpful to think about an ideal implementation. In this, the preparation device generates a maximally-entangled state $(|00\rangle + |11\rangle)/\sqrt{2}$ and for $A, B \in \{0, 1\}$ the measurements are as described in (85). Furthermore, for $B = 2$, the measurement is in the $\{|\psi_0\rangle, |\psi_\pi\rangle\}$ basis, i.e., the same basis as for $A = 0$. If α is chosen to be small, on most of the rounds both parties measure in the $\{|0\rangle, |1\rangle\}$ basis which should give perfectly correlated outcomes, suitable for key. However, on some of the rounds (those with $T_i = 1$), a CHSH test is performed, in order to keep the devices honest. These are the spot-checks that give the protocol its name. The parameter β is the expected CHSH value of the setup ($\beta = 2\sqrt{2}$ in the ideal implementation) and δ is some tolerance to statistical fluctuations.

The probability that an ideal implementation with no eavesdropping leads to an abort is called the *completeness error*. Using the implementation given above, this occurs when statistical fluctuations cause devices with an expected CHSH value of β to produce a value below $\beta - \delta$. An ideal implementation behaves in an independent and identically distributed (i.i.d.) way and hence standard statistical bounds imply that the completeness error is exponentially small in the number of rounds.

It is worth making some remarks about the protocol:

1. It is important that the preparation device is unable to access information from Alice's measurement device, even though these may be in the same lab (if access were granted, the preparation device could send previous measurement results to Eve via the quantum channel).

2. The choice T_i needs to be communicated after the state is shared (otherwise Eve can choose whether to intercept and modify the quantum state depending on whether or not a test will be performed). This requires Alice and Bob to have a (short-lived) quantum memory; without such a memory, Alice and Bob could instead use some pre-shared randomness to make these choices and then consider the modified protocol to be one for *key expansion*. For reasonable parameter ranges, this would still lead to expansion, because α can be low and so a small amount of pre-shared key is needed to jointly choose the values of $\{T_i\}$.

3. Bob's device can tell when it is being used to generate key ($B_i = 2$). Crucially though, Alice's device cannot (Alice's device learns only A_i and not the value of T_i), and it is this that forces her device to behave honestly; not doing so will lead to her getting caught out if the round is a test. If Bob's device does not behave close enough to the way it should in the case $B_i = 2$, then the protocol will abort during EC step.

There are many other possible protocols, but they follow the same basic idea of generating shared randomness while occasionally doing tests based on some non-local game, estimate the amount of min-entropy that any devices that pass the tests with high probability must give and then using classical protocols to eliminate errors and remove any information Eve may have through PA.

E. Historical remarks

Using violation of a Bell inequality as part of a key distribution protocol goes back to the Ekert protocol [114], and many device-independent protocols can be seen as a development of this. However, Ekert's work didn't envisage foregoing trust on the devices, and the idea behind this came many years later under the name of self-checking [41]. The first protocol with a full security proof was that of Barrett, Hardy and Kent [42], and their protocol is even secure against eavesdroppers not limited by quantum theory, but by some hypothetical post-quantum theory, provided it is no-signalling.

However, it has the drawback of a negligible key rate and the impracticality of needing as many devices as candidate entangled pairs to ensure all of the required no-signalling conditions are met. Following this were several works that developed protocols with reasonable key rates, proving security against restricted attacks [116, 214, 221, 222] with as many devices as candidate entangled states [148, 216, 223, 224]. Later proofs avoided such restrictions [108, 225–227], but still were not able to tolerate reasonable levels of either noise or had poor rates (or both). Using the EAT [213] leads to a reasonable rate and noise tolerance [212], and better rates still can be derived from recent strengthened versions of the EAT [228].

F. Putting DI-QKD protocols into practice

Although device-independence in principle allows for stronger security, adopting it in practice is more challenging than ordinary QKD. This is because it is difficult to generate correlations that violate a Bell inequality at large separations. Using photons is a natural way to quickly distribute entanglement. However, detecting single photons is difficult. In a device-dependent QKD protocol such as BB84, failed detection events slow down the generation of key, but it is possible to post-select on detection; in a device-independent protocol, below a certain detection threshold, no key can be securely generated. This is because post-selecting on detection events leads to the possibility that the post-selected events appear to be non-local when they are in fact not. To treat this problem, suppose that each detector detects a photon with probability $\eta \in [0,1]$. A distribution of the form P_ε from Eq. (84) will become

$$P_{\varepsilon,\eta} := \left(\begin{array}{ccc|ccc} \eta^2(\frac{1}{2}-\varepsilon) & \eta^2\varepsilon & \frac{\eta(1-\eta)}{2} & \eta^2(\frac{1}{2}-\varepsilon) & \eta^2\varepsilon & \frac{\eta(1-\eta)}{2} \\ \eta^2\varepsilon & \eta^2(\frac{1}{2}-\varepsilon) & \frac{\eta(1-\eta)}{2} & \eta^2\varepsilon & \eta^2(\frac{1}{2}-\varepsilon) & \frac{\eta(1-\eta)}{2} \\ \frac{\eta(1-\eta)}{2} & \frac{\eta(1-\eta)}{2} & (1-\eta)^2 & \frac{\eta(1-\eta)}{2} & \frac{\eta(1-\eta)}{2} & (1-\eta)^2 \\ \hline \eta^2(\frac{1}{2}-\varepsilon) & \eta^2\varepsilon & \frac{\eta(1-\eta)}{2} & \eta^2\varepsilon & \eta^2(\frac{1}{2}-\varepsilon) & \frac{\eta(1-\eta)}{2} \\ \eta^2\varepsilon & \eta^2(\frac{1}{2}-\varepsilon) & \frac{\eta(1-\eta)}{2} & \eta^2(\frac{1}{2}-\varepsilon) & \eta^2\varepsilon & \frac{\eta(1-\eta)}{2} \\ \frac{\eta(1-\eta)}{2} & \frac{\eta(1-\eta)}{2} & (1-\eta)^2 & \frac{\eta(1-\eta)}{2} & \frac{\eta(1-\eta)}{2} & (1-\eta)^2 \end{array}\right), \tag{90}$$

where the third outcome corresponds to a no-detection event. Post-selecting on both detectors clicking recovers the distribution P_ε, but it can be the case that P_ε is not a convex combination of local deterministic distributions, but that $P_{\varepsilon,\eta}$ is. To avoid this, the experimental conditions need to be such that the distribution *including no-click events* has no deterministic decomposition. In the terminology of Bell experiments, this is referred to as closing the *detection loophole*. For the distribution $P_{\varepsilon,\eta}$ given above, this loophole is closed provided $\eta > 2/(3-8\varepsilon)$ (see the examples file for [229]). Note that for $\eta \leq 2/3$ this cannot be satisfied for any ε. Hence, for protocols based on CHSH, 2/3 is a lower bound on the detection efficiency required. This is known as Eberhard's bound [230].

Another loophole that is of interest for Bell experiments is the *locality loophole*, which is closed by doing measurements at space-like separation. The desire to close this loophole comes from a concern that the devices are able to talk to each other during the measurements, and, in particular, that one device is able to learn the measurement choice of the other, which makes it trivial to violate a Bell inequality in a classical deterministic way. It was a longstanding technical problem to simultaneously close the locality and detection loopholes [231, 232], a feat that was only recently achieved [233–235]. In the context of DI-QKD, however, it is not necessary to close the locality loophole (although it does not hurt). The reason is that for QKD it is necessary that Alice's and Bob's lab are secure (Assumption 1 above). If their devices could communicate with each other during the measurements then this assumption is broken, and it makes little sense to allow communication between devices without allowing it from the devices to Eve.

G. Measurement device independence

In DI-QKD one avoids the formulation of a mathematical model describing the devices involved in the experiment and aims at proving the security of the communication protocol only from the collected data. This is possible because only a purely quantum experiment can provide data that violate Bell inequalities. This approach is conceptually powerful but limited in terms of attainable key rates. Here we review the main ideas of MDI-QKD [52, 53]. This is a framework in which no assumptions is made on the detectors involved in the QKD protocols, which can be operated by a malicious eavesdropper.

In a typical MDI-QKD protocol, both trusted users Alice and Bob send quantum signals to a central receiver (also called relay). The assumptions are that Alice and Bob have perfect control on the quantum state they prepare and send through the quantum channels. On the other hand, no assumption is made on the central relay, which can be under the control of Eve. In this way one does not need to bother about the trustfulness of any detector or in general of any measurement device. Although at first sight it may seem impossible to extract any secrecy at all from such a scheme, it is indeed possible to exploit this MDI scheme to generate secret key at a nonzero rate.

In a simple (idealized) scheme of MDI-QKD, Alice and Bob locally prepare single-photon states with either rectilinear polarization (Z basis) $\{|H\rangle, |V\rangle\}$ or diagonal polarization (X basis) $\{|D\rangle, |A\rangle\}$, where $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$ and $|A\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$. These states are sent to a central relay that is assumed under control of Eve. Notice that the states initially sent to Eve are statistically independent. Any possible physical transformation may affect the signals traveling through the quantum channels that connect Alice and Bob to the central relay. Also, Eve can apply any measurement on the received signals, or she can store them in a long term quantum memory. However, to explain the working principle of MDI-QKD let us assume for a moment that the channels from the trusted users to Eve are noiseless, and that Eve performs an ideal Bell detection on the incoming signals. These assumptions will be relaxed later. Moreover, we require that Eve publicly announces the outcome $\alpha = 0, 1, 2, 3$ of the Bell detection.

The ideal Bell detection is a positive-operator valued measurement (POVM) with four elements, $\Lambda_\alpha := (\mathbb{1}\otimes\sigma_\alpha)|\beta\rangle\langle\beta|(\mathbb{1}\otimes\sigma_\alpha^\dagger)$, where $|\beta\rangle = 2^{-1/2}\,(|HH\rangle + |VV\rangle)$ is a maximally entangled state, and σ_α are the Pauli operators (including the identity), i.e, $\sigma_0 = |H\rangle\langle H| + |V\rangle\langle V|$, $\sigma_1 = |H\rangle\langle V| + |V\rangle\langle H|$, $\sigma_2 = -i|H\rangle\langle V| + i|V\rangle\langle H|$, and $\sigma_3 = |H\rangle\langle H| - |V\rangle\langle V|$. It is easy to check that the four POVM elements are projectors onto the states of the Bell basis (up to a global phase)

$$\Phi^\pm = (|HH\rangle \pm |VV\rangle)/\sqrt{2}, \quad \text{for } \alpha = 0, 3 \tag{91}$$

$$\Psi^\pm = (|HV\rangle \pm |VH\rangle)/\sqrt{2}, \quad \text{for } \alpha = 1, 2. \tag{92}$$

Note that, if both Alice and Bob encode information in the rectilinear basis $\{|H\rangle, |V\rangle\}$, then they know that their encoded bit values are the same if the outcome is $\alpha = 0$ or $\alpha = 3$, otherwise they know that they are opposite if $\alpha = 1$ or $\alpha = 2$ and one of the two needs to apply a bit flip. Therefore, Bob can obtain Alice's bit by flipping (or not flipping) his local bit according to the value of α. Similar is the situation if Alice and Bob use the diagonal basis $\{|D\rangle, |A\rangle\}$. The overall situation is summarized in Table V which shows the rule to apply (bit flip or identity) given the Bell outcome α and the common basis chosen by the parties. If the parties choose different bases, they simply discard their data.

	$\{\|H\rangle, \|V\rangle\}$	$\{\|D\rangle, \|A\rangle\}$
$\alpha = 0$	–	–
$\alpha = 1$	bit flip	–
$\alpha = 2$	bit flip	bit flip
$\alpha = 3$	–	bit flip

TABLE V.

The above example shows that the Bell detection performed by the relay can induce (or post-select) strong correlations between the bits locally prepared by the trusted users, after they sift their data according to the choice of local polarization basis. In other words, ideal Bell detection simulates a virtual noiseless communication channel connecting the two honest users. Notice that the output of the Bell detection contains information about the identity (or non-identity) of the pair of bit values encoded by Alice and Bob (after sifting) but does not contain any information about the actual bit values.

In a more realistic scenario, we need to consider that linear optical implementations of the DV Bell measurement do not realize the ideal POVM above, but they are restricted to a partial realization where only two out of the four Bell states are unambiguously distinguished. Therefore, in a practical realization [53], the signals are mixed in a 50 : 50 beam splitter, and the outputs processed by two polarizing beam splitters (PBS), filtering the input photons into states $|H\rangle$ or $|V\rangle$, and finally detected by two pairs of single-photon detectors. The measurement is successful when two of the four detectors click. This corresponds to perform a partial Bell measurement which distinguishes between the two Bell states Ψ^+ and Ψ^-. It is clear that this feature automatically halves the rate of the protocol.

To further move towards experimental implementations, one shall replace single-photon states with realistic phase-randomized weak coherent states with intensities (mean photon numbers) μ_A and μ_B for Alice and Bob, respectively. We therefore need to use the method of decoy states to estimate the single-photon contributions to the rate, following the same methodology described for the BB84 protocol (see Sec. III C 2). Assuming that the rectilinear basis $\{|H\rangle, |V\rangle\}$ is used to generate the key and the diagonal basis $\{|D\rangle, |A\rangle\}$ is used for testing (computation of the QBER), the asymptotic rate of decoy-state DV MDI QKD is given by the following expression [53]

$$R_{\rm MDI}^{\rm decoy} = Q_{11}^{\rm rect}[1 - H_2(e_{11}^{\rm diag})] - Q^{\rm rect}\ f(E^{\rm rect})H_2(E^{\rm rect}). \tag{93}$$

In this formula, $Q^{\rm rect}$ is the overall gain and $E^{\rm rect}$ is the overall QBER, both in the rectilinear basis. The parameter $f \geq 1$ is the efficiency of classical EC codes, e.g., $f(E^{\rm rect}) = 1.16$. Then, $Q_{11}^{\rm rect}$ is the gain associated with single-photon pulses in the rectilinear basis, and $e_{11}^{\rm diag}$ is the QBER when Alice and Bob send single-photon pulses in the diagonal basis. In particular, we

have $Q_{11}^{\rm rect} = P_{11}^{\rm rect} Y_{11}^{\rm rect}$, where

$$P_{11}^{\rm rect} = \mu_A \mu_B \exp[-(\mu_A + \mu_B)] \tag{94}$$

is the joint probability that both emitters generate single-photon pulses in the rectilinear basis, and $Y_{11}^{\rm rect}$ (single-photon yield) is the probability of successful Bell detection given that Alice and Bob send single-photon states in the rectilinear basis. Note that $Y_{11}^{\rm rect}$ includes the 1/2 efficiency of the partial Bell detection, the sifting factor 1/2, and also another factor 1/2 due to the diagonal basis not being used for the key. In the EC rate $Q^{\rm rect}\ f(E^{\rm rect}) H_2(E^{\rm rect})$ and the PA rate $Q_{11}^{\rm rect} H_2(e_{11}^{\rm diag})$, the quantities $Q_{11}^{\rm rect}$ and $e_{11}^{\rm diag}$ can be practically bounded by using a finite number of decoy intensities [236–238].

In ideal conditions of zero QBER, the key rate of Eq. (93) would be just the gain $Q_{11}^{\rm rect}$. Assuming zero dark counts, one may write $Y_{11}^{\rm rect} = \eta_A \eta_B / 8$, where 1/8 accounts for the factors described above, and the product of the transmissivities $\eta_A \eta_B$ is the probability that Alice's and Bob's single-photon states reach the middle relay. Thus, one has

$$Q_{11}^{\rm rect} = \frac{\eta_A \eta_B \mu_A \mu_B}{8} \exp[-(\mu_A + \mu_B)]. \tag{95}$$

By optimizing over the intensities ($\mu_A = \mu_B = 1$) and assuming the symmetric configutation $\eta_A = \eta_B = \sqrt{\eta}$, one finds that the key rate would scale as $\eta/(8e^2)$. Finally assume that the Bell detection can be done with unit efficiency (e.g., via non-linear optics) and the diagonal basis is also used for key extraction. In this ideal case, the rate of decoy-state DV MDI-QKD would scale as

$$R_{\rm MDI}^{\rm decoy\text{-}ideal} = \frac{\eta}{2e^2}. \tag{96}$$

The above example is a special case of a general approach that protect QKD from side-channel attacks on the measurement devices. In the more general framework introduced by Ref. [52], each honest user prepares a bipartite quantum state and sends one subsystem to the relay. The state received by the relay has thus the form $\rho_{AA'} \otimes \rho_{B'B}$, where the system A, B are those retained by the Alice and Bob, respectively. A generic operation applied by the relay is described by a quantum instrument [239] characterized by a set of operators $\Lambda^z_{A'B' \to E}$. This includes a measurement with outcome z and storage of information in a quantum memory E. If Eve applies the measurement and then announces the outcome z, for any given value of z the correlations between Alice, Bob, and Eve, are described by the tripartite state

$$\rho^z_{ABE} = \frac{1}{p(z)} \left(\mathcal{I}_A \otimes \mathcal{I}_B \otimes \Lambda^z_{A'B' \to E} \right) (\rho_{AA'} \otimes \rho_{B'B}), \tag{97}$$

where $p(z) = {\rm Tr}(\Lambda^z_{A'B' \to E} \rho_{A'} \rho_{B'})$.

The conditional reduced state ρ^z_{AB} is no longer factorized and exhibits correlations between Alice and Bob. To extract secret bits from such a state Alice and Bob must apply local measurements with outcome variables X and Y, so that the total conditional state ρ^z_{ABE} is projected onto a tripartite classical-quantum state ρ^z_{XYE}. The asymptotic secret key rate is obtained from the expression of the mutual information between Alice and Bob averaged over z, i.e., $I_{AB} = \sum_z p(z) I(X:Y)_{\rho^z}$, minus the average Holevo information between Alice and Eve, i.e., $\chi_{AE} = \sum_z p(z) I(X:E)_{\rho^z}$ (in the case of DR). The general approach of Ref. [52] not only provides a security proof for DV MDI-QKD schemes but also sets the basis for an extension to CV systems, later realized in Ref. [240]. Since 2012, many theoretical studies on DV MDI-QKD appeared in the literature and giving a list would not be exhaustive [241–245].

H. Twin-field QKD

In the MDI-QKD protocol, the idea is to use a middle relay that may be untrusted, i.e., run by Eve. This is a very first practical step towards the end-to-end principle of networks which assumes a scenario with 'cheap' and unreliable middle nodes. On the other hand, despite MDI-QKD employs an untrusted relay, it is not able to beat the PLOB bound for point-to-point QKD [43]. This limitation has been recently lifted by the introduction of the more efficient protocol of TF-QKD [54]. The TF-QKD protocol has led to further theoretical investigations [246] and a number of TF-inspired variants, including the phase-matching (PM) protocol [247] (see also Ref. [248]), the "sending or not sending" (SNS) version of TF-QKD [249–251], further improved into the active odd-parity pair (AOPP) protocol [252], and the no-phase-postselected TF (NPPTF) protocol [253–255] (see also Refs. [256–258]).

In the TF-QKD protocol [54], Alice and Bob send two phase-randomized optical fields (dim pulses) to the middle relay (Charlie/Eve) to produce a single-photon interference to be detected by a single-photon detector, whose outcomes are publicly declared. The term *twin* derives from the fact that the electromagnetic phases of the optical fields should be sufficiently close in order to interfere. More precisely, Alice and Bob ($i = A$ or B) send to the relay pulses whose intensities $\xi_i \in \{\mu, \nu, \tilde{\nu}\}/2$ are randomly selected between the signal intensity $\mu/2$, and the decoy intensities $\nu/2$ and $\tilde{\nu}/2$. Then, they respectively choose phases φ_A and φ_B as $\varphi_i = (\alpha_i + \beta_i + \delta_i) {\rm mod}(2\pi)$, where $\alpha_i \in \{0, \pi\}$ encodes a bit $(0,1)$, $\beta_i \in \{0, \pi/2\}$ determines the basis, and the final term δ_i is randomly selected. The parties split the interval $[0, 2\pi)$ into M equal slices Δ_k with $k = \{0, 1..., M-1\}$. They then record to which phase slices Δ_k^A (for Alice) and Δ_k^B (for Bob) their values δ_A and δ_B belong.

At the relay the two incoming pulses interfere on a beam splitter whose outputs are measured by two single-photon detectors D_0 and D_1. At the end of the quantum communication, Charlie declares the instances where one of the two detectors clicked. Depending on which detec-

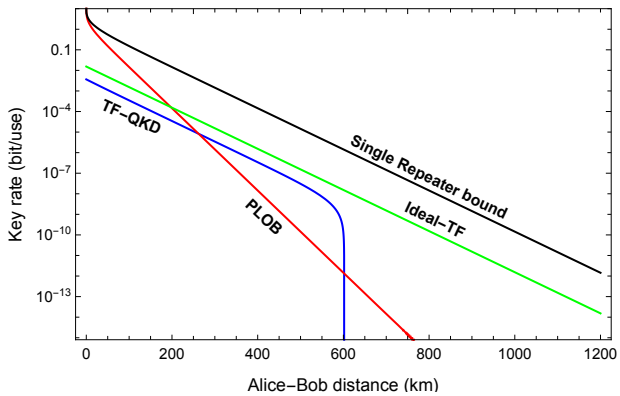

FIG. 3. Key rate of the TF-QKD protocol [54] versus Alice-Bob total distance in standard optical fiber (0.2 dB/km), assuming realistic (blue line) and ideal (green line) conditions. For the realistic key rate we assume 10^{-8} dark count probability per detector, 75% loss at the relay, 50% detector efficiency, and EC efficiency of 1.1 (for more details see Ref. [54]). For the ideal key rate we consider the rate in Eq. (102). We also plot the point-to-point repeaterless PLOB bound [43] and the single-repeater bound [58, 59]. We can see that the PLOB bound is violated, showing that the TF-QKD protocol is equivalent to an active repeater.

tor clicks, Alice and Bob assign the value 0 or π to a public variable γ (no-detection and double-detection events are discarded). Next, Alice announces the intensity ξ_A, the basis β_A and the phase slice Δ_k^A she has used for each instance, with Bob declaring those instances where his choices were the same. Alice and Bob disclose the values α_A and α_B of the matched runs, except those associated with the signal intensity $\mu/2$ and the basis choice $\beta_A = \beta_B = 0$, which are processed into the key: from α_B and $\gamma = |\alpha_B - \alpha_A|$, Bob can retrieve Alice's α_A and decode her secret bit. All the other (public) bits are used to perform estimation of the error rates and the decoy-state parameters.

An important feature to note is that TF-QKD has an intrinsic QBER E_M which is due to the finite slicing of the phase: the interfering beams are 'twins', i.e., their phases are very similar but not exactly identical, due to the randomness of δ_A and δ_B within the selected slice. On average, one can compute [54]

$$E_M = \frac{1}{2} - \frac{\sin(2\pi M^{-1})}{4\pi M^{-1}}. \tag{98}$$

While this error goes to zero for large M, we simultaneously have that the rate is affecting by sifting factor M^{-1} that would send it to zero. There is therefore an optimal M for the protocol, which is estimated to be $M = 16$ with intrinsic QBER $E_M \simeq 1.275\%$ [54].

In Ref. [54], the authors considered a restricted scenario where the 'global phase' does not leak any useful information to Eve. Assuming that Alice and Bob are separated by an overall channel of transmissivity η and they use sources with total signal intensity μ, the key rate is given by

$$R_{\rm TF}(\mu,\eta) = \frac{d}{M}\left[R^{\rm dec}_{\text{eff-BB84}}(\mu,\sqrt{\eta})\right]_{E_M}, \tag{99}$$

where $d \leq 1$ is a duty cycle factor related to the correction of misalignments, and $R^{\rm dec}_{\text{eff-BB84}}$ is the secret key rate of an efficient decoy-state BB84 protocol given in Eq. (69), to be computed accounting for the intrinsic QBER E_M.

One can extrapolate the ideal scaling of the TF-QKD protocol starting from Eq. (99). Assuming perfect devices ($d = 1$, and no dark counts), minimal QBER (i.e., equal to the intrinsic one), perfect EC ($f = 1$) and an infinite number of decoy intensities, one can set

$$e_1^{\rm UB} = E_\mu = E_M,\ Q_\mu = \mu\sqrt{\eta},\ Q_1^{\rm LB} = \mu e^{-\mu}\sqrt{\eta}, \tag{100}$$

so that the TF-QKD rate becomes [54]

$$R^{\rm ideal}_{\rm TF}(\mu,\eta) = \frac{\mu\sqrt{\eta}}{M}\left\{e^{-\mu}[1 - H_2(E_M)] - H_2(E_M)\right\}. \tag{101}$$

This is further optimized by taking $M = 16$, so that one picks the optimal values $E_M \simeq 1.275\%$ and $\mu \simeq 0.765$, which leads to

$$R^{\rm ideal}_{\rm TF}(\eta) \simeq 0.01535\sqrt{\eta}. \tag{102}$$

It is easy to check that the ideal rate $R^{\rm ideal}_{\rm TF}(\eta)$ beats the fundamental PLOB bound $\simeq 1.44\eta$ at the equivalent of 197km in optical fiber, assuming the standard loss rate of 0.2dB/km. Note that the larger Takeoka-Guha-Wilde (TGW) bound [259], with scaling $\simeq 2.88\eta$, would only be intercepted at 227km, missing the correct value by 30km, i.e., by non-trivial 6dB in optical fiber or the equivalent of two extra 50:50 beam splitters on the line.

It is interesting to note an important feature of TF-QKD with respect to MDI-QKD. In DV MDI-QKD, the Bell measurement is successful when two of the four detectors click (see previous Sec. IV G). The joint probability of a successful Bell measurement given the transmission of Alice's AND Bob's single-photon pulses (1-photon yield Y_{11}) is given by the product of the probabilities η_A and η_B. As a result, the 1-photon gain Q_{11} of DV MDI-QKD protocol is given by Eq. (95), which scales as η in the symmetric configuration ($\eta_A = \eta_B = \sqrt{\eta}$). At zero QBER, this is the surviving quantity in Eq. (93) which limits the scaling of DV MDI-QKD to η bits per use as in Eq. (96). By contrast, TF-QKD is based on single detections at the relay, so that the measurement is successful if Alice's OR Bob's single-pulse reaches the relay and is detected. The conditional probability of this event (1-photon yield Y_1) is given by $\sqrt{\eta}$. As a result, the 1-photon gain Q_1 in Eq. (100) goes as $\sqrt{\eta}$. At zero QBER, this quantity provides the improved scaling $O(\sqrt{\eta})$ of the ideal TF-QKD key rate.

Later, Ref. [246] proved the unconditional security of the TF-QKD protocol against general attacks (see also the Ref. [247]). While a general attack considerably increases Eve's gain, the key rate scaling $O(\sqrt{\eta})$ remains

unchanged. As a matter of fact, using the TF-QKD protocol [54] (and the PM-QKD protocol [247]) over a communication line with total Alice-Bob's transmissivity η, not only the PLOB bound is beaten but the rate performance is not so far from the single-repeater bound of $-\log_2(1-\sqrt{\eta})$ [58, 59]. See Fig. 3.

Yet other variants of the TF-QKD protocol have been recently proposed [260–264] and experimental implementations have been carried out [258, 265–267]. In particular, the proof-of-concept experiment in Ref. [265] has shown, for the first time, that one can overcome the fundamental PLOB bound by means of an untrusted measurement-based QKD repeater, a result previously thought to be out of the reach of present technology.

V. EXPERIMENTAL DV-QKD PROTOCOLS

The original BB84 protocol requires perfect single photon sources which emit only one photon at a time. Since these sources are notoriously hard to build they have been replaced by coherent state sources which are heavily attenuated to a fraction of a photon per pulse. However, these sources lead to security concerns due to the probability to have more than a photon per pulse and a photon splitting attack has been proposed and demonstrated to exploit the wrong assumption in the security proofs. As described before a rigorous security [157, 268] analysis has been proposed with the idea of estimating the ratio of secure signals from which the secure bits are distilled by post-processing. For practical sources the bounds found in the security analysis are not tight leading to a degradation of system performance. To circumvent this problem several novel protocols with different encoding schemes have been proposed and in the following sections we explain the development of their implementations in detail. Despite the different encoding schemes all DV QKD system have single photon detectors in common to detect the arriving states. To achieve high key rates high count rates and, thus, low dead times are necessary. Extremely long distances require however low dark count rates.

A. Detector technology

At the receiver side the arriving photon pulses are processed by e.g. beam splitters, interferometers or a like to decode the information encoded in various degrees of freedoms. After optical processing the photons are detected by single photon detectors which set limits on the achievable performance.

Indium Gallium Arsenide (InGaAs) avalanche photodiodes detect single photons by generating a strong electron avalanche at the absorption of a photon when operated with a reverse voltage above the breakdown voltage. However, the strong avalanche current can lead to trapped electron charges in defects. Spontaneously released they trigger a second avalanche pulse, a so-called afterpulse. A common approach to suppress the afterpulse is gating. To further suppress this afterpulse and to allow for gating frequencies beyond 1 GHz, a self-differentiating technique was introduced to detect much weaker avalanches [269]. Operating at $-30°$ C the APD was gated at 1.25 GHz, obtaining a count rate of 100 MHz with an detection efficiency of 10.8%, an afterpulse probability of about 6% and a dark count rate of about 3 kHz.

To achieve higher quantum efficiencies and in particular lower dark count rates, superconducting nanowire single photon detectors (SNSPDs) have been developed. They consist of a nanometer thick and hundreds of nanometer wide nanowire with a length of hundreds of micrometers. Compactly patterned in a meander structure they fill a square or circular area on the chip. The nanowire is cooled below its superconducting critical temperature and a bias current just below the superconducting critical current is applied. An incident photon breaks up Cooper pairs in the nanowire which lowers the superconducting critical current below the bias current which produces a measurable voltage pulse. A recent development [270] shows dark count rates of 0.1 Hz, low jitter of 26 ps and a quantum efficiency of 80 % at a temperature of 0.8 K. SNSPDs have been integrated into photonic circuits [271, 272].

B. Decoy state BB84

As described before decoy state QKD severely increases security and distance for attenuated coherent laser pulse sources and is much more practical in comparison to single photon sources. The first implementation was performed in 2006 with one decoy state by modifying a commercial two-way idQuantique system [273]. In the two-way protocol with phase encoding Bob sent bright laser pulses to Alice who after attenuating them to the single photon level and applying a phase shift sent them back to Bob for measurement. The intensity of the pulses was randomly modulated by an acousto-optical modulator inserted into Alice's station to either signal state or decoy state level before sending the pulses back to Bob. Shortly later the same group implemented a two decoy state protocol with an additional vacuum state to detect the background and dark count detection probability [274].

The demonstration of two-decoy states BB84 in a one-way QKD system was reported by three groups at the same time in 2007. In Ref. [275] phase encoding was employed and secure key generation was shown over a distance of 107 km using optical fiber on a spool in the lab. Including finite statistics in the parameter estimation, a secret key rate of 12 bit/s was achieved. To generate the decoy states pulses from a distributed-feedback laser diode at a repetition rate of 2.5 MHz were amplitude modulated with an amplitude modulator. For detection single-photon sensitive superconducting transition-edge

detectors were employed.

The second group demonstrated two-decoy state QKD over a 144 km free-space link with 35 dB attenuation between the canary islands La Palma and Tenerife [276]. Here, the BB84 states were polarization encoded. Four 850 nm laser diodes oriented at 45° relative to the neighbouring one were used in the transmitter. At a clock rate of 10 MHz one of them emitted a 2 ns pulse. The decoy states of high intensity were generated at random times by two laser diodes emitting a pulse at the same time, while for the vacuum state no pulse was emitted. The receiver performed polarization analysis using polarizing beam splitters and four avalanche photo detectors. A secure key rate of 12.8 bit/s was achieved.

The third group used polarization encoding and demonstrated secret key generation over 102 km of fiber [277]. The transmitter consisted of 10 laser diodes each of which produced 1 ns pulses at the central wavelength of 1550 nm with a repetition rate of 2.5 MHz. Four laser diodes were used for signal and high intensity decoy state generation, respectively, using a polarization controller to transform the output polarization of a laser diode to the respective polarization of one of the four BB84 states. Two additional laser diodes were used for calibrating the two sets of polarization basis which was performed in a time multiplexed fashion. The outputs of the 10 laser diodes were routed to a single optical fiber using a network of multiple beam splitters and polarization beam splitters. An additional dense wavelength division multiplexing filter ensured that the wavelengths of the emitted photons was equal. The receiver consisted of two single photon detectors and a switch to randomly choose one polarization basis.

Using advances in InGaAs avalanche photon detection (APD) operating in self-differencing mode [269] GHz clocked decoy state QKD was demonstrated in 2008 [278]. A self-differencing circuit can sense smaller avalanche charges thereby reducing after pulse probability and thus dead time. The demonstrated QKD system clocked at 1.036 GHz was based on a phase encoded GHz system implementing the BB84 protocol [279] and used two decoy states generated by an intensity modulator. Dispersion shifted single mode fiber was employed since for channel lengths over 65 km fiber chromatic dispersion must be compensated for in standard SMF28 single mode fiber.

In the standard BB84 protocol Bob measures in the wrong basis 50 % of the time. Moreover, in decoy state BB84, it is advantageous to send the states with higher intensity more often than the others. To increase the usable signal generation rate an efficient version with asymmetric bases choice and highly unbalanced intensities was introduced, with an implementation reported in [280]. They prove the protocol's composable security for collective attacks and improved parameter estimation with a numerical optimization technique. Based on phase encoding the GHz system achieved a secure key rate of 1.09 MBit/s in contrast to 0.63 MBit/s for the standard protocol over 50 km of fiber. Its experimental implementation is depicted in Fig. 4a.

Composable security against coherent attacks was only achieved recently. Ref. [284] describes an experiment demonstrating it with a modified two-way commercial plug-and-play QKD system where the authors also included imperfect state generation. Security against coherent attacks was furthermore demonstrated in [285] with a one-way phase-encoding system. With the latter system the authors achieved a distance in ultra-low loss fiber (0.18 dB/km) of 240 km. Using APDs with a detection efficiency of 10 % a dark count rate of 10 counts/s was achieved at −60°C reached with a thermal-electrical cooler.

The current distance record of 421 km in ultra low-loss optical fiber (0.17 dB/km) was achieved by a simplified BB84 scheme with one decoy state [281] but under the restrictive assumption of collective attacks. The distance record was achieved by optimizing the individual components and simplifying the protocol. The system was clocked at 2.5 GHz and used efficient superconducting detectors (about 50 %) with a dark count rate below 0.3 Hz. The protocol was based on a scheme with three states using time bin encoding. Two states were generated in the Z basis, a weak coherent pulse in the first or the second time bin, respectively. The third state, a state in the X basis, was a superposition of two pulses in both time bins. While the Z basis states were used to estimate the leaked information to the eavesdropper, the X basis state was used to generate the raw key. The experimental setup is shown in Fig. 4b.

C. Differential phase shift QKD

Differential phase shift (DPS) QKD encodes information into the differential phase shift of two sequential pulses. The first QKD system employing this encoding technique was reported in 2004 over 20 km fiber [286]. A continuous-wave (CW) laser diode from an external-cavity laser was intensity modulated at 1 GHz to carve 125 ps long pulses. Afterwards a phase modulator was used to modulate the phase of each pulse randomly by 0 or π. An attenuator attenuated the beam to 0.1 photon per pulse. At the receiver side the differential phase between two sequential pulses was measured with an unbalanced Mach-Zehnder interferometer. The incoming pulses were split 50:50 and before recombination at another 50:50 splitter, one arm was delayed by the interval of time between two pulses. The two outputs of the unbalanced Mach-Zehnder interferometer were detected by gated avalanche single photon detectors. The Mach-Zehnder interferometer was as waveguides and the arm length difference could be controlled thermally.

Using superconducting single photon detectors and a 10 GHz clock frequency keys were distributed over 200 km dispersion shifted fiber [287]. In a different experiment, a secure bit rate in the MBit/s range was achieved over 10 km by using a 2 GHz pulse train with 70 ps long

pulses [288]. At the receiver after the unbalanced Mach-Zehnder interferometer the photons were upconverted in a nonlinear process and detected by a Silicon avalanche photo diode which enabled count rates of 10 MHz with a low timing jitter. High-rates of 24 kbit/s over 100 km were achieved using 2 GHz sinusoidally gated avalanche photo diodes and the important influence of laser phase noise has been studied [289]. Using a Michelson interferometer with unequal arm length based on a beam splitter and two Faraday mirrors and superconducting detectors at the receiver the maximum transmission distance has been boosted to 260 km in standard telecom fiber [282]. Its experimental implementation is depicted in Fig. 4c.

Experimental implementations of DPS-QKD have been done assuming restrictive eavesdropping strategies. For instance, this protocol was implemented in the Tokyo QKD network [49, 290] under the assumption of individual attacks [291]. The unconditional security against coherent attacks was proven in Ref. [292]. It is also important to mention that, connected with DPS-QKD, there is the variant of differential-quadrature-phase-shift (DQPS) QKD [293]. DQPS-QKD was proven to be secure in Ref. [294] and experimentally implemented in Ref. [295].

D. Coherent one-way

The first proof-of-principle implementation of the COW protocol has been reported in 2005 [296]. A 1550 nm CW laser beam was intensity modulated to generate the quantum or decoy states and a variable attenuator attenuates the beam to the single photon level. Bits were encoded into arrival time by two consecutive pulses: A vacuum state followed by a coherent state represented bit 0, a coherent state followed by a vacuum state represented bit 1. The decoy state was represented by two coherent states. On the receiver side the beam was split by a tap coupler (tapping e.g. 10 %). While the highly transmissive output was detected by a single photon detector, the tap was injected into an interferometer with asymmetric arms which interfered the two pulses. One output of the interferometer was measured by a single photon detector and the measurement outcomes were used to calculate the visibility to check channel disturbances. The unbalanced interferometer was implemented as Michelson interferometer by using a 3 dB coupler and two Faraday mirrors.

Running at a high clock speed of 625 MHz a fully automated system was built and demonstrated over 150 km in deployed telecom fiber [297]. The high clock speed was reached with a CW distributed fiber-Bragg telecom laser diode, a 10 GHz Lithium Niobate intensity modulator and Peltier cooled InGaAs avalanche photo diodes in free-running mode for short distances and SNSPDs operating at sub-4 K with lower noise for long distances. Synchronization was achieved by wavelength division multiplexing of a synchronization channel and a classical communication channel through a second optical fiber. Using ultra-low loss fibers and low-noise superconducting detector operating at 2.5 K a distance of 250 km was reached [298]. In the experiment, the security level was asymptotic against collective attacks.

Finite-size effects (still under collective attacks) were taken into consideration in the implementation described in 2014 [299] which reached 21 kbit per second over 25 km fiber with gated InGaAs detectors and a key distillation in FPGAs. Here, the COW QKD system was tested with one single optical fiber only using dense-wavelength division multiplexing for quantum and all classical channels.

The distance record of a system implementing the coherent one-way protocol was reported in 2015 [283] reaching 307 km. Novel free-running InGaAs/InP negative feedback avalanche detectors operated at 153 K with low background noise (few dark counts per second) and low loss optical fibers enabled the result. The experimental implementation is schematically depicted in Fig. 4d. The security analysis was composable accounting for finite size effects, under the assumption of collective attacks. The unconditional security against coherent attacks was proven for a variant of the COW protocol in Ref. [292].

E. DV MDI-QKD

DV MDI-QKD was first experimentally demonstrated in 2013 by three groups. The first group implemented MDI-QKD between three locations in Calgary with a distance of about 12 km between Alice and the untrusted relay Charlie and about 6 km between Bob and Charlie [300]. Alice's and Bob's transmitter generated time-bin qubits at a rate of 2 MHz using an attenuated pulsed laser at 1552 nm and an intensity and phase modulator. The generated states were chosen by Alice and Bob independently from the set $|\psi_{A,B}\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. By choosing between three intensity levels, vacuum, a decoy state level and a signal state level, the decoy state protocol was implemented. Both transmitters were synchronized by a master clock located at Charlie which was optically transmitted to the respective stations through another deployed fiber. After receiving the photons Charlie performed a Bell state measurement by superimposing the pulses at a balanced beam splitter and detecting the outputs with gated InGaAs single photon detectors with 10 μs dead time. If the two detectors coincidentally clicked within 1.4 ns the states were projected into a Bell state. Those instances were publicly announced by Charlie.

The second group implemented the protocol over 50 km in the lab [301]. They implemented a similar qubit time-bin encoding scheme as in the Calgary experiment, but used four decoy intensity levels with 0, 0.1, 0.2 and 0.5 photons per pulse on average. A pulsed laser was fed through an unbalanced Mach-Zehnder interferometer to generate two time-bin pulses. The encoding of qubits and decoy were implemented with three amplitude and one phase modulator situated in a thermostatic container for

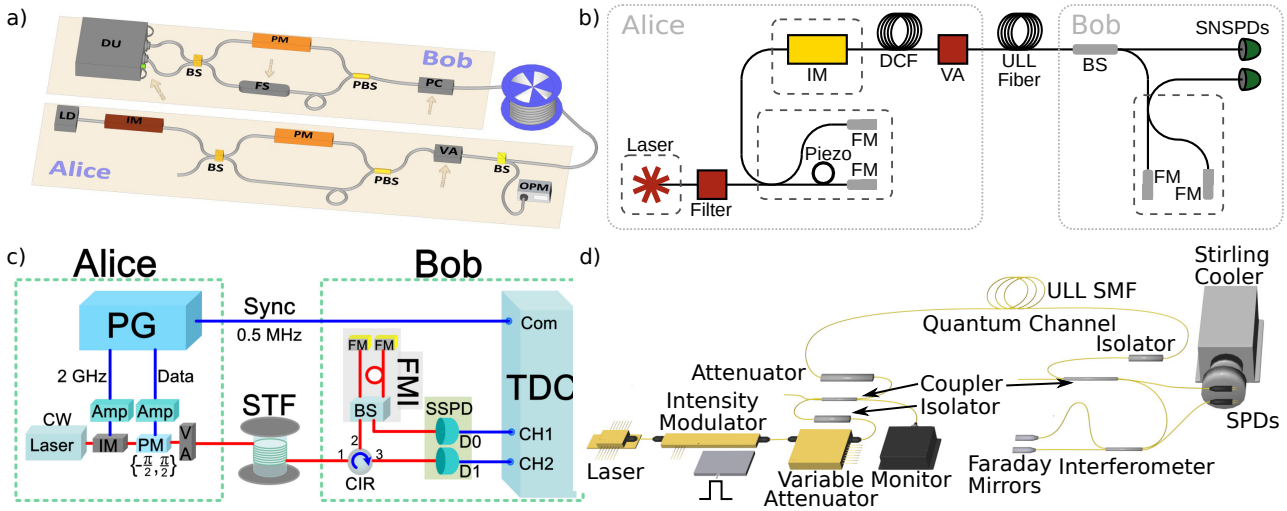

FIG. 4. Experimental implementations of discrete-variable QKD. a) Two-decoy state BB84 protocol with biased basis choice reported in Ref. [280]. A laser diode emitted pulses at 1550 nm which were intensity modulated (IM) to generate the different intensity of the states. An unbalanced Mach-Zehnder interferometer with a phase modulator (PM) in one arm was used to generate the different BB84 states, i.e. 0 and π for the Z basis and $\pi/2$ and $3\pi/2$ for the X basis. After attenuation to the single photon level with a variable attenuator (VA), the states were transmitted through a fiber. At Bob's side decoding was performed with an identical Mach-Zehnder interferometer and a PM either set to 0 or π. A fiber stretcher (FS) matched the two interferometers. The detection unit (DU) consisted of two InGaAs APDs. BS: Beam Splitter, PBS: Polarizing Beam Splitter, OPM: Optical Power Meter, PC: Polarization Controller. b) Simplified one-decoy state BB84 protocol with three states implemented over 421 km [281]. Alice uses a phase randomized laser pulse with a repetition rate of 2.5 GHz which is tightly bandpass filtered around 1550 nm. The pulses pass through an unbalanced Michelson interferometer with 200 ps delay made of beam splitter and two Faraday mirrors (FM) and a piezo in one of the arms to control the phase, to enable time bin encoding. Afterwards the pulses are intensity modulated (IM) to generate the different qubit states. After dispersion compensation (DCF) and attenuation to the single photon level (variable attenuator: VA), the pulses are transmitted through an ultra-low-loss (ULL) fiber. To implement the different bases choices at Bob's station the pulses are split with a beam splitter. One of its outputs is directly detected with an SNSPD, measuring the arrival time in Z basis which is used for the raw key. The other is used to measure the X basis by passing the pulses through an unbalanced interferometer identical to Alice's. This measurement is used to estimate the eavesdropper information. c) Implementation of the differential phase shift (DPS) protocol reported in [282] over 260 km with a rate of 2 GHz. A continuous wave (CW) laser at 1560 nm is chopped into pulses with an intensity modulator (IM). A phase modulator then randomly applies a $\pi/2$ or $-\pi/2$ phase shift on the pulses before they are attenuated to the single photon level. The pulses are then transmitted through standard telecom fiber (STF). At Bob's side the encoded information is decoded by a Faraday Michelson interferometer (FMI) which interferes a pulse with the one before and after it. The two outputs of the interferometer were detected by superconducting single photon detectors (SSPD). TDC: time to digit converter. d) Coherent one-way protocol implementation over 307 km with a repetition rate of 625 MHz reported in [283]. Pulses were carved into a CW laser beam at 1550 nm using two different intensities to encode bits using consecutive time bins. After attenuating to the single photon level the pulses were sent through an ultra-low loss (ULL) single mode fiber (SMF). Bob's receiver is similar to the receiver described in b). All figures are adapted with permission from: Ref. [280] ©OSA (2013), Ref. [281] ©APS (2018), Ref. [282] ©OSA (2012), and Ref. [283] ©NPG (2015).

stability reasons. After traveling through 25 km of fiber the untrusted relay Charlie performed a Bell state measurement identically to described above. The employed photo detectors used an upconversion technique where a nonlinear process in periodically poled lithium niobate converted the 1550 nm photons to 862 nm detected by Silicon avalanche photo detectors with a dark count rate of 1 kHz.

The third implementation [302] was a proof-of-principle demonstration based on polarization qubits instead and demonstrated MDI-QKD over 8.5 km long fiber links between the two trusted parties and the relay. Using a CW laser pulses were carved with an amplitude modulator. The decoy state levels were chosen by variable optical attenuators and the polarization encoding was performed with an automatic polarization controller. The relay was built from a balanced beam splitter and two polarization beam splitters. Four gated InGaAs avalanche single photon detectors with a dark count probability of 15 ppm and 10 μs dead time detected their output.

The distance of MDI-QKD was then boosted to 200 km [303] and 404 km [304] using ultra-low loss fiber with an attenuation of 0.16 dB/km. To achieve such a large communication length of 404 km the MDI-QKD protocol was optimized to improve on the effects of statistical fluctuations on the estimation of crucial security parameters. The protocol consisted of four decoy states with three levels in the X basis and only one in the Z basis.

The probabilities for each was carefully optimized to obtain largest key rate. Five intensity modulators and one phase modulator was employed to implement those. The receiver was implemented in the same way as described above for the first two experiments. Superconducting single photon detectors improved the quantum efficiency (about 65%) and dark count rate (30 Hz). Furthermore to achieve 404 km in the order of 10^{14} successful transmissions were recorded which took with a clock rate of 75 MHz over 3 months. The achieved secret key rate was 3.2×10^{-4} bits per second.

Furthermore at zero transmission distance a secret key rate of 1.6 MBit/s was reached [305] by introducing a pulsed laser seeding technique to achieve indistinguishable laser pulses at 1 GHz repetition rate. The new technique where a master laser pulse is injected into a slave laser as a seed to trigger stimulated emission at a defined time yielded very low timing jitter and close-to-transform limited pulses.

To demonstrate MDI-QKD over quantum networks in star topology extending over 100 km distance, cost-effective and commercially available hardware was used to build a robust MDI-QKD system based on time-bin encoding [306]. Similar plug and play systems with time-bin or polarization encoding and different level of immunity against environmental disturbances have been implemented as well in other groups [307–311].

F. Twin-Field QKD

The promise of beating the fundamental rate-distance limit of a repeaterless QKD protocol using the TF-QKD protocol (see Sec. IV H) has an often overlooked practical advantage: the protocol can boost the secret key generation rate (possibly by multiple orders of magnitude), especially at long distances. Experimental demonstration of TF-QKD [54] has however been challenging because TF-QKD requires a steady interference between weak coherent pulses, sent by the two distant parties (Alice and Bob), at the intermediate node (Charlie).

Maintaining interefence with a high visibility proves to be the main challenge in the implementation of TF-QKD. The differential phase fluctuations that limits the interference visibility between Alice and Bob can be described to the first order by [54]

$$\delta\phi_{AB} = \frac{2\pi}{c}(\nu\Delta L + \Delta\nu L), \tag{103}$$

where ν is the optical frequency of the light sources used by Alice and Bob, L is the optical fiber length, and c is the speed of light in the fiber. As evident from the equation above, there are two sources of phase fluctuations that must be compensated. The first term represents the phase difference due to fluctuations in the optical fiber length and the second term represents the phase difference due to the frequency mismatch between Alice's and Bob's lasers.

To overcome the fast phase drift in the optical fibers connecting Alice and Bob with Charlie, i.e., the first term in Eq. (103), laboratory demonstrations of TF-QKD, simulated with variable optical attenuator (VOA) [265] or fiber spools [258, 266, 267], include phase stabilization mechanisms. The phase stabilization schemes interfere bright reference pulses from Alice and Bob, and the error signals from the measurements are fed back to phase modulators that compensate for the differential phase between the two channels. This experimental challenge can be demanding in a field test where the parties are separated by long optical fibers that are exposed to environmental stresses, such as temperature or vibrations, in the field.

As for the frequency difference between Alice's and Bob's lasers, i.e., the second term in Eq. (103), all laboratory demonstrations of TF-QKD include an optical phase-locked loop (OPLL) that either directly interfere Alice's and Bob's lasers directly [265–267] or indirectly interfere their lasers with a third reference laser [258]. The interference is performed through an optical channel parallel to the main quantum transmission channel, and the error signals generated are used to modulate the cavity of Alice's and Bob's lasers, so that their light sources have a constant frequency offset (that is as close to zero as possible). Initial demonstrations of the OPLL systems [258, 265, 266] have relied on short optical fiber connections between Alice and Bob that can be unrealistic once they are in remote locations. Recent demonstration [267] showed that the fast phase fluctuations of an OPLL with optical fiber lengths similar to that of the quantum channels can be compensated with fast readout and feedback circuitry.

To date, proof-of-principle TF-QKD experiments have been demonstrated within the confines of a laboratory. As the protocol is of considerable interests to both QKD theorists and experimentalists, we expect that TF-QKD will be demonstrated in a field test setting in the near future. The protocol can be used to generate secret keys at a faster rate for QKD systems placed hundreds of kilometers apart.

G. High-dimensional QKD

Most DV QKD schemes encode quantum states in qubits ($d = 2$), such as the polarization states used in the first QKD experiment [312]. Going back to the early 2000s, there has been considerable interest in developing large-alphabet DV QKD schemes that encode photons into qudits: high-dimensional basis states with $d > 2$. Such schemes offer the ability to encode multiple ($\log_2 d$) bits of information in each photon. This benefit is not without a drawback; the information density per mode decreases as $(\log_2 d)/d$. Nevertheless, high-dimensional QKD (HD QKD) can offer major advantages over their qubit counterparts.

HD QKD can increase the effective secret key genera-

tion rate when this rate is limited by the bandwidth mismatch between the transmitter and the receiver. This mismatch happens when either the transmitter is limited to a flux below the available receiver bandwidth or the single-photon detector is saturated by the high photon flux received. While the former does not typically occur with attenuated laser source, the latter often arises due to detector dead time. In a SNSPD, the dead time is dominated by the time it takes to recover its supercurrent (which flows with zero resistance)—during which the nanowire is insensitive to any photon [313].

Fig. 5 shows a representative plot of qubit-based DV QKD secret key rate versus distance for currently achievable parameters. Three distinct regimes are apparent: regime II denotes normal operation where the secret key rate scales as the transmissivity in the fiber, which decays exponentially with distance. At longer distances, we enter regime III where the received photon rate is comparable to the detectors' background rate—masking any correlation between the key-generating parties and abruptly reducing the secret key rate. However, at short distances with low photon loss (regime I with distances up to $\sim$ 100 km), the secret key rate is limited due to the detector dead time. The highest QKD key rate is achieved in this regime and it currently amounts to 13.72 Mb/s [314]. To increase this key rate further, more detectors could be added so to distribute the initial intensity among them. Another strategy would be increasing the dimensionality of the alphabet to reduce the transmitted photon rate until the detectors are just below saturation. To date, multiple degrees of freedom have been investigated for high-dimensional QKD, including position-momentum [315], temporal-spectral [316–321], distributed-phase-reference [322, 323], and orbital angular momentum (OAM) [324–326].

Initial security analysis by Cerf *et al.* for discrete large-alphabet QKD showed improved resilience against noise and loss [327] (see also Refs. [328, 329]). HD QKD with discrete quantum states is capable of tolerating error rates than the 11% limit for qubit-based protocols. However, the proposed scheme with its two early proposals—one using OAM and another using temporal-spectral encoding—was challenging to demonstrate. The main difficulty lies in the measurement of discrete high-dimensional states within at least two mutually unbiased bases. Efficient implementation of the scheme for the two proposed degrees of freedom required single-photon detectors that scale with the dimensionality d—prohibiting the use of large d. Therefore, there has been a strong desire in developing HD QKD schemes with the ability to measure higher-order correlations using only a few single photon detectors.

One detector-efficient temporal scheme—borrowing techniques from CV QKD and applying them to the temporal-spectral mode—demonstrated QKD operations with an extremely high alphabet of $d = 1278$, i.e., over 10 bits per photon [321]. However, no security proof against collective or coherent attacks was available at the

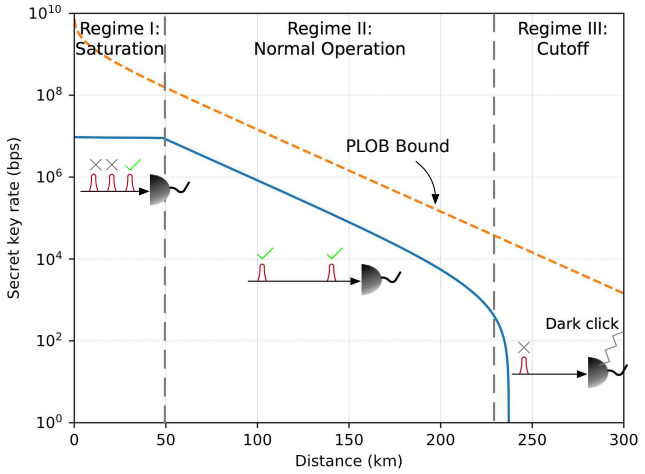

FIG. 5. Representative plot of secret key generation rate against channel distance for a traditional qubit DV QKD protocol for currently achievable device parameters. The plot assumes a 1 GHz clock rate, a 93% detector efficiency, a 1000 cps dark count rate, and a 100 ns detector dead time. We denote three distinct regimes: I. Short metropolitan-scale distances, where the secret key rate is limited by detector saturation (here the top-left plateau is about 13 Mb/s [314]); II. Longer distances, where the secret key rate decays exponentially with distance; III. Extremely long distances, where the secret key rate is sharply limited by detector dark count rates. The PLOB bound [43] is plotted for comparison.

time. The challenge is that time and energy states are not inherently discrete, but rather they form a continuous basis. Therefore, the security proof on discrete dimensional bases do not transfer directly to these continuous-basis schemes. Considerable effort was made to extend the proofs for CV QKD to HD QKD by realizing that the security of temporal-spectral HD QKD can be guaranteed by measuring the covariance matrices between Alice's and Bob's information.

Measuring the covariance matrices involves detection in the frequency basis. Direct spectral detection of the incoming light can be done using a single-photon-limited spectrometer: a spectral grating followed by d single photon detectors. However, the required number of detectors would again prevent reaching a large dimensionality. To work around these limitations, new techniques were introduced to convert the spectral information to time information by using group-velocity dispersion [330], Franson interferometers [331], or a time-varying series of phase shifts [319].

The development of temporal-spectral encoded HD QKD spurred record demonstrations of secret key capacity at 7.4 secret bits per detected photon [332] and secret key generation rates of 23 Mbps [333] and 26.2 Mbps [334] with $d = 16$ at 0.1 dB loss and $d = 4$ at 4 dB induced loss, respectively. Furthermore, a 43-km (12.7 dB loss) field demonstration between two different cities show a maximum secret key generation rate of 1.2 Mbps [333].

Since HD QKD is vulnerable against photon number splitting attacks as it relies on transmission of single photons, these demonstrations make use of decoy state techniques to close this security loophole [335]. More recently, the security of temporal-spectral HD QKD has been extended to include the composable security framework, which takes into account statistical fluctuations in estimating parameters through only a finite number of measurements [336, 337].

High-dimensional QKD with OAM has also witnessed rapid development due as it is directly compatible with free-space QKD systems [338]. Since OAM modes rely on the preparation and the measurement of discrete high-dimensional states, the security proofs extend directly from the work by Cerf *et al.* Recently, the security proof has also been successfully extended to include finite-key analysis for composable security [339].

A photon carrying an OAM information has a helical or twisted wave front with an azimuthal phase φ which wraps around ℓ (helicity) times per wavelength. For the popular Laguerre-Gauss mode, a photon carrying an $\ell\hbar$ OAM can be described as $|\Psi_Z^\ell\rangle = e^{i\ell\varphi}$. ℓ is an unbounded integer, which allows arbitrarily high encoding dimension, but practically one limits $\ell \in [-L, L]$ to achieve a dimensionality $d = 2L+1$. A mutually unbiased basis set can be constructed using a linear combination of OAM modes

$$|\Psi_X^n\rangle = \frac{1}{\sqrt{d}} \sum_{\ell=-L}^{L} \exp\left(i\frac{2\pi n\ell}{d}\right) |\Psi_Z^\ell\rangle. \tag{104}$$

Both sets of quantum states can be generated using a spatial light modulator (SLM) [340], a digital micro-mirror device (DMD) [341], or a tunable liquid crystal device known as q-plates [342, 343].

The first laboratory demonstration of high-dimensional OAM QKD achieved a secret key generation rate of 2.05 bits per sifted photon using a seven-dimensional alphabet ($L = 3$ and $d = 7$) [325]. More recently, a 300-m free-space field demonstration in Ottawa with four-dimensional quantum states achieved 0.65 bits per detected photon with an error rate of 11%: well below the QKD error rate threshold for $d = 4$ at 18% [324]. Although moderate turbulence was present during the experiment, going to longer distances will require active turbulence monitoring and compensation [344]. Very recently, high-dimensional OAM QKD, in the form of a multiplexed BB84 protocol, has been further investigated with the use of air-core fibers [345].

The main challenge in high-dimensional OAM QKD towards achieving a high secret key generation rate is the relatively low switching speed of the encoding and decoding devices when compared to the multi-gigahertz-bandwidth electro-optic modulators used in time-bin encoded high-dimensional QKD. QKD demonstrations involving SLM, DMD, and q-plates so far have required a time in the order of 1 ms to reconfigure—limiting the QKD clock rate in the kHz regime. While q-plates can potentially be operated at GHz rates by using electro-optic tuning, these have yet to be demonstrated [346]. One appealing new direction is the use of photonic integrated circuits (PICs), which may dramatically reduce the configuration time. Thermo-optically tuned on-chip ring resonators have demonstrated a switching time of 20 μs [347, 348]. More recently, precise control of OAM mode generation has been demonstrated using a 16×16 optical phase array which allows for generation of higher fidelity OAM states [349]. Furthermore, large scale on-chip micro-electro-mechanical-system (MEMS) actuation has also been demonstrated with a switching time of 2.5 μs with the potential of application to OAM generation and control [350].

Demonstrations of HD QKD using a single set of conjugate photonic degrees of freedom, such as time-energy or OAM, to increase the secret key generation rate have been successful. Investigation in new techniques, which include the miniaturized photonic integrated circuit platform (see Sec. V H), to manipulate and detect multiple degrees of freedom simultaneously can dramatically increase the dimensionality that would improve the secret key rate even further. Moreover, a more detailed study into the choices of degrees of freedom and the choice of mutually unbiased bases can shed light into which means of encoding is most robust for the different QKD settings. For example, it has been hinted that the Laguerre-Gauss OAM modes show greater resilience to cross talk in turbulent environments than the Hermite-Gaussian OAM modes [351]. With the potential of high-dimensional QKD systems generating secret keys at rates commensurate to those of data communication rates, further study into HD QKD in a measurement-device-independent configuration is warranted. HD QKD and, more generally, high-rate QKD is a very active experimental area, and our discussion is clearly not exhaustive of all the contributions [352–358].

H. Photonic integrated circuits

QKD devices have more demanding requirements than those offered by standard off-the-shelf telecommunication equipments. QKD transmitter needs single photon sources or weak coherent sources modulated at an extremely high ($\geq$ 20 dB) extinction ratio for low-error QKD operations. Furthermore, quantum-limited detectors such as single photon detectors or shot-noise limited homodyne detectors are also required on the receiver side.

Photonic integrated circuits (PICs) provide a compact and stable platform for the integration of multiple high-speed quantum photonic operations into a single compact monolithic circuit. PICs allow experimentalists to engineer quantum devices in the different material platforms at lithographic precision to meet the stringent requirements of QKD devices. The amount of complexity that can be achieved with PICs has been shown

to enable practical implementation of wavelength multiplexing for higher secret key rates [359, 360], space-division multiplexing for standard and high-dimensional QKD [361, 362], multi-protocol operations for flexibility [363], and additional monitoring and compensation capabilities against timing and polarization drifts in the channel [364]. Various material platforms have been explored for building high-performance QKD devices—each with its own strengths and weaknesses. (See [365] for further discussion of the different material platforms.)

Active III–V laser materials, such as indium phosphide (InP), is a promising platform for QKD transmitters because of the availability of gain laser medium for producing weak coherent light [366]. The InP platform also has the advantage of building quantum well structures using other ternary and quaternary III–V semiconductors that are lattice-matched to InP, such as InGaAs, InGaAsP, or InAlAsP [367]. Within these quantum wells, carriers—electrons and holes—are confined within the resulting one-dimensional potential wells. Applying electric field to the well shifts the energies of the carriers, which in turn changes its absorption spectrum and its refractive index shift. This process, named quantum-confined Stark effect (QCSE) [368], is the strongest electro-optic modulation available in the platform—albeit with the undesirable phase-dependent loss. Intensity and phase modulation with QCSE has been demonstrated to achieve high extinction ratio beyond 50 dB at bandwidths $\geq$ 40 GHz [369]. InP allows to have all the optics integrated on a single chip and fully integrated links with real fibre. This platform was used in Ref. [370] that implemented, for the first time on chip, the laser-seeding technique of Ref. [371] achieving very high secret key rates.

The SiO_2-Si_3N_4 TriPleX technology has record low loss passive components at $\sim 10^{-4}$ dB/cm [372] which makes it an attractive platform for time-based or phase-based QKD receiver components in high-speed gigahertz-clocked QKD operations, where Bob has to interfere weak coherent pulses spaced by ~ 1 ns. The combination of low propagation loss and high interference visibility and stability can enable Bob to maintain low error-rate QKD operations without sophisticated stabilization circuitry typically required for fiber- based or bulk optical interferometers [363]. The TriPleX platform, however, relies solely on thermo-optic phase modulation which is slow (with $\sim$MHz bandwidth) for high-speed QKD operations.

Silicon photonics recently has gained traction as the leading platform for quantum communications with the promise of its high density integration with the existing complementary metal-oxide-semiconductor processes that have enabled monolithic integration of both photonic and electronic components. With no natural electro-optic nonlinearity, silicon photonics rely on the slow thermo-optic phase modulation [373] to achieve high-visibility interference [374]. Carrier injection and depletion within an intrinsic region between p-doped and n-doped silicon offer high-speed modulation within silicon photonics, but with a phase-dependent loss that must be mitigated [375, 376]. Recently, MEMS-based phase shifters have shown great promise in miniaturizing the device further, in lowering the power consumption, and in achieving gigahertz-bandwidth phase shifts without the undesirable phase-dependent loss [377].

While the development of a fully integrated light source within the silicon photonics platform is still underway, the platform has been proven to be highly amenable to heterogeneous bonding of the active III–V materials mentioned above [378–382]. Moreover, SNSPDs have been integrated into silicon photonics using a pick-and-place method, paving the way for a possible monolithic compact QKD receiver with single photon counting capabilities [383]. Quantum-limited homodyne detectors have also been demonstrated with sufficiently large noise clearance between shot noise and electronic noise that can be useful for CV QKD applications [384, 385].

A recent demonstration of QKD with PIC uses an InP transmitter to leverage its on-chip source capability and a TriPleX to leverage its low-loss performance. The experiment showcased PIC's flexibility in being able to demonstrate multiple time-bin encoded protocols using the same chip set at a clock rate of one GHz [363]. More recently, recent demonstrations of time-bin and polarization QKD transmitters in silicon photonics with further miniaturized components hinted at possible performance advantage over off-the-shelf fiber optical components with $LiNbO_3$-based modulators [386, 387]. Silicon photonics recently proved possible QKD operations using polarization encoding over a 43-km intercity fiber link which was commonly thought too unstable because of fiber polarization drifts [364]. The experiment demonstrated secret-key rate generation comparable to state-of-the-art time-bin demonstrations but with polarization stabilization capabilities. See Fig.6.

The PIC platform also offers new methods of generating quantum sources of light: single photons and entangled photon sources. While weak coherent light is currently the most popular approach for QKD operations, its Poissonian statistics create side-channel vulnerability that must be closed with decoy state approaches [159–163]. QKD with true single photons or entangled photons can circumvent this problem without needing decoy state protocols [37], which consume random bits. In the InP platform, single photons can be generated from quantum dots that are grown epitaxially to emit light in the standard telecom 1550 nm window. In silicon photonics, on-chip entangled pair sources based on spontaneous four-wave mixing (SFWM) have been demonstrated without the need of any off-chip filtering [388, 389].

One important challenge that remains in these novel quantum sources is in increasing the brightness to be sufficient for gigahertz-clocked QKD operations. Currently, the amount of output flux of these quantum sources has been limited at ~ 10 MHz even at near unity collection efficiency [390, 391]. These quantum sources are typically pumped using a coherent laser. Increasing the pump power of the quantum dot sources induces multi-photon

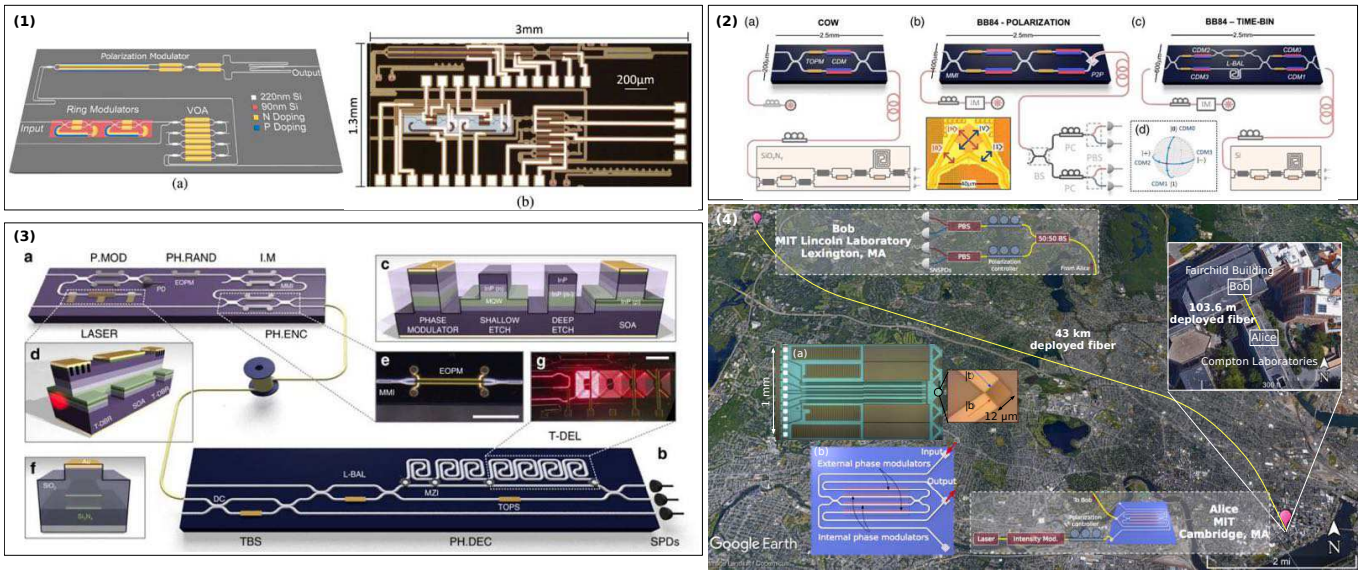

FIG. 6. Experimental demonstrations of QKD using PICs. (1) (a) Schematic and (b) micrograph of the silicon photonics polarization QKD transmitter. The full transmitter consists of ring pulse generators, a variable optical attenuator (VOA), and polarization controller [387]. (2) Schematic of integrated silicon photonics QKD transmitters for (a) coherent-one-way (COW) protocol, (b) polarization BB84 protocol, and (c) time-bin BB84 protocol [386]. (3) (a) Schematic of the InP QKD transmitter, which combines a laser, pulse modulator, phase randomization, intensity modulator, and phase encoder. (b) Schematic of the TriPleX QKD time-bin receiver, which either immediately sends the signal for direct detection or interferes the signal before sending it to detectors. Cross-section of (c) InP PIC, (d) laser in InP PIC, and (f) TriPleX PIC. (e) and (g) are micrographs of the PICs [363]. (4) Aerial view of the intercity polarization QKD field test between the cities of Cambridge and Lexington and the local field test between two adjacent buildings. Insets: (a) Micrograph and (b) schematic of the polarization silicon photonics QKD transmitter used [364]. ©Google. Map data from Google, Landsat/Copernicus. All figures are adapted with permission from: Ref. [387] ©OSA (2016), Ref. [386] ©OSA (2017), Ref. [363] ©NPG (2017), and Ref. [364] ©APS (2018).

emissions which degrade the single photon purity. However, alternative schemes of excitation have shown great promise of reducing the probability of multi-photon emissions by several orders of magnitude [392]. Increasing the pump power of the entangled SFWM sources has been shown to induce two-photon absorption which saturates the source brightness [393].

Integrated photonics is poised to deliver major benefits towards building QKD networks. The miniaturization of devices coupled with highly robust manufacturing processes can accelerate the adoption of QKD for real-world data encryption, especially with the MDI configuration. In this setting, only several central receiver nodes need to have cryogenic high-efficiency SNSPDs [394], while all the clients can make use of personal PICs to generate secret keys among each other. The lithographic precision afforded by the platform also promises the possibility of identical integrated light sources for MDI-QKD [395, 396].

In conclusion, PIC presents a novel opportunity to design new devices that meet the needs of low-error QKD operations. Investigations into new device physics through heterogeneous integration of the multiple platforms can enable the development of new quantum sources and receivers with superior performance [397]. Furthermore, PIC's phase stable platform also lends itself to highly-dense-multiplexed QKD operations, which can dramatically increase the secret-key generation rate.

VI. SATELLITE QUANTUM COMMUNICATIONS

A. Introduction

The quantum communication protocols on which QKD is based are very well suited to be applied in space. Space channels, in connection with ground single-links and networks, may be exploited in a number of scenarios embracing the entire planet Earth, the satellite networks around it and novel and more ambitious projects aimed at more distant links with the Moon or other planets. In the context of an evolving society that leverage more and more on secure communications, space is expected to play a crucial role in quantum communications as it is now playing for global communication, navigation and positioning, time distribution, imaging and sensoring, realized by several generation of satellites.

B. The satellite opportunity

The extension of the QKD to secure links to long distance, to connect nodes of networks spanning large scales, including national, continental, planetary as well as space missions, was devised in feasibility studies more than a decade ago [398–402]. The extension to space of quantum communication (QC) was initially proposed in combination with experiments devoted to testing fundamental principles and resources of quantum information in the novel space context. Some of these were directed to the development of a payload for the International Space Station (ISS) [403, 404], others as standalone satellites [399].

These proposals were supported by the early evidence of long distance free-space QC experiments on the ground [405–407]. In this way it was proved that significant portion of atmosphere paths were suitable not only for classical optical communications but also for the quantum one. Indeed, the degrading role of the atmosphere on the channel performances was already assessed in terms of beam widening and wandering, fading of signal and scintillation at the receiver as a function of the turbulence level, wavelength and link length [408, 409]. However, the single photon discrimination at the correct wavelength, arrival time and direction as well as the detection with an effective rejection of the background noise is more demanding than the classical counterpart.

Starting in 2003 with an experimental campaign at the Matera Laser Ranging Observatory (Italy), it was possible to demonstrate that the exchange of single photons are suitably achievable between a Low-Earth-orbit (LEO) satellite and the ground [410]. In this case, even without an active photon source in orbit, the demonstration was obtained by exploiting satellites equipped with optical retroreflectors, and directing to them a train of pulses with calibrated energy such that the collected portion that is retroreflected back toward the transmitter on the Earth is a coherent state with a content of a single photon or less. A suitable bidirectional telescope on the ground allows for the transmission of the uplink train of pulses and of the single photons in downlink. This technique was then extended to demonstrate QC using different degrees of freedom, as later discussed [411, 412] and is a candidate for QKD with a very compact payload [411].

The application of space QC for a global QKD was considered since the beginning as an effective solution to joint separate networks of fibre-based ground links. Indeed, the key exchange between a trusted satellite and two ground terminals may then be used to generate a secure key between the two terminals via one-time pad. Despite these attracting opportunities for the improvement of secure communications on ground, as well as other that have been conceived for the use in space (described below), the realization of a satellite for QKD was kept on hold in Europe and USA and found at the beginning of this decade a concrete interest in Asia. More in detail China and Japan put in their roadmaps the demonstration of the space QKD with ambitious but concrete plans to develop and launch satellites for QC. The Japanese SOTA satellite was indeed launched in 2014 and Chinese Micius in 2015, as will be described below. The perspective of using a very compact payloads as nanosat o cubesat has recently vamped the European initiatives, spurring for the development of space components of great efficiency and small dimension [413, 414]. Such direction is expected to be beneficial for the ground QKD as well, for the realization of high performance small components to be used in compact and power-saving QKD terminals on ground networks.

C. Type of orbits and applications

The type of key exchange provided by an orbiting terminal changes significantly with the type of orbit. The altitude has relevant implications in the losses of the optical link. Although the possible configuration of a space QKD setup could use the transmitter in both the space terminal (downlink of the qubits) and the ground terminal (uplink), the detrimental impact of the atmosphere is asymmetric. Indeed in the uplink, the propagation of the wavefront associated to the qubit stream in the turbulent atmosphere occurs at the beginning of the path. This induce a non uniform modulation of the wavefront phase. The subsequent propagation results in the development of an amplitude modulation at the satellite altitude, with a significant beam diameter broadening and a scintillation that causes a fluctuation of the link transmissivity. On the contrary, in the downlink the propagation of the qubit train occurs in vacuum and get degraded by the atmosphere only in the final portion, with an exponential air density increase within the last 10 km. The broadening of the beam at the receiving terminal is then mainly due to the diffraction and the scintillation is also reduced. Therefore the downlink is the common configuration, and the subsequent analysis will be referred to it.

1. *Space-link losses*

The evaluation of the QKD rate in a space link is based on the analysis of the losses and the fluctuations of the corresponding optical channel. From classical studies in satellite optical communications [409], we know that the geometric losses (namely the losses due to diffraction) may be modeled considering, at the transmitter, a Gaussian beam with waist w_0 passing through a telescope aperture of diameter D. The far-field distribution at distance $d \gg D$, can be written in terms of the coordinates (x, y) of the plane transverse to propagation as

$$E(x,y) \propto \frac{D}{2a} \int_{X^2+Y^2 \leq 1} e^{\left[i\frac{2\pi}{\lambda}\frac{D}{2d}(xX+yY)-\frac{X^2+Y^2}{a^2}\right]} \mathrm{d}X\mathrm{d}Y, \tag{105}$$

where $a = 2w_0/D$ is the ratio between the beam waist and the Tx aperture radius. As first obtained by Sieg-

man [415], to optimize the received power it is necessary to choose $a \simeq 0.89$ for classical communication. However, for QKD we may use different values if we consider the single-photon regime after the Tx aperture. By using $a \simeq 2$ we obtain in the far-field (at distance d from the transmitter) a beam which is well-approximated by a Gaussian beam with radius $w(d) \simeq 0.9\frac{\lambda}{D}d$. The total losses of the channel is evaluated in dB as $\simeq -10\log_{10}\frac{D^2}{2w^2(d)}$ by assuming a receiver aperture with equal diameter D.

In Fig. 7 we show the expected losses with a selection of significant wavelengths and telescope diameters as a function of the terminal separation. The range of losses is radically different according to the orbit altitude, conditioning the possible applications. In the classification below, we discuss the roles played by the different satellites and types of orbits for the purpose of QC.

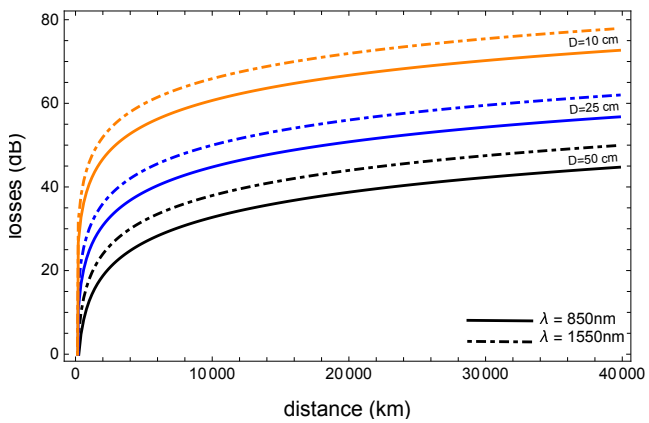

FIG. 7. Space-link losses for an optimized beam waist w_0 at the transmitter, different telescope diameters D, and two relevant wavelengths for space QKD, i.e., $\lambda = 850$nm (solid line) and $\lambda = 1550$nm (dotted-dashed line).

2. *LEO satellites*

This type of orbit, reaching not above the altitude of 2000 km, was the first choice to demonstrate QC protocols from space. This is because of the relative ease to reach the orbit with multiple launcher options combined with the lower exposition to the aggressive ionizing radiation affecting higher altitudes. The rapid round-trip time around Earth of about one to two hours combined with a wide selection of orbit inclinations, open possibilities so as to cover all the planet in hours with a single sat or to maintain a constant position relative to the Sun. Among the limitations of LEO there is the fact that the passage over a ground terminal is limited to just a few minutes of effective link, whereas the sat is above the 10 degrees of elevation from the horizon. Moreover, satellite speed relative to ground may reach 7 km/s for a 400-km orbit, like that of the ISS, which causes a varying Doppler shift of the order of tens of GHz.

LEO sats for QKD were the first to be considered [403, 416], initially as payload to be operated on the ISS for six months to one year, and then as independent spacecrafts. Ajisai, a LEO sat devoted to geodynamic studies, was used as the first source of single photons in orbit using its corner-cube retroreflectors. These were illuminated by a train of pulses from the Matera Laser Ranging Observatory (MLRO, Italy) in such a way that a single photon was reflected on average by the satellite [410]. This approach was later used with 4 satellites equipped with polarization preserving retroreflectors to realize an orbiting source of polarization qubits, providing the experimental feasibility of the BB84 protocol on a space-link [411]. See Fig. 8. The QBER observed was well within the applicability of the BB84 protocol, and in line with criteria of both general or pragmatic security [417]. Later and still at MLRO, the use of temporal modes, or phase encoding, was also demonstrated [412]. Theoretically, it is worth to mention previous works on the feasibility of the BB84 protocol in turbulent channels, both terrestrial [418] and between satellite and ground [419].

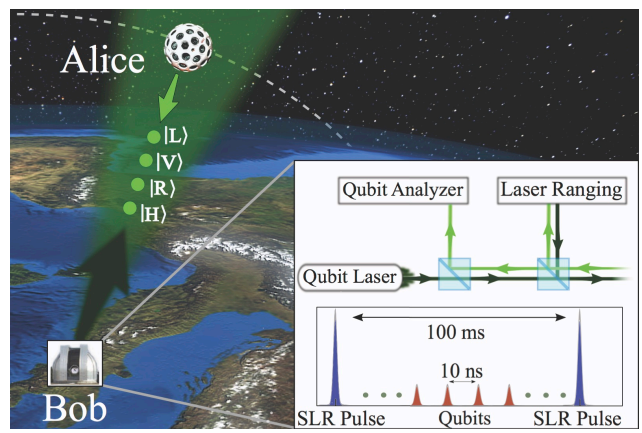

FIG. 8. Satellite QKD demonstration. A train of qubit pulses is sent to the satellite with a repetition rate of 100 MHz. These are reflected back from the satellite at the single photon level, therefore mimicking a QKD source. In order to achieve synchronization the experiment also employed a train of bright satellite laser ranging (SLR) pulses at a repetition rate of 10 Hz. Reprinted figure with permission from Ref. [411] ©APS (2015).

The Chinese satellite Micius was announced as a major step of the space program of the Chinese Academy of Science [420] and was launched on the 16th of August 2016. It provided the experimental verification of various QC protocols in space. Indeed the spacecraft was equipped as a quantum optics lab capable not only to generate coherent and entangled states and to transmit them to the ground but also to measure qubit sent by the ground terminal. In this way, ground-to-satellite quantum teleportation was realized by teleporting six input states in mutually unbiased bases with an average fidelity of 0.80 ± 0.01 from the Ngari ground station in Tibet [421]. The decoy-BB84 protocol was realized with

a key rate exceeding 10 kbps at about the central part of the satellite passage. This remarkable result was possible by very accurate pointing of the downward beam, whose far field angle was about 10 μrad at $1/e^2$ and the pointing fluctuation was reported to be a factor five lower [422]. The wavelength for the qubit was chosen to be about 850 nm and the observed losses were about 22 dB, in line with the theoretical modeling based on a 300-mm telescope.

Entangled-based QKD was also demonstrated by Micius, using a high visibility source onboard. The twin beam downlink was used to establish a secret key (via violation of Bell inequalities) between the two stations of Delingha and Lijiang, with a slant distance of about 1200 km [423]. Due to the composition of the losses of the two channels, the QKD rate resulted of the order of half a bps. In 2017, entangled-based QKD (in particular, the Ekert protocol [114]) was also realized with one of the entangled photons measured at the satellite while the other one was detected at the receiver in the Delingha ground station. The link losses ranged from 29 dB at 530 km to 36 dB at 1000 km, allowing for a max key rate of a few bps [424]. Remarkably, Micius was also used for demonstrating the first intercontinental quantum network, distributing keys for a text and video exchange between the ground stations of Xinglong (China), Nanshan (China) and Graz (Austria) [79].

In 2017, QKD was also demonstrated in downlink from the Tiangong-2 Space Lab, where a compact transmitter with a 200-mm telescope was installed. Photons were transmitted down to the 1.2-m telescope at the Nanshan ground station [425]. The key rate was assessed to reach beyond 700 bps with about 30 dB of losses. In the same year, a Japanese team at the National Institute of Information and Communications Technology developed the SOTA lasercom terminal for testing the optical downlinks as well as QC with a low-cost platform, the microsatellite SOCRATES at an altitude of 650 km [426].

Since the beginning of this decade, the cubesats have grown rapidly in the several areas of space science and technology, including space QC [413, 414]. Two main tasks are envisaged for such small sats: the test of novel technology for QC in the space context and the operation of a space network for capillary coverage of low rate QKD. For the first purpose, a team at the National University of Singapore developed a prototype of source and detector that was successfully operated first on a balloon and then in Space [427, 428]. Several proposals of cubesat use have been put forward worldwide (e.g., see [414]).

3. *Higher Earth orbits (MEO and GEO)*

The medium Earth orbit (MEO) is above LEO and below the geostationary orbit (GEO), the latter being at 35,786 km above Earth's equator. The MEO includes the Global Navigation Satellite Systems (GNSS) while GEO includes weather and communication satellites. These higher orbits are preferable because they would extend the link duration (becoming permanent for a GEO). However, they involve larger losses and the payloads are exposed to much more aggressive ionizing radiation from the Sun.

The first experimental single-photon exchange with a MEO sat at 7000 km of slant distance was realized in 2016 at MLRO [429]. The QKD links were modeled in previous studies [401, 402]. A recent result addressing the photon exchange with two Glonass sats has supported the future possibility of QKD-enabled secure services for the GNSS satellites [430]. This opportunity is seriously considered, given the critical service that the navigation system are playing in several continents. Finally, the feasibility of quantum-limited measurement of optical signal from an existing GEO communication satellite has been recently carried out [431].

4. *Night and day use of the link*

Space QKD was so far investigated experimentally during night-time only. However, the operation in daylight is of great interest for a significative expansion of the satellite usage. The possibility of a daylight use in intersatellite communication was supported by a study on the ground [432]. The key ingredients were a strong rejection of the background radiation, via a precise pointing and a narrow field-of-view, together with the reduction of the temporal integration interval for the arrival qubits, obtained by means of a very precise temporal synchronization. Finally, the wavelength of 1550 nm was used thanks to its lower scattering.

D. Beyond satellite QKD

Several areas may be found in which quantum communication from and in space are crucial. Below we review some possible other protocols (beyond QKD) that can be realized by sending single photons at large distance in space. We discuss some fundamental tests that were and can be realized in this context.

1. *Other protocols*

Some possible protocols that can be realized with long distance quantum communication are quantum digital signature (QDS) and blind quantum computing (BQC). A QDS refers to the quantum mechanical equivalent of a digital signature (see Sec. XV). In a QDS protocol, Alice sends a message with a digital signature to two recipients, Bob and Charlie. Then QDS guarantees nonrepudiation, unforgeability, and transferability of a signature with information-theoretical security. A very recent long-distance ground demonstration exploiting decoy states has been realized without assuming any secure channel.

A one-bit message was successfully signed through a 102-km optical fiber [433].

A second example is BQC where a client sends a quantum state $|\psi\rangle$ to the server, with such state encoding both the chosen algorithm and the input (for a review see Ref. [434]). For a cloud computer (an in particular a cloud quantum computer), the privacy of the users may be a serious issue. BQC allows a client to execute a quantum algorithm by using one or more remote quantum computers while at the same time keeping the results of the computation hidden. By satellite quantum communication it could be possible to send quantum states from a satellite to ground servers that may perform the BQC.

2. *Tests of quantum mechanics in space*

Quantum communication in free space at large distance not only is an unexplored scenario for implementing quantum information protocols [435–438] but it is also a natural setting to perform fundamental tests of quantum mechanics. Indeed, as for any scientific theory, quantum mechanics can be considered valid only within the limits in which it has been experimentally verified. By exploiting quantum communication in space it is possible to extend such limits, by observing quantum phenomena in unexplored conditions, such as moving terminals and/or larger and larger distances. The possibly interplay of quantum mechanics with general (or special) relativity can be studied in this context [439–444]. Bell's inequality with observers at relative motion and gravitational-induced redshifts on quantum objects are some very significant experiments that can be performed in space (for a detailed review of these possible experiments see [440]). As paradigmatic examples of the possibilities offered by space quantum communication we may recall two recent demonstrations: the violation of a Bell's inequality at a distance of about 1200km [423] and the Wheeler's delayed-choice experiment along a 3500-km space channel [445].

As we know, Bell's inequalities [446] demonstrate that a local hidden variable model cannot reproduce the experimental results that can be achieved by entangled states. Nowadays, Bell's inequality are used as a simple and effective tool to *certify* the presence of entanglement between separate observers. 'Cosmic' Bell tests have been proposed [447] and performed [448, 449], which are able to close locality while addressing the loophole of the 'freedom of choice' (or measurement dependence). Satellite Bell tests have also been conducted. In 2017, the Micius satellite, orbiting at an altitude of about 500km and hosting a source of polarization entangled photons, allowed the demonstration of the persistence of entanglement at the record distance of 1200km between the two ground station of Delingha and Lijiang in China [423]. The experiment realized the violation of the CHSH inequality, with a value $S = 2.37 \pm 0.09$ larger than the limit of 2 by four standard deviations. This result confirmed the nonlocal feature of quantum mechanics excluding the local models of reality on the thousand km scale.

Previous demonstrations using fiber or ground free-space links [407, 450] were limited to one order of magnitude less in distance, due to photon loss in the fiber or the Earth curvature for ground free-space links. On the other hand, by analyzing the experimental data from the main injector neutrino oscillation search (MINOS), Ref. [451] also showed another remarkable long-distance violation: neutrino oscillations were able to violate the Leggett-Garg inequality by 6 standard deviations over a distance of 735km (recall that the Leggett-Garg inequality is an analogue of Bell's inequality which is formulated in terms of correlations of measurements performed on a quantum system at different times).

Quantum mechanics predicts that quantum entanglement should be measured at any distance: however, it is tempting to challenge such prediction and verify if some unexpected effects (such as gravitational influence) will put some limits of such distance. The availability of quantum communication in space now allows to extend such limit at larger and larger distance. For instance, by using an entangled source on a GEO satellite that sends the two photons on ground, it would be possible to increase by one order of magnitude the distance between two entangled photons.

The second example is Wheeler's delayed-choice experiment [452], a wave-particle duality test that cannot be fully understood using only classical concepts. Wave-particle duality implies that is not possible to reveal both the wave- and particle-like properties of a quantum object at the same time. Wheeler's gedankenexperiment was invented to highlight the contradictory interpretation given by classical physics on a single photon measured by Mach-Zehnder interferometer (MZI). In his idea, a photon emerging from the first beam splitter (BS) of a MZI may find two alternative configurations: the presence or absence of a second BS at the output of the interferometer. In the former/latter case the apparatus reveals the wave/particle-like character of the photon. In a classical interpretation, one could argue that the photon decides its nature at the first BS. However, if the MZI configuration is chosen *after* the photon entered the interferometer (hence the name delayed-choice), a purely classical interpretation of the process would imply a violation of causality. Several implementations of Wheeler's Gedankenexperiment have been realized on the ground [453]. In the experiment of Ref. [454], a space-like separation between the choice of the measurement and the entry of the particle into the interferometer was achieved with a 48-m-long polarization interferometer and a fast electro-optic modulator controlled by a quantum random number generator (QRNG).

Then, in Ref. [439], the delayed-choice paradigm has been extended to space, by exploiting the temporal degree of freedom of photons reflected by a rapidly moving satellite in orbit. The two time bins represents the two

distinct paths of the interferometer. Photon polarization was used as an ancillary degree of freedom to choose the insertion or removal of the BS at the measurement apparatus and thus observe interference or which-path information. The experiment showed the correctness of the wave-particle model for a propagation distance of up to 3500 km, namely at a much larger scale than all previous experiments.

E. Concluding remarks

We have reviewed the opportunities offered by space quantum communications and their possible applications. In particular, they are expected to have a great impact in the creation of a secure quantum network around the globe. The design of a QKD network in space encompass the realization of the single-link connections, the modeling of their performances and their further exploitation in networks based on multiples ground stations. The study of such features needs further investigations both theoretically and experimentally.

VII. CONTINUOUS-VARIABLE QKD

A. Brief introduction to CV systems

We start by providing some basic notions on CV quantum systems and bosonic Gaussian states. Here, and in the following discussions on CV-QKD protocols, the variance of the vacuum state is set to 1. This is also known as the vacuum or fundamental shot noise unit (SNU) (an alternative choice for the value of the SNU is 1/2 as discussed in Appendix A). Recall that CV quantum systems are described by infinite-dimensional Hilbert spaces [7, 8]. In particular, we consider n bosonic modes of the electromagnetic field with tensor-product Hilbert space $\otimes_{k=1}^{n}\mathcal{H}_k$ and associated n pairs of field operators $\hat{a}_k^\dagger$, $\hat{a}_k$, with $k = 1, \ldots, n$. For each mode k we can define the following field quadratures

$$\hat{q}_k := \hat{a}_k + \hat{a}_k^\dagger, \quad \hat{p}_k := i\left(\hat{a}_k^\dagger - \hat{a}_k\right). \tag{106}$$

These operators can be arranged in an N-mode vector $\hat{\mathbf{x}} := (\hat{q}_1, \hat{p}_1, \ldots, \hat{q}_n, \hat{p}_n)^T$. Using the standard bosonic commutation relation, for field's creation ($\hat{a}_k^\dagger$) and annihilation ($\hat{a}_k$) operators, one can easily verify that any pairs of entries of vector $\mathbf{x}$ satisfy the following commutation relation

$$[\hat{x}_l, \hat{x}_m] = 2i\Omega_{lm}, \quad \Omega_{lm} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{107}$$

where Ω_{lm} is the symplectic form [7].

An n-mode quantum state can be represented either as a density operator $\hat{\rho}$ acting on $\otimes_{k=1}^{n}\mathcal{H}_k$ or as a Wigner function defined over a $2n$-dimensional phase space (see Ref. [7] for more details). In particular, a state is Gaussian if its Wigner function is Gaussian, so that it is completely characterized by the first two statistical moments, i.e., the mean value $\bar{\mathbf{x}} := \langle\hat{\mathbf{x}}\rangle = \mathrm{Tr}(\hat{\mathbf{x}}\hat{\rho})$ and covariance matrix (CM) $\mathbf{V}$, whose arbitrary element is defined by

$$V_{ij} := \tfrac{1}{2}\left\langle\{\Delta\hat{x}_i, \Delta\hat{x}_j\}\right\rangle, \tag{108}$$

where $\Delta\hat{x}_i := \hat{x}_i - \langle\hat{x}_i\rangle$ and $\{,\}$ is the anti-commutator.

For a single-mode, one can consider different classes of quantum states, the most known are the coherent states. These are states with minimum (vacuum) noise uncertainty, symmetrically distributed in the two quadratures, and characterized by their complex amplitudes in the phase space. They are denoted as $|\alpha\rangle$, where $\alpha = (\bar{q} + i\bar{p})/2$, where $(\bar{q}, \bar{p})$ are the components of the mean value. Another important class is that of squeezed states, where the noise is less than the vacuum in one of the two quadratures (while greater than in the other) [7]. The reader can consult Appendix A for more details on the CV notation and a number of formulas that are relevant for calculations with Gaussian states.

The basic one-way CV-QKD protocols can be classified with respect to the quantum states employed (coherent or squeezed), the type of encoding adopted (Gaussian modulation or discrete alphabet), and the type of measurement used (homodyne or heterodyne detection). In particular, Gaussian protocols based on the Gaussian modulation of Gaussian states have received an increasing attention in the latest years, not only because Gaussian states are routinely produced in quantum optics labs but also because they are relatively easy to study, due to their description based on mean value and CM.

B. Historical outline

As an alternative to DV-QKD protocols, which are ideally based on a single photon detection, CV-QKD protocols encode keys into CV observables of light fields [8] that can be measured by shot-noise limited homodyne detection. In a homodyne detector an optical signal is coupled to a shot-noise limited strong local oscillator (LO) beam on a balanced beamsplitter and the light intensities on the output ports are measured. Depending on the optical phase difference between the signal and LO, the difference of photocurrents produced at each of the two detectors will be proportional to one of the two field quadratures. The LO therefore carries the phase reference, which allows to switch between the measurement of $q-$ and $p-$quadrature (or more generally perform the state tomography by measuring the Wigner function associated to the state).

The first proposal of using the quadratures of the bosonic field for implementing QKD dates back to 1999, when Ralph [455] considered the encoding of key bits by using four fixed quadrature displacements of bright coherent or two-mode entangled beams. Later, Ralph

discussed the security of the two-mode entanglement-based scheme in more detail [456], considering not only intercept-resend attacks but also CV teleportation. The latter was identified as an optimal attack against the protocol, imposing the requirements of high signal squeezing and low channel loss [456]. Independently, Hillery [457] suggested a CV-QKD protocol based on quadrature encoding of a single-mode beam, randomly squeezed in one of the quadrature directions. Security against intercept-resend and beam-splitting attacks were assessed on the basis of the uncertainty principle. Another early CV-QKD scheme was suggested by Reid [458] and based on the verification of EPR-type correlations to detect an eavesdropper.

In 2000 Cerf et al. [459] proposed the first *all continuous* QKD protocol, where the quadratures of a squeezed beam were used to encode a Gaussian-distributed secure key. The security of the protocol was shown against individual attacks based on the uncertainty relations and the optimality of a quantum cloner. Later, reconciliation procedures were introduced for Gaussian-distributed data, which allowed to implement EC and PA close to the theoretical bounds [460]. Another CV-QKD protocol based on the Gaussian modulation of squeezed beams was suggested by Gottesman and Preskill [461]. This protocol was shown to be secure against arbitrary attacks at feasible levels of squeezing, by using quantum error-correcting codes.

In 2001 Grosshans and Grangier introduced a seminal coherent-state protocol with Gaussian quadrature modulation and showed its security against individual attacks [462] by resorting to the CV version of the no-cloning theorem [463]. The standard protocol based on DR, where Alice is the reference side for the information post-processing, was however limited to 50% channel transmittance, i.e., 3dB. As an attempt to beat the 3dB limit, the use of post-selection in CV-QKD was suggested by Silberhorn et al. [464]. Alternatively, it was shown that the use of RR, where the reference side is Bob, allowed the coherent-state protocol to be secure against individual attacks up to arbitrarily-low channel transmittances [465]. In 2004, the heterodyne detection was then suggested for coherent-state protocols [466]; this *non-switching protocol* had the advantage that both the quadratures are measured, thus increasing the key rate.

The security of CV-QKD against collective Gaussian attacks was shown independently by Navascués et al. [467] and by García-Patrón and Cerf [468]. Collective Gaussian attacks were fully characterized by Pirandola et al. [469], who later derived the secret-key capacities for CV-QKD [43, 44]. Security against collective attacks was extended to the general attacks by Renner and Cirac [87] using the quantum de Finetti theorem applied to infinite-dimensional systems. This concluded the security proofs for the basic one-way CV-QKD protocols in the asymptotic limit of infinitely large data sets [470] including those with trusted-noise [124, 471, 472]. Next developments were the study of finite-size effects and fully composable proofs (e.g. see Ref [93]). It is also worth to mention the existence of other direction lines where the limitations of a realistic eavesdropper are taken into account in the computation of the secret key rate [473, 474]. In this context, we will analyze the consequences of a bounded quantum memory for the eavesdropper in Sec. XIII.

Besides the development of one-way Gaussian protocols and their security proofs, the quantum information community has developed a number of other types of protocols, Gaussian or not, which are based on the use of CV systems. In the following sections, apart from standard one-way Gaussian protocols (based on coherent-states or squeezed-states), we will treat two-way protocols, thermal-state protocols, unidimensional protocols, discrete-modulated protocols, and relay-assisted protocols such as CV MDI-QKD. It is clear that this does not encompass all the current production in the wide field of CV-QKD. For instance, we will not explicitly discuss protocols that are based on the use of non-Gaussian operations such as photon-subtraction [475], quantum catalysis [476], or quantum scissors [477].

C. One-way CV-QKD protocols

The family of one-way CV-QKD protocols can be divided into four major ones, depending on the signal states and the type of measurements applied. It was already mentioned that CV-QKD can be realized using coherent or squeezed signal states, and the homodyne measurement is used to obtain quadrature value of an incoming signal. As an alternative to the homodyne detection, the heterodyne measurement can be applied. Here the signal mode is divided on a balanced beamsplitter and q- and p-quadratures are simultaneously detected using homodyne detectors at the outputs. A vacuum noise is then unavoidably being mixed to the signal.

The "prepare and measure" realization of a generic one-way CV-QKD protocol includes the following steps:

- Alice encodes a classical variable α in the amplitudes of Gaussian states which are randomly displaced in the phase space by means of a zero-mean Gaussian distribution, whose variance is typically large. If coherent states are used, the modulation is symmetric in the phase space. If squeezed states are used instead, then the displacement is along the direction of the squeezing and Alice randomly switches between q- and p- squeezings.

- Alice then sends the modulated signal states to Bob through the quantum channel, which is typically a thermal-loss channel with transmissivity η and some thermal noise, quantified by the mean number of thermal photons in the environment $\bar{n}$ or, equivalently, by the excess noise $\varepsilon = 2\eta^{-1}(1-\eta)\bar{n}$. In some cases, one may have a fading channel where

the channel's transmissivity varies over time (e.g. due to turbulence) [478].

- At the output of the quantum channel, Bob performs homodyne or heterodyne detection on the incoming signals, thus retrieving his classical variable β. If homodyne is used, this is randomly switched between the q- and the p- quadratures.

- If Alice and Bob have switched between different quadratures, they will implement a session of CC to reconcile their bases, so as to keep only the choices corresponding to the same quadratures (sifting).

- By publicly declaring and comparing part of their sifted data, Alice and Bob perform parameter estimation. From the knowledge of the parameters of the quantum channel, they can estimate the maximum information leaked to Eve, e.g., in a collective Gaussian attack. If this leakage is above a certain security threshold, they abort the protocol.

- Alice and Bob perform EC and PA on their data. This is done in DR if Bob aims to infer Alice's variable, or RR if Alice aims to infer Bob's one.

D. Computation of the key rate

In a Gaussian CV-QKD protocol, where the Gaussian signal states are Gaussianly-modulated and the outputs are measured by homodyne or heterodyne detection, the optimal attack is a collective Gaussian attack. Here Eve combines each signal state and a vacuum environmental state via a Gaussian unitary and collects the output of environment in a quantum memory for an optimized and delayed joint quantum measurement. The possible collective Gaussian attacks have been fully classified in Ref. [469]. A realistic case is the so-called entangling cloner [463] where Eve prepares a two-mode squeezed vacuum (TMSV) state with variance $\omega = 2\bar{n} + 1$ and mixes one of its modes with the signal mode via a beamsplitter with transmissivity η, therefore resulting in a thermal-loss channel (see Ref. [479] for a comparison of this attack with respect to an all-optical teleportation attack). Under a collective Gaussian attack, the asymptotic secret key rates in DR ($\blacktriangleright$) or RR ($\blacktriangleleft$) are respectively given by

$$R^{\blacktriangleright} = \xi I(\alpha:\beta) - I(\alpha:E), \tag{109}$$

$$R^{\blacktriangleleft} = \xi I(\alpha:\beta) - I(\beta:E), \tag{110}$$

where $\xi \in (0,1)$ is the reconciliation efficiency, defining how efficient are the steps of EC and PA, $I(\alpha:\beta)$ is Alice and Bob's mutual information on their variables α and β, while $I(\alpha:E)$ is Eve's Holevo information [83] on Alice's variable, and $I(\beta:E)$ on Bob's variable. Note that a sifting pre-factor may be present in protocols that need basis reconciliation.

Theoretical evaluation of these rates is performed in the equivalent entanglement-based representation of the protocol, where Alice's preparation of signal states on the input mode a is replaced by a TMSV state Φ^{μ}_{aA} in modes a and A. A Gaussian measurement performed on mode A is able to remotely prepare a Gaussian ensemble of Gaussian states on mode a. For instance, if A is subject to heterodyne, then mode a is projected onto a coherent state whose amplitude is one-to-one with the outcome of the heterodyne and is Gaussianly modulated in phase space with variance $\mu - 1$. In this representation, Alice's classical variable is equivalently represented by the outcome of her measurement.

Once mode a is propagated through the channel, it is perturbed by Eve and received as mode B by Bob. Therefore, Alice and Bob will share a bipartite state ρ_{AB}. In the worst case scenario, the entire purification of ρ_{AB} is assumed to be held by Eve. This means that we assume a pure state Ψ_{ABE} involving a number of extra modes E such that $\mathrm{Tr}_E(\Psi_{ABE}) = \rho_{AB}$. For a Gaussian protocol under a collective Gaussian attack, we have that Ψ_{ABE} is pure, so that the Eve's reduced output state $\rho_E := \mathrm{Tr}_{AB}(\Psi_{ABE})$ has the same entropy of ρ_{AB}, i.e.,

$$S(E) := S(\rho_E) = S(\rho_{AB}) := S(AB). \tag{111}$$

Assuming that Alice and Bob performs rank-1 Gaussian measurements (like homodyne or heterodyne), then they project on pure states. In DR, this means that the output α of Alice measurement, with probability $p(\alpha)$, generates a pure conditional Gaussian state $\Psi_{BE|\alpha}$ whose CM does not depend on the actual value of α. Then, because the reduced states $\rho_{B(E)|\alpha} := \mathrm{Tr}_{E(B)}(\Psi_{BE|\alpha})$ have the same entropy, we may write the following equality for the conditional entropies

$$\begin{aligned} S(E|\alpha) &:= \int d\alpha\; p(\alpha) S(\rho_{E|\alpha}) \\ &= S(\rho_{E|\alpha}) = S(\rho_{B|\alpha}) \\ &= \int d\alpha\; p(\alpha) S(\rho_{B|\alpha}) := S(B|\alpha). \end{aligned} \tag{112}$$

Similarly, in RR, we have Bob's outcome β with probability $p(\beta)$ which generates a pure conditional Gaussian state $\Psi_{AE|\beta}$ with similar properties as above. In terms of the reduced states $\rho_{A(E)|\beta} := \mathrm{Tr}_{E(A)}(\Psi_{AE|\beta})$ we write the conditional entropies

$$\begin{aligned} S(E|\beta) &:= \int d\beta\; p(\beta) S(\rho_{E|\beta}) \\ &= S(\rho_{E|\beta}) = S(\rho_{A|\beta}) \\ &= \int d\beta\; p(\beta) S(\rho_{A|\beta}) := S(A|\beta). \end{aligned} \tag{113}$$

By using Eqs. (111), (112) and (113) in the key rates of Eqs. (109) and (110) we may simplify the Holevo quantities as

$$I(\alpha:E) := S(E) - S(E|\alpha) = S(AB) - S(B|\alpha), \tag{114}$$

$$I(\beta:E) := S(E) - S(E|\beta) = S(AB) - S(A|\beta). \tag{115}$$

This is a remarkable simplification because the two rates are now entirely computable from the output bipartite state ρ_{AB} and its reduced versions $\rho_{B|\alpha}$ and $\rho_{A|\beta}$. In particular, because all these state are Gaussian, the von Neumann entropies in Eqs. (114) and (115) are very easy to compute from the CM of ρ_{AB}. Similarly, the mutual information $I(\alpha:\beta)$ can be computed from the CM. Given the expressions of the rates, one can also compute the security thresholds by solving $R^{\blacktriangleright}=0$ or $R^{\blacktriangleleft}=0$.

Note that there is a more generalized framework for security analysis, where Alice and Bob have trusted loss and noise in their devices and they cannot purify into a TMSV state. This is a device-dependent scenario which is typical in realistic implementations where both the preparation of the signals and the measurements of the outputs are affected by imperfections. In this case, a generalized treatment is possible following Refs. [124, 480].

E. Ideal performances in a thermal-loss channel

The ideal performances of the main one-way Gaussian protocols can be studied in a thermal-loss channel, assuming asymptotic security, perfect reconciliation ($\xi=1$), and infinite Gaussian modulation. Let us consider the entropic function

$$s(x):=\frac{x+1}{2}\log_2\frac{x+1}{2}-\frac{x-1}{2}\log_2\frac{x-1}{2}, \tag{116}$$

so that $s(1)=0$ for the vacuum noise. For the protocol with Gaussian-modulated coherent states and homodyne detection [463], one has

$$R^{\blacktriangleright}_{\text{coh,hom}}=\frac{1}{2}\log_2\frac{\eta\,(1-\eta+\eta\omega)}{(1-\eta)\,[\eta+(1-\eta)\omega]}-s(\omega)+s\left[\sqrt{\frac{\eta+(1-\eta)\omega}{1-\eta+\eta\omega}\omega}\right], \tag{117}$$

$$R^{\blacktriangleleft}_{\text{coh,hom}}=\frac{1}{2}\log_2\frac{\omega}{(1-\eta)\,[\eta+(1-\eta)\omega]}-s(\omega). \tag{118}$$

For the non-switching protocol with Gaussian-modulated coherent states and heterodyne detection [466], one instead has

$$R^{\blacktriangleright}_{\text{coh,het}}=\log_2\frac{2}{e}\frac{\eta}{(1-\eta)\,[1+\eta+(1-\eta)\omega]}-s(\omega)+s\left[\eta+\omega(1-\eta)\right], \tag{119}$$

$$R^{\blacktriangleleft}_{\text{coh,het}}=\log_2\frac{2}{e}\frac{\eta}{(1-\eta)\,[1+\eta+(1-\eta)\omega]}-s(\omega)+s\left[\frac{1+(1-\eta)\omega}{\eta}\right]. \tag{120}$$

For the protocol with Gaussian-modulated squeezed states (in the limit of infinite squeezing) and homodyne detection [459], here we analytically compute

$$R^{\blacktriangleright}_{\text{sq,hom}}=\frac{1}{2}\left[\log_2\frac{\eta}{1-\eta}-s(\omega)\right], \tag{121}$$

$$R^{\blacktriangleleft}_{\text{sq,hom}}=\frac{1}{2}\left[\log_2\frac{1}{1-\eta}-s(\omega)\right]. \tag{122}$$

Note that, for this specific protocol, a simple bound can be derived at low η and low $\bar{n}$, which is given by [481] $R^{\blacktriangleleft}_{\text{sq,hom}}\simeq(\eta-\bar{n})\log_2 e+\bar{n}\log_2\bar{n}$, which provides a security threshold $\bar{n}_{max}(\eta)=\exp[1+W_{-1}(-\eta/e)]$ in terms of the Lambert W-function.

Finally, for the protocol with Gaussian-modulated infinitely-squeezed states and heterodyne detection [482], here we analytically compute

$$R^{\blacktriangleright}_{\text{sq,het}}=\frac{1}{2}\log_2\frac{\eta^2\omega}{(1-\eta)\,[1+(1-\eta)\omega]}-s(\omega), \tag{123}$$

$$R^{\blacktriangleleft}_{\text{sq,het}}=\frac{1}{2}\log_2\frac{1-\eta+\omega}{(1-\eta)\,[1+(1-\eta)\omega]}-s(\omega)+s\left[\sqrt{\frac{\omega\,[1+\omega(1-\eta)]}{1+\omega-\eta}}\right]. \tag{124}$$

Note that this is a particular case of protocol where trusted noise added at the detection can have beneficial effects on its security threshold [471, 472]. In CV-QKD this effect was studied in Refs. [44, 124, 482–484], and later in Refs. [485–487] as a tool to increase the lower bound to the secret key capacity of the thermal-loss and amplifier channels. In particular, the protocol presented in Ref. [487] has the highest-known security threshold so far (see also Sec. XI).

Also note that for a pure-loss channel ($\omega=1$), we find

$$R^{\blacktriangleleft}_{\text{sq,het}}=R^{\blacktriangleleft}_{\text{sq,hom}}=\frac{1}{2}\log_2\frac{1}{1-\eta}, \tag{125}$$

which is half of the PLOB bound $-\log_2(1-\eta)$. According to Ref. [44], this bound is achievable if one of these two protocols is implemented in the entanglement-based representation and with a quantum memory. In particular for the squeezed-state protocol with homodyne detection, the use of the memory allows Alice and Bob to always choose the same quadrature, so that we may remove the sifting factor 1/2 from $R^{\blacktriangleleft}_{\text{sq,hom}}$ in Eq. (125).

F. Finite-size aspects

The practical security of CV-QKD [38] deals with finite data points obtained experimentally. In this finite-size regime the security of CV-QKD was first analyzed against collective attacks [488] by including corrections to the key rate taking into account of the data points used and discarded during parameter estimation and the convergence of the smooth min-entropy towards the von Neumann entropy. The channel estimation in the finite-size regime of CV-QKD was further studied in Ref. [489]

where it was suggested the use of a double Gaussian modulation, so that two displacements are applied and each signal state can be used for both key generation and channel estimation. See also Ref. [490] for excess noise estimation using the method of moments.

The finite-size security under general coherent attacks have been also studied. Ref. [91, 92] used entropic uncertainty relations for the smooth entropies to show this kind of security for an entanglement-based protocol based on TMSV states. The analysis was extended to the protocol with squeezed states and homodyne detection [491]. Finite-size security for one-way coherent-state protocols against general attacks was studied in Ref. [492] by using post-selection and employing phase-space symmetries. More recently, it was shown that, for coherent-state protocols, the finite-size security under general attacks can be reduced to proving the security against collective Gaussian attacks by using a Gaussian de Finetti reduction [93]. See Sec. IX D for more details.

G. Two-way CV-QKD protocols

In a two-way CV-QKD scheme [493], similar to its DV counterpart [173, 177], Alice and Bob use twice the insecure channel in order to share a raw key. During the first quantum communication, Bob randomly prepares and sends a reference state to Alice who, in turn, encodes her information by performing a unitary transformation on the received state, before sending it back to Bob for the final measurement. The appeal of this type of protocol is its increased robustness to the presence of excess noise in the channel. From an intuitive point of view, this is due to the fact that Eve needs to attack both the forward and backward transmissions in order to steal information, resulting in an increased perturbation of the quantum system. The promise is a higher security threshold with respect to one-way protocols.

Let us now describe in detail a two-way protocol based on coherent states and heterodyne detection [493]. Here Bob prepares a reference coherent state $|\beta\rangle$ whose amplitude is Gaussianly-modulated with variance μ_B. This is sent through the quantum channel and received as a mixed state $\rho(\beta)$ by Alice. At this point, Alice randomly decides to close (ON) or open (OFF) the "circuit" of the quantum communication. When the circuit is in ON, Alice encodes a classical variable α on the reference state by applying a displacement $\hat{D}(\alpha)$ whose amplitude is Gaussianly-modulated with variance μ_A. This creates the state $\hat{D}(\alpha)\rho(\beta)\hat{D}(-\alpha)$ which is sent back to Bob, where heterodyne detection is performed with outcome $\gamma \simeq \alpha + \beta$. From the knowledge of γ and β, Bob can generate a post-processed variable $\alpha' \simeq \alpha$. In DR, the key is generated by Bob trying to infer Alice's variable α. In RR, the situation is reversed with Alice guessing Bob's variable α'.

When the circuit is in OFF, Alice first applies heterodyne detection on the incoming reference state $\rho(\beta)$, obtaining a variable β'. Then she prepares a new Gaussian-modulated coherent state $|\alpha\rangle$ to be sent back to Bob. His heterodyne detection provides an output variable α'. In such a case the parties may use the variables $\{\beta, \beta'\}$ and $\{\alpha, \alpha'\}$ to prepare the key. In DR the variables β and α are guessed while, in RR, the primed variables β' and α' are. For both the ON and the OFF configuration, Alice and Bob publicly declare and compare a fraction of their data in order to estimate the transmissivity and noise present in the round-trip process.

Note that the control of the parties over the ON/OFF setup of the two-way communication represents an additional *degree of freedom* evading Eve's control. As a matter of fact, Alice and Bob may decide which setup to use for the generation of the key. The safest solution is to use the ON configuration if Eve performs an attack of the round-trip based on two memoryless channels, while the OFF configuration is used when Eve performs an attack which has memory, i.e., with correlations between the forward and the backward paths.

1. *Asymptotic security of two-way CV-QKD*

The security of two-way CV-QKD protocols has been first studied in the asymptotic limit of infinitely-many uses of the channel and large Gaussian modulation [493–495]. The most general coherent attack can be reduced by applying de Finetti random permutations [87] which allow the parties to neglect possible correlations established by Eve between different rounds of the protocol. In this way the attack is reduced to a two-mode attack which is coherent within a single round-trip quantum communication. Then, the security analysis can be further simplified by using the extremality of Gaussian states [496], which allows one to just consider two-mode Gaussian attacks. The most realistic of these attacks is implemented by using two beam-splitters of transmissivity η, where Eve injects two ancillary modes E_1 and E_2, the first interacting with the forward mode and the second with the backward mode. Their outputs are then stored in a quantum memory which is subject to a final collective measurement.

In each round-trip interaction, Eve's ancillae E_1 and E_2 may be coupled with to another set of modes so as to define a global pure state. However, these additional ancillary modes can be neglected if we consider the asymptotic limit where Eve's accessible information is bounded by the Holevo quantity [469]. As a result, we may just consider a two-mode Gaussian state $\rho_{E_1E_2}$ for Eve's input ancillary modes. In practical cases, its CM can be assumed to have the normal form

$$\mathbf{V}_{E_1E_2} = \begin{pmatrix} \omega\mathbf{I} & \mathbf{G} \\ \mathbf{G} & \omega\mathbf{I} \end{pmatrix}, \ \mathbf{G} := \begin{pmatrix} g & 0 \\ 0 & g' \end{pmatrix}, \tag{126}$$

where ω is the variance of the thermal noise, $\mathbf{I} = \mathrm{diag}(1,1)$, $\mathbf{Z} = \mathrm{diag}(1,-1)$, and matrix $\mathbf{G}$ describes the

two-mode correlations. Here the parameters ω, g and g' must fulfill the bona fide conditions [497]

$$|g| < \omega,\ |g'| < \omega,\ \omega^2 + gg' - 1 \geq \omega\,|g + g'|\,. \tag{127}$$

We notice that when $g = g' = 0$, then CM of Eq. (126) describes the action of two independent entangling cloners, i.e., the attack simplifies to one-mode Gaussian attack.

2. Asymptotic key rates

Here we provide the asymptotic secret key rates of the main two-way protocols based on coherent states and heterodyne or homodyne detection [493]. For each protocol, we summarize the key rates in DR or RR for the two configurations in ON or OFF. In particular, ON is assumed against one-mode Gaussian attacks, while OFF is assumed to be used under two-mode Gaussian attacks [493–495]. For an ON key rate under two-mode attacks see Ref. [494], but we do not consider this here.

For the two-way protocol based on coherent states and heterodyne detection we write the key rates

$$R^{\blacktriangleright}_{\rm ON} = \log_2 \frac{2\eta(1+\eta)}{e(1-\eta)\Lambda} - s(\omega). \tag{128}$$

$$R^{\blacktriangleleft}_{\rm ON} = \log_2 \frac{\eta(1+\eta)}{e(1-\eta)\Lambda} + \sum_{i=1}^{3} s(\bar{\nu}_i) - 2s(\omega), \tag{129}$$

$$R^{\blacktriangleright}_{\rm OFF} = \log_2 \frac{2\eta}{e(1-\eta)\tilde{\Lambda}} + \sum_{k=\pm} \frac{s(\bar{\nu}_k) - s(\nu_k)}{2}, \tag{130}$$

$$R^{\blacktriangleleft}_{\rm OFF} = \log_2 \frac{2\eta}{e(1-\eta)\tilde{\Lambda}} + \sum_{k=\pm} \frac{s(\bar{\nu}'_k) - s(\nu_k)}{2}, \tag{131}$$

where $\Lambda := 1 + \eta^2 + (1-\eta^2)\omega$, $\tilde{\Lambda} := 1 + \eta + (1-\eta)\omega$, the eigenvalues $\bar{\nu}_i$ are computed numerically and

$$\bar{\nu}_\pm = \sqrt{[\eta + 2(\omega \pm g)(1-\eta)][\eta + 2(\omega \pm g')(1-\eta)]}, \tag{132}$$

$$\nu_\pm = \sqrt{(\omega \pm g)(\omega \pm g')}, \tag{133}$$

$$\bar{\nu}'_\pm = \frac{\sqrt{[(\omega \pm g)(1-\eta)+1][(\omega \pm g')(1-\eta)+1]}}{\eta}. \tag{134}$$

Note that, if we set $g = g' = 0$ in the OFF rates, we retrieve the two rates of the one-way coherent-state protocol in Eqs. (119) and (120).

Consider now the two-way coherent state protocol with homodyne detection. In this case, the solution is fully analytical. In fact, we have the following key rates

$$R^{\blacktriangleright}_{\rm ON} = \frac{1}{2}\log_2 \frac{\eta(1+\eta)\omega}{(1-\eta)[\eta^2 + (1-\eta^2)\omega]} - s(\omega), \tag{135}$$

$$R^{\blacktriangleleft}_{\rm ON} = \frac{1}{2}\log_2 \frac{\eta^2 + \omega + \eta^3(\omega-1)}{(1-\eta)[\eta^2 + (1-\eta^2)\omega]} + s(\tilde{\nu}) - s(\omega), \tag{136}$$

$$R^{\blacktriangleright}_{\rm OFF} = \frac{1}{2}\log_2 \frac{\eta\sqrt{[1+\eta(\omega-1)]^2 - \eta^2 g^2}}{(1-\eta)[\eta + (1-\eta)\omega]} + \sum_{k=\pm} \frac{s(\delta_k) - s(\nu_k)}{2}, \tag{137}$$

$$R^{\blacktriangleleft}_{\rm OFF} = \frac{1}{2}\log_2 \frac{\sqrt[4]{(\omega^2 - g^2)(\omega^2 - g'^2)}}{(1-\eta)[\eta + (1-\eta)\omega]} - \sum_{k=\pm} \frac{s(\nu_k)}{2}, \tag{138}$$

where the eigenvalues ν_k are given in Eq. (133), and

$$\tilde{\nu} := \sqrt{\frac{\omega[1 + \eta^2\omega(1-\eta) + \eta^3]}{\eta^2 + \omega + \eta^3(\omega-1)}}, \tag{139}$$

$$\delta_\pm = \sqrt{\frac{(\omega \pm g')[\eta + (\omega \pm g)(1-\eta)]}{1 - \eta + \eta(\omega \pm g')}}. \tag{140}$$

Other cases with encoding by squeezed states and decoding by heterodyne/homodyne detection, have been discussed in Ref. [495].

3. Further considerations

As discussed in Refs. [493–495] the security thresholds of the two-way protocols, given by setting $R = 0$ in the expression above, are higher of the corresponding one-way protocols. This makes two-way CV-QKD a good choice in communication channels affected by high thermal noise (e.g., at the THz or microwave regime). The security analyses provided in Refs. [493–495, 498] are limited to the asymptotic regime. However, recently the composable security has been also proven [499]. Other studies on the security of two-way CV-QKD protocols have been carried out in Refs. [500, 501], besides proposing the use of optical amplifiers [502]. Let us also note that, besides the Gaussian two-way protocols, one may also consider schemes that are based on quantum illumination [503] or may implement floodlight QKD [504–507]. The latter is a two-way quantum communication scheme which allows one to achieve, in principle, Gbit/s secret-key rate at metropolitan distances. This is done by employing a multiband strategy where the multiple optical modes are employed in each quantum communication.

H. Thermal-state QKD

In the protocols treated so far one assumes that the Gaussian states are pure. This requirement can however be relaxed. The possibility of using "noisy" coherent states, more precisely optical thermal states, was first considered in Ref. [508] which showed that these states are suitable for QKD if the parties adopt RR and the signals are purified before transmission over the channel. This approach was later reconsidered in Ref. [509], which proved its security in realistic quantum channels. Refs. [510, 511] showed that thermal states can be directly employed in CV-QKD (without any purification at the input) if the protocol is run in DR. Similarly, they can be directly employed in two-way CV-QKD if the protocol is run in RR [512]. By considering thermal states at any frequency, not just optical, Refs. [510–512] pioneered the possibility to extend CV-QKD to longer wavelengths down to the microwave regime, where the protocols can be implemented for short-range applications and are sufficiently robust to finite-size effects [513]. More recently, the terahertz regime has been also proposed for short-range uses of CV-QKD [514]. This regime may also have applications for satellite (LEO) communications where the issue of the background thermal noise is mitigated.

1. *One-way thermal communication*

For simplicity, we focus on the one-way protocol where Bob homodynes the incoming signals, randomly switching between the quadratures. An alternative no-switching implementation based on heterodyne detection can be considered as well. The protocol starts with Alice randomly displacing thermal states in the phase space according to a bivariate Gaussian distribution. She then sends the resulting state to Bob, over the insecure quantum channel. The generic quadrature $\hat{A} = (q_A, p_A)$ of Alice's input mode A can be written as $\hat{A} = \hat{0} + \alpha$, where the real number α is the Gaussian encoding variable with variance V_α, while operator $\hat{0}$ accounts for the thermal 'preparation noise', with variance $V_0 \geq 1$. The overall variance of Alice's average state is therefore $V_A = V_0 + V_\alpha$.

The variance V_0 can be broken down as $V_0 = 1 + \mu_{th}$, where 1 is the variance of the vacuum shot-noise, and $\mu_{th} \geq 0$ is the variance of an extra trusted noise confined in Alice's station and uncorrelated to Eve. Bob homodynes the incoming signals, randomly switching between position and momentum detections. In this way, Bob collects his output variable β which is correlated to Alice's encoding α. After using a public channel to compare a subset of their data, to estimate the noise in the channel and the maximum information eavesdropped, the parties may apply classical post-processing procedures of EC and PA in order to extract a shorter secret-key.

The security analysis of this type of protocol is analogous to that of the case based on coherent states. Because the protocol is Gaussian, we may consider collective Gaussian attacks and Eve's accessible information is overestimated by the Holevo bound. Assuming a realistic entangling-cloner attack, in the typical limit of large variance $V_\alpha \gg 1$, we obtain the following expressions for the asymptotic key-rates [510, 511]

$$R_{\text{th}}^{\blacktriangleright} = \frac{1}{2}\log_2 \frac{\eta\Lambda(\omega, V_0)}{(1-\eta)\Lambda(V_0, \omega)} + s\left[\sqrt{\frac{\omega\Lambda(1, \omega V_0)}{\Lambda(\omega, V_0)}}\right] - s(\omega)\ , \tag{141}$$

$$R_{\text{th}}^{\blacktriangleleft} = \frac{1}{2}\log_2 \frac{\omega}{(1-\eta)\Lambda(V_0, \omega)} - s(\omega), \tag{142}$$

where the function $\Lambda(x, y) := \eta x + (1-\eta)y$ and $s(x)$ is defined in Eq. (116).

2. *Two-way thermal communication*

The two-way thermal protocol [512] extends the one-way thermal protocol [510, 511] to two-way quantum communication. The steps of the protocol are the same as described in Sec. VII G but with thermal states replacing coherent ones. Therefore, Bob has an input mode B_1, described by the generic quadrature $\hat{B}_1 = \hat{0} + \beta_1$, where β_1 is the encoding Gaussian variable having variance V_{β_1} while mode $\hat{0}$ has variance $V_0 = 1 + \mu_{th} \geq 1$. After the first quantum communication Alice receives the noisy mode A_1 and randomly switches between the two possible configurations [495, 512]. In case of ON configuration, Alice encodes a Gaussian variable α with variance $V_\alpha = V_{\beta_1}$, randomly displacing the quadrature of the incoming mode $\hat{A}_1 \to \hat{A}_2 = \hat{A}_1 + \alpha$. When the two-way circuit is set OFF, Alice homodynes the incoming mode A_1 with classical output α_1, and prepares another Gaussian-modulated thermal state $\hat{A}_2 = \hat{0} + \alpha_2$, with the same preparation and signal variances as Bob, i.e., V_0 and $V_{\alpha_2} = V_{\beta_1}$. In both cases, the processed mode A_2 is sent back to Bob in the second quantum communication through the channel. At the output, Bob homodynes the incoming mode B_2 with classical output β_2.

At the end of the double quantum communication, Alice publicly reveals the configuration used in each round of the protocol, and both the parties declare which quadratures were detected by their homodyne detectors. After this stage, Alice and Bob possess a set of correlated variables, which are $\alpha_1 \approx \beta_1$ and $\alpha_2 \approx \beta_2$ in OFF configuration, and $\alpha \approx \beta$ in ON configuration. By comparing a small subset of values of these variables, the parties may detect the presence of memory between the first and the second use of the quantum channel. If two-mode coherent attacks are present then they use the OFF configuration, extracting a secret-key from $\alpha_1 \approx \beta_1$ and $\alpha_2 \approx \beta_2$. If memory is absent, the parties assume one-mode collective attacks against the ON configuration, and they post-process α and β. We remark that the switching between the two configurations can be used as a virtual

basis against Eve [495], who has no advantage in using two-mode correlated attacks against the CV two-way protocol.

Let us assume the realistic Gaussian attack composed by two beam-splitters of transmissivity η, where Eve injects two ancillary modes E_1 and E_2 in a Gaussian state whose CM is specified in Eq. (126). This is a two-mode (one-mode) attack for $g, g' \neq 0$ $(= 0)$. Assuming ideal reconciliation efficiency, working in the asymptotic limit of many signals and large Gaussian modulations, one can compute the following secret key rates for the two-way thermal protocol with homodyne decoding

$$R^{\blacktriangleright}_{\text{2-th}} = \frac{1}{2}\log_2 \frac{\eta(1+\eta)\omega}{(1-\eta)\left[\eta^2 V_0 + (1-\eta^2)\omega\right]} - s(\omega), \quad (143)$$

$$R^{\blacktriangleleft}_{\text{2-th}} = \frac{1}{2}\log_2 \frac{\eta^2 V_0 + \omega + \eta^3(\omega - V_0)}{\left[V_0\eta^2 + (1-\eta^2)\omega\right](1-\eta)} - s(\omega) + s\left(\sqrt{\frac{\omega\left[1+\eta^2 V_0\omega + \eta^3(1-V_0\omega)\right]}{\eta^2 V_0 + \omega + \eta^3(\omega - V_0)}}\right). \quad (144)$$

I. Unidimensional protocol

As an alternative to the standard CV-QKD protocols described above, where both quadratures have to be modulated and measured (be it simultaneously or subsequently), one may consider a unidimensional (UD) protocol [515, 516], which relies on a single quadrature modulation at Alice's side while Bob performs a randomly-switched homodyne detection. Because it requires a single modulator, the UD CV-QKD protocols provide a simple experimental realization with respect to conventional CV QKD [516, 517]. This also means that the trusted parties are not able to estimate the channel transmittance in the un-modulated quadrature, which remains an unknown free parameter in the protocol security analysis. This parameter however can be limited by considerations of physicality of the obtained CMs. In other words, Eve's collective attack should be pessimistically assumed to be maximally effective, but is still limited by the physicality bounds related to the positivity of the CM and its compliance with the uncertainty principle [7, 518].

Therefore, Eve's information can be still upper-bounded and the lower bound on the key rate can be evaluated. The performance of the protocol was compared to standard one-way CV-QKD in the typical condition of a phase-insensitive thermal-loss channel (with the same transmittance and excess noise for both the quadratures). While the UD protocol is more fragile to channel loss and noise than conventional CV-QKD, it still provides the possibility of long-distance fiber-optical communication. In the limit of low transmissivity η and infinitely strong modulation, the key rate for the UD CV-QKD protocol with coherent-states and homodyne detection is approximately given by $(\eta \log_2 e)/3$ [515], which is slightly smaller than the similar limit for the standard one-way protocol with coherent states and homodyne detection [519] with a rate approximately given by $(\eta \log_2 e)/2$.

UD CV-QKD was recently extended to squeezed states [520], which were shown to be advantageous only in the DR scenario if the anti-squeezed quadrature is modulated. Unfortunately, the squeezed-state UD CV-QKD protocol does not have a good performance in RR [520, 521]. Finally, it is worth to mention that the security of coherent-state UD CV-QKD was recently extended to the finite-size regime [522] with a study of its composability security against collective attacks [523].

J. CV-QKD with discrete modulation

In CV-QKD, information is encoded in quantum systems with infinite-dimensional Hilbert spaces. This allows the sender to use bright coherent states and highly-efficient homodyne detections, which naturally boost the communication rate. These features do not come for free. At the EC stage, one pays a penalty in mapping the continuous output data from the physical Gaussian channel into a binary-input additive white Gaussian-noise channel. This mapping is more accurate by employing discrete modulation [524]. The first discrete-modulated CV-QKD protocol was based on a binary encoding of coherent states [464] and was designed to overcome the 3dB limitation of CV-QKD in DR. Besides binary encoding into two states [525, 526], later protocols have considered three [527], four [524], and an arbitrary number of phase-encoded coherent states [528, 529]. A number of works have recently appeared in this area [530–532], including a study that shows the enhancement of discrete-modulated CV-QKD by means of quantum scissors [533].

The basic idea in Ref. [464] is to perform a binary encoding which assigns the bit-value 0 (1) to a coherent state with positive (negative) displacement. Then, the receiver switches the homodyne detection setup, measuring quadrature q or p. After the quantum communication, the parties discard *unfavorable* data by applying an advantage distillation routine [534, 535], which is a post-selection procedure which extracts a key by using two-way classical communication. The asymptotic security of this protocol was first studied under individual attacks [464] and later against collective Gaussian attacks, with also a proof-of-concept experiment [536]. In general, the security of CV-QKD with non-Gaussian modulation remains an open question. In the asymptotic limit and against (general) collective attacks, its security was proven in Ref. [537] by using decoy Gaussian states. Recently, a lower bound to the asymptotic secret key rate under (general) collective attacks has been established in Ref. [538], without the use of additional decoy states. It is an open question to extend the security proof to the composable scenario, even though this can certainly be achieved under the (restricted) assumption of collective Gaussian attacks [539].

K. CV MDI-QKD

1. Basic concepts and protocol

As we know, MDI-QKD [52, 53] has been introduced to overcome a crucial vulnerability of QKD systems, i.e., the side-channel attacks on the measurement devices of the parties. The basic advantage of MDI scheme is that Alice and Bob do not need to perform any measurement in order to share a secret key. The measurements are in fact performed by an intermediate relay, which is generally untrusted, i.e., controlled by Eve. This idea can also be realized in the setting of CV-QKD with the promise of sensibly higher rates at metropolitan distances. The protocol was first introduced on the arXiv at the end of 2013 by Ref. [240] and independently re-proposed in Ref. [540].

The protocol proceeds as follows: Alice and Bob possess two modes, A and B respectively, which are prepared in coherent states $|\alpha\rangle$ and $|\beta\rangle$. The amplitude of these coherent states is randomly-modulated, according to a bi-variate Gaussian distribution with large variance. Each one of the parties send the coherent states to the intermediate relay using the insecure channel. The modes arriving at the relay, say A' and B', are measured by the relay by means of a CV-Bell detection [541]. This means that A' and B' are first mixed on a balanced beam splitter, and the output ports conjugately homodyned: on one port it is applied a homodyne detection on quadrature $\hat{q}$, which returns the outcome q_-, while the other port is homodyned in the $\hat{p}$-quadrature, obtaining an outcome p_+. The outcomes from the CV-Bell measurement are combined to form a new complex outcome $\gamma := (q_- + ip_+)/\sqrt{2}$ which is broadcast over a public channel by the relay.

For the sake of simplicity, let us consider lossless links to the relay. Then we can write $\gamma \simeq \alpha - \beta^*$, so that the public broadcast of γ creates *a posteriori* correlations between Alice's and Bob's variables. In this way, each of the honest parties may infer the variable of the other. For instance, Bob may use the knowledge of β and γ to compute $\beta^* - \gamma \simeq \alpha$ recovering Alice's variable up to detection noise [240]. Eve's knowledge of the variable γ does not help her to extract information on the individual variables α and β. This means that Eve needs to attack the two communication links with the relay in order to steal information, which results in the introduction of loss and noise to be quantified by the parties. In terms of mutual information this situation can be described writing that $I(\alpha : \gamma) = I(\beta : \gamma) = 0$, while as a consequence of the broadcast of variable γ Alice-Bob conditional mutual information is non-zero, i.e., $I(\alpha : \beta|\gamma) > I(\alpha : \beta) = 0$.

As discussed in Ref. [240], the best decoding strategy is to guess the variable of the party who is closer to the relay (i.e., whose link has the highest transmissivity). Also note that, as proven in Ref. [94], the whole raw data can be used to perform both secret key extraction and parameter estimation. This is because the protocol allows the parties to recover each other variable from the knowledge of γ, so that they can locally reconstruct the entire CM of the shared data without disclosing any information.

2. Asymptotic security

The security of CV MDI-QKD has been first studied in the asymptotic limit [240, 542] (including fading channels [478]). The asymptotic security analysis starts by considering the general scenario of a global unitary operation correlating all the uses of the protocol. However, using random permutations [85, 87], Alice and Bob can reduce this scenario to an attack which is coherent within the single use of the protocol. After de Finetti reduction, this is a joint attack of both the links and the relay. In particular, since the protocol is based on the Gaussian modulation and Gaussian detection of Gaussian states, the optimal attack will be Gaussian [7, 467, 468]. More details can be found in Ref. [240].

In analogy with the two-way CV-QKD protocol, a realistic two-mode Gaussian attack consists of Eve attacking the two links by using two beam-splitters of transmissivity η_A and η_B that are used to inject to modes E_1 and E_2 in a Gaussian state with CM given in Eq. (126). Detailed analysis of the possible two-mode attacks showed that, in the asymptotic regime, the optimal attack is given by the *negative EPR attack*, which corresponds to the case where $g = -g'$ with $g' = -\sqrt{\omega^2 - 1}$ in Eq. (126). In such a case Eve injects maximally entangled states with correlations contrasting those established by the CV-Bell detection, resulting in a reduction of the key rate.

Indeed, assuming the asymptotic limit of many uses, large variance of the signal modulation, and ideal reconciliation efficiency, it is possible to obtain a closed formula for the secret key rate of CV MDI-QKD at any fixed value of the transmissivities and excess noise. In particular, we can distinguish between two setups: the symmetric configuration, where the relay lies exactly midway the parties ($\eta_A = \eta_B$), and the asymmetric configuration ($\eta_A \neq \eta_B$). Assuming that Alice is the encoding party and Bob is the decoding party (inferring Alice's variable), the general expression of the asymmetric configuration takes the form

$$R_{\text{asy}} = \log_2 \frac{2\left(\eta_A + \eta_B\right)}{e\left|\eta_A - \eta_B\right|\bar{\chi}} + s\left[\frac{\eta_A \bar{\chi}}{\eta_A + \eta_B} - 1\right] - s\left[\frac{\eta_A \eta_B \bar{\chi} - \left(\eta_A + \eta_B\right)^2}{\left|\eta_A - \eta_B\right|\left(\eta_A + \eta_B\right)}\right], \tag{145}$$

where $\bar{\chi} := 2\left(\eta_A + \eta_B\right)/(\eta_A \eta_B) + \varepsilon$, ε is the excess noise, and $s\left(x\right)$ is defined in Eq. (116). For pure-loss links ($\varepsilon = 0$) the rate of Eq. (145) reduces to

$$R_{\text{asy}} = \log_2 \frac{\eta_A \eta_B}{e|\eta_A - \eta_B|} + s\left(\frac{2 - \eta_B}{\eta_B}\right) - s\left(\frac{2 - \eta_A - \eta_B}{|\eta_A - \eta_B|}\right). \tag{146}$$

The asymmetric configuration, under ideal conditions, allows to achieve long-distance secure communication. In particular, for $\eta_A = 1$ and arbitrary η_B the maximum achievable distance can be of 170 km (in standard optical fibers with attenuation 0.2 dB/Km) and key rate of 2×10^{-4} bit/use [543]. Under such conditions, the rate of Eq. (146) becomes

$$R_{\rm asy} = \log_2 \frac{\eta_B}{e(1-\eta_B)} + s\left(\frac{2-\eta_B}{\eta_B}\right), \tag{147}$$

which coincides with the RR rate of the one-way protocol with coherent states and heterodyne detection. The performance degrades moving the relay in symmetric position with respect to Alice and Bob. In such a case, we set $\bar{\chi} = 4/\eta + \varepsilon$ where $\eta := \eta_A = \eta_B$, and we write the rate [240, 542]

$$R_{\rm sym} = \log_2 \frac{16}{e^2 \bar{\chi}\left(\bar{\chi}-4\right)} + s\left(\frac{\bar{\chi}}{2} - 1\right). \tag{148}$$

For pure-loss links, this simplifies to

$$R_{\rm sym} = \log_2 \frac{\eta^2}{e^2(1-\eta)} + s\left(\frac{2-\eta}{\eta}\right), \tag{149}$$

and the maximum achievable distance is about 3.8 km of standard optical fiber from the relay.

3. *Composable security*

Finite-size analysis and composable security have been developed for CV MDI-QKD. In Refs. [544, 545] finite-size corrections have been studied assuming collective Gaussian attacks. The estimation of the channel parameters is provided within confidence intervals which are used to identify the worst-case scenario, corresponding to assuming the lowest transmissivity and the highest excess noise compatible with the limited data. The analysis showed that using signal block-size in the range of $10^6 - 10^9$ data points is sufficient to obtain a positive secret key rate of about 10^{-2} bits/use.

The composable secret key rate of CV MDI-QKD has been studied in Ref. [94]. Here we present a revised version which follows our Appendix B. Let us start from the asymptotic key rate of the protocol, which can be written as $R_{\infty|\gamma} = \xi I(\alpha : \beta|\gamma) - \chi_{E|\gamma}$ where ξ is the reconciliation efficiency, $I(\alpha : \beta|\gamma)$ is Alice-Bob mutual information conditioned on γ, and $\chi_{E|\gamma}$ is Eve's Holevo information conditioned on γ. Since the parties run the protocol for n times and they sacrifice $m_{\rm PE}$ runs for parameter estimation, only $n - m_{\rm PE}$ runs are used for key generation. Because of the imperfect parameter estimation, the asymptotic rate $R_{\infty|\gamma}$ has to be replaced by a finite-size rate $R_{\infty|\gamma} \to \frac{n-m_{\rm PE}}{n} R_{{\rm PE}|\gamma}$. As a first step, assume collective Gaussian attacks. In such a case, $R_{{\rm PE}|\gamma}$ can be evaluated using standard techniques orginally developed for one-way protocols (estimators and confidence intervals) [488, 489] and later extended [544, 545]. Then, the composable secret key rate under such attacks takes the form

$$\begin{aligned} R_n^{\epsilon} \geq & \frac{n-m_{\rm PE}}{n} R_{{\rm PE}|\gamma} \\ & - \frac{\sqrt{n-m_{\rm PE}}}{n} \Delta_{\rm AEP}\left(\frac{2}{3} p \epsilon_{\rm s}, d\right) \\ & + n^{-1}\left\{\log_2[p\left(1-2\epsilon_{\rm s}/3\right)] + 2\log_2 2\epsilon_{\rm h}\right\}, \end{aligned} \tag{150}$$

where the functional $\Delta_{\rm AEP}(...)$ quantifies the error committed by bounding the smooth-min entropy using the asymptotic equipartition property (AEP) [546]. The dimensionality parameter d describes the number of bits used in the analog-to-digital conversion sampling, by which the unbounded continuous variables used in the protocols (q, p) are mapped into discrete variables, described as a set of 2^{2d} elements (cardinality). Parameter p gives the probability of success of EC. The protocol has an overall epsilon security $\epsilon = \epsilon_{\rm cor} + \epsilon_{\rm s} + \epsilon_{\rm h} + \epsilon_{\rm PE}$, where $\epsilon_{\rm cor}$ is the conditional probability that Alice's and Bob's final sequences are different even though their hashes were the same (this contribution is included in the reconcilation parameter ξ), ϵ_s and $\epsilon_{\rm h}$ are the smoothing and hashing parameters, while $\epsilon_{\rm PE}$ is the error probability affecting parameter estimation (see Appendix B for more details on these quantities).

Starting from the rate in Eq. (150) one can derive a composable secret key rate under general coherent attacks by employing the methods in Ref. [93]. In fact, let us symmetrize the CV-MDI-QKD protocol with respect to a Fock-space representation G of the group $U(n)$ of $n \times n$ unitary matrices [93]. Call $m_{\rm ET}$ the number of uses that are employed in a suitable energy test, so that $m := m_{\rm PE} + m_{\rm ET}$ uses are sacrificed by the parties, and denote by d_A and d_B Alice's and Bob's effective local dimensions [93]. Then, the CV-MDI-QKD protocol is also ϵ'-secure under coherent attacks, with $\epsilon' = K^4\epsilon/50$ where the explicit expression of K is given in Eq. (B24) of Appendix B. In particular, the secret key rate will be modified to the following form

$$\begin{aligned} R_n^{\epsilon'} \geq & \frac{n-m}{n} R_{{\rm PE}|\gamma} - \frac{\sqrt{n-m}}{n} \Delta_{\rm AEP}\left(\frac{2}{3} p \epsilon_{\rm s}, d\right) \\ & + n^{-1}\left\{\log_2[p\left(1-2\epsilon_{\rm s}/3\right)] + 2\log_2 2\epsilon_{\rm h}\right\} \\ & - \frac{2}{n}\log_2\binom{K+4}{4}. \end{aligned} \tag{151}$$

Using this rate, one can check that CV MDI-QKD is composably secure against general attacks with block-sizes of the order of $10^7 - 10^9$ data points [94]. Note that Refs. [94, 95] also designed a novel parameter estimation procedure which is in principle more efficient (further analysis is however needed in order to establish the rigorous conditions for using this novel procedure within the fully composable framework).

4. Variants of CV MDI-QKD

Several schemes have been introduced to modify the original design of the CV MDI-QKD scheme. One approach was based on non-Gaussian operations, like noiseless linear amplifiers (NLA) and photon subtraction/addition (whose importance is well-known in entanglement distillation [547]). The use of NLAs in CV MDI-QKD setups was investigated in Ref. [548] while photon subtraction has been explored in Refs. [549, 550]. Among other approaches, CV MDI-QKD has been studied with squeezed states [551] (with composable security [552]), squeezed states and phase-sensitive optical amplifiers [553], discrete modulation (alphabet of four coherent states) [554], phase self-alignment [555], imperfect phase reference calibration [556], dual-phase modulation [557], relay-concatenation [558], atmospheric-fading channels [559], and unidimensional encoding [560]. A multi-party version of the CV MDI-QKD protocol [561] has been also introduced and it is discussed below.

5. Multipartite CV MDI-QKD

An interesting feature to achieve in quantum cryptography is the ability to reliably connect many trusted users for running a secure quantum conference or quantum secret-sharing protocols [562–568]. The MDI architecture, restricted to two [240] or three users [569], has been recently generalized in this direction. In the MDI network of Ref. [561], an arbitrary number N of remote users send Gaussian-modulated coherent states $|\alpha_k\rangle$ to an untrusted relay where a generalized multipartite Bell detection is performed. This detection consists of a suitable cascade of beam-splitters with increasing transmissivities $T_k = 1 - k^{-1}$, followed by $N-1$ homodyne detection in the $\hat{q}$-quadrature, and a final homodyne detection in the $\hat{p}$-quadrature. The result can be denoted as a single variable $\gamma := (q_2, \ldots, q_N, p)$ which is broadcast to all parties. This measurement is responsible for creating a bosonic type of Greenberger-Horne-Zeilinger (GHZ) correlations among the parties. Ideally, it projects on an asymptotic bosonic state with EPR conditions [570] $\sum_{k=1}^{N} \hat{p}_k = 0$ and $\hat{q}_k - \hat{q}_{k'} = 0$ for any $k, k' = 1, \ldots, N$.

After the measurement is broadcast, the individual variables α_k of the parties share correlations which can be post-processed to obtain a common secret key. To implement quantum conferencing, the parties choose the ith user as the one encoding the key, with all the others decoding it in DR. To realize quantum secret sharing, the parties split in two ensembles which locally cooperate to extract a single secret key across the bipartition. The scheme can always be studied in a symmetric configuration, where the users are assumed to be equidistant from the relay and the links are modeled by memoryless thermal channels, with same transmissivity and thermal noise (in case of asymmetries, one can in fact consider the worst-case scenario where each link of the network is replaced with a link with minimum transmissivity and maximum thermal noise). In this scenario, high rates are achievable at relatively short distances. The security of the quantum conferencing has been proved in both the asymptotic limit of many signals and the composable setting that incorporates finite-size effects. The analysis shows that, in principle, 50 parties can privately communicate at more than 0.1 bit/use within a radius of 40m. With a clock of 25MHz this corresponds to a key rate of the order of 2.5Mbits per second for all the users.

One of the features of the network proposed by Ref. [561] is its modular structure. In other words, each MDI star network can be seen as a single module implementing the protocol described above. Then, two different modules can be connected via a common trusted node and the corresponding conferencing keys composed via one-time pad to generate a single key for both modules. This procedure can be iterated many times, for an arbitrary number of modules, so that the shortest among the generated conferencing keys can be shared by the entire modular network.

VIII. EXPERIMENTAL CV-QKD

A. Introduction

As discussed in the previous section, the various kinds of CV-QKD protocols basically differ by the choice of input states (coherent or squeezed states), input alphabets (Gaussian or discrete) and detection strategy (homodyne or heterodyne detection). Most of these schemes have been tested in proof-of-concept experiments in a laboratory setting while a few have been going through different stages of developments towards real-life implementations. Specifically, the scheme based on Gaussian modulation of coherent states and homodyne detection has matured over the last 15 years [571], from a simple laboratory demonstration based on bulk optical components creating keys with very low bandwidth [572–575] to a robust telecom-based system that generates keys with relatively high bandwidth [576–589] and allows for in-field demonstrations [590, 591] and network integration [592–594]. In the following sections, we will first describe the experimental details of the standard point-to-point coherent state protocol with emphasis on the most recent developments followed by a discussion of some proof-of-concept experiments demonstrating more advanced CV-QKD protocols such as squeezed state QKD and measurement-device-independent QKD.

B. Point-to-point CV-QKD

The very first implementation of CV-QKD was based on coherent state modulation and homodyne detection [572]. The optical setup comprised bulk optical components and the operating wavelength was 780 nm.

This seminal work together with some follow-up experiments [573–575] constituted the first important generation of CV-QKD systems. Despite its successful demonstration of the concept of CV-QKD, it was however unsuitable for realizing robust long-distance and high-speed QKD in optical fibers because of the use of telecom-incompatible wavelengths, the relatively low mechanical stability of the systems and the low efficiency of the employed error-correction protocols.

To overcome these impediments, a new generation of CV-QKD systems was developed. This new generation made use of telecom wavelength, was mainly based on telecom components, combined optimized error-correction schemes and comprised several active feedback control systems to enhance the mechanical stability [577, 579, 581, 589]. With these new innovations, key rates of up to 1Mbps for a distance of 25km [577] and key rates of around 300bps for a distance of 100km [579] have been obtained. Two different field tests of CV-QKD through commercial fiber networks were performed over distances up to $\simeq$ 50km with rates $>$ 6kpbs [594], which are the longest CV-QKD field tests so far, achieving two orders-of-magnitude higher secret key rates than previous tests. More recently, Zhang et al. [595] were able to demonstrate CV-QKD over 202km of ultra-low loss optical fiber, closing the gap with the very long distances that are achievable with DV-QKD protocols.

A third generation of CV-QKD systems are now under development. They are based on the generation of power for a phase reference (or LO) at the receiver station in contrast to previous generations where the power of the LO was generated at the transmitter station and thus co-propagating with the signal in the fiber. These systems have also evolved from simple proof-of-concept demonstrations [596, 597] to technically more advanced demonstrations using telecom components [578, 582, 587, 592, 598, 599].

The basic optical configuration for realizing CV-QKD is shown in Fig. 9. The signal is modulated in amplitude and phase according to a certain distribution, typically following a continuous Gaussian distribution but also discrete distributions may be considered, e.g., quadrature phase shift keying (QPSK). It is then multiplexed in time, polarization and/or frequency with a phase reference (a strong local oscillator or a weak pilot tone) and subsequently injected into the fiber channel. At the receiver side, the signal and reference are de-multiplexed and made to interfere on a balanced homodyne (or heterodyne) detector. A subset of the measurement data are used for sifting and parameter estimation, while the rest are used for the generation of a secret key via EC and PA.

In Fig. 10 we show the main layouts of three different types of point-to-point CV-QKD experiments based on coherent state encoding with a Gaussian distribution. The three experiments represent important steps in the development of a telecom compatible QKD system, and they illustrate different techniques for encoding and detection. The experiment in Fig. 10a [581] applies a time-multiplexed LO propagating along the fiber with the signal while the experiments in Fig. 10b [578] and Fig. 10c [588] use a locally generated LO. The two latter experiments deviate by the signal encoding strategy (centered or up-converted base-band), the detection method (homodyne or heterodyne) and the phase and frequency difference determination. The experimental details are described in the figure caption and discussed in the following sections.

The overarching aim for all QKD systems is to generate secret keys with as high speed as possible and over as long distance as possible. These two quantifying parameters for QKD are strongly connected and they crucially depend on the system's clock rate, the excess noise produced by the system and the efficiency, quality and speed of the post-processing algorithms. With these critical parameters in mind, in the following we describe the technical details associated with transmitter, the receiver and the post-processing schemes.

1. *Coherent state encoding*

At the transmitter station, a telecom laser is often transformed into a train of pulses using an amplitude modulator with a certain clock rate (e.g. 1MHz [581] or 50MHz [577]). It is also possible to use a CW signal where the clock rate is determined by the measurement bandwidth. The clock rate should be large as it dictates the upper bound for the final rate of the secret key and the accuracy in estimating the parameters of the channel. However, using high clock rates also places extra demands on the detection system and the post-processing schemes as discussed later. After pulse generation, a pair of modulators encode information using different strategies. The traditional approach is to create a base band signal around the carrier frequency but in more recent implementations, the base band signal is up-converted to the GHz range to limit the amount of photons scattered from the carrier [598, 600]. As the base band signal is separated from the carrier in frequency, it is possible to significantly suppress the carrier through interference and thus reduce the amount of excess noise resulting from scattered carrier photons [582, 588].

2. *Detection*

At the receiver side, the signal is detected using either homodyne, dual-homodyning or heterodyne detection. A homodyne detector (sometimes called single-quadrature intradyne detection) basically consists of the interference of two light beams with identical frequencies - the signal and the local oscillator - on a balanced beam splitter, and two PIN diodes combined in subtraction and followed by a transimpedance amplification stage. In dual-homodyne detection (also known a phase diverse

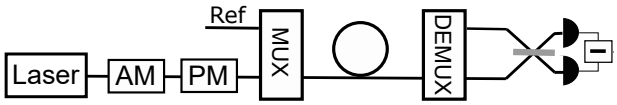

FIG. 9. Schematic setup of a generic experimental CV-QKD system. A laser beam is modulated with an amplitude modulator (AM) and a phase modulator (PM), and subsequently multiplexed (MUX) with a reference beam, sent through the optical fiber and de-multiplexed (DEMUX) at the receiver site. The quadrature variables of the signal is then measured with a homodyne or heterodyne detector. A subset of the measurement outcomes are used for the estimation of channel parameters while the rest are used for secret key generation using EC and PA.

detection), the LO and the signal are split in balanced couplers and sent to two individual homodyne detector to measured orthogonal phase-space components simultaneously. It enhances the phase estimation capabilities as two quadratures are measured but it also increases the complexity of the setup. The heterodyne detection scheme combines the advantages of the homodyne and dual-homodyne schemes: It mimics the low-complexity of homdyning and outputs the enhanced phase information of dual-homodyning. In heterodyne detection, the LO frequency is offset with respect to the carrier frequency of the signal, and therefore is down-converting the signal band to an intermediate frequency. Electronic downconversion is subsequently able to extract information about orthogonal phase space quadratures similar to dual-homodyning. It is worth noting that in the quantum community dual-homodyne detection is often referred to as a heterodyne detection while in the classical community heterodyne detection is reserved for the scheme described above. The gained signal information and noise penalties are basically similar for the two approaches but the hardware implementations are very different.

The figure of merits associated with the detectors are the quantum efficiency, the bandwidth and the electronic noise power relative to the shot noise power. Naturally, a large clock rate requires a large homodyne detector bandwidth. E.g. in Ref. [577] a detector with GHz bandwidth was used to resolve a 50MHz clock rate while in Ref. [581] a much lower bandwidth suffices to detect 1MHz clocked pulses. Homodyne detectors with large bandwidths are commercially available but they have relatively poor electronic noise performance and low quantum efficiency. Although these detectors have been widely used for CV-QKD, a new generation of improved homodyne detectors are under development [601, 602] which in turn will improve the performance of future QKD systems.

Homodyne and heterodyne detectors require a stable phase and frequency reference also known as a LO. Two strategies for realizing such a reference have been studied:

Transmission of local oscillator. The traditional strategy is to use a LO from the same laser as the signal and let it co-propagate with the signal through the optical fiber. Different techniques for combining the LO and signal have been tested including time multiplexing [589] and time-polarization multiplexing [581]. This method however entails some significant problems. First, due to channel loss, the power of the LO at the receiver is strongly reduced and thus in some cases insufficient for proper homodyne detection, second, the large power of the LO in the fiber scatters photons and thus disturbs the other quantum or classical fiber channels [577, 583, 586], and third, the co-propagating LO is vulnerable to side-channel attacks [581, 603]. The approach is thus incompatible with the existing telecom infra-structure and it opens some security loopholes.

Receiver generation of local oscillator. The alternative strategy which is now gaining increasing interest and which is compatible with classical coherent communication is to use a LO that is generated at the receiver station, thereby avoiding the transmission of the large powered LO through the optical fiber. To enable coherent detection between the LO and the signal, strong synchronization of the frequencies and phases is required. This can be performed in post-processing similar to carrier-phase recovery schemes applied in classical communication: The phase and frequency synchronization of the LO do not have to be carried out prior to signal measurements but can be corrected a posteriori in digital signal processing (DSP). This is done by measuring the phase and frequency differences and subsequently counter-rotate the reference axes to correct for the drifts. Phase and frequency estimation cannot be performed by using the quantum signal as a reference since its power is too weak. Therefore, a small reference beam or pilot tone must be sent along with the signal in the fiber channel to establish the phase and frequency at the receiver. However, it is important to note that this pilot tone is very dim compared to a LO and thus do not result in the complications associated with the transmission of a LO. CV-QKD with a locally generated LO have been demonstrated by transmitting the reference beam with the signal using time multiplexing [578, 599], frequency multiplexing [598] and frequency-polarization multiplexing [582]. In all these works, advanced DSP was used to correct for phase and frequency mismatch in post-measurements. The quality of the DSP algorithm is of utmost importance as inaccuracies in correcting for drifts directly lead to excess noise and thus a reduction of the resulting key rate and distance. Recovery of the clock has been achieved either by using or wavelength multiplexed clock laser [577], known patterns as a header to the quantum signal [582] or a second frequency multiplexed pilot tone [598].

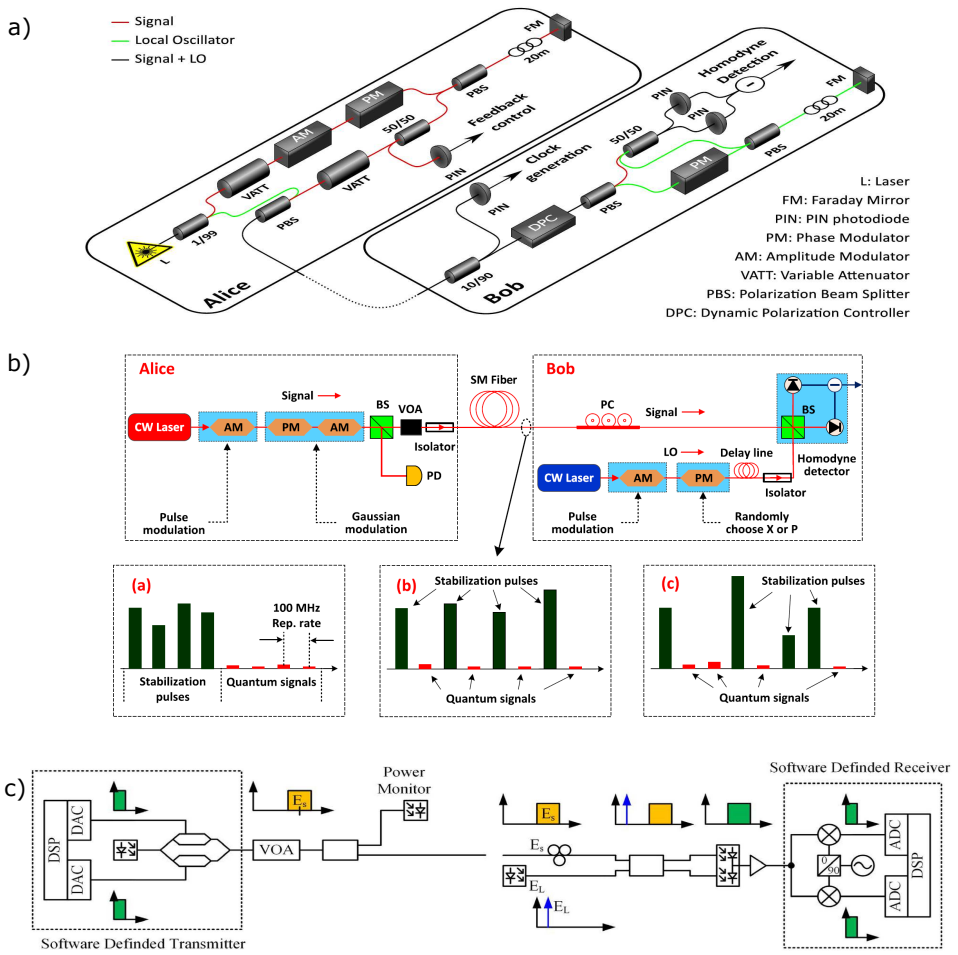

FIG. 10. Details of three experimental setups for CV-QKD based on a Gaussian coherent state alphabet. a) Coherent state pulses of 100ns with repetition rate 1MHz generated by a 1550nm telecom laser diode are split by an asymmetric beam splitter (99/1) into a signal beam (which is attenuated by variable attenuators (VATTs)) and a bright local oscillator. The signal is modulated by an amplitude (AM) and phase modulator (PM) and subsequently delayed by 200ns using a fiber delay line and a Faraday mirror. The local oscillator (LO) and signal are then multiplexed in time and further in polarization (with a polarizing beam splitter (PBS)) before being injected into the fiber channel. At Bob's site the LO and signal are polarization de-multiplexed with a PBS and a dynamical polarization controller (DPC) and time-multiplexed with a delay line of the LO. The pulses are finally interfered in a homodyne detector. The PM in the LO enables random π phase shift and thus random quadrature measurement. Taken from Ref. [581]. b) A CW telecom laser at 1550nm is transformed into 1nsec pulses with a repetition rate of 100MHz using an amplitude modulator (AM). The Gaussian distributed signal is produced with a pair of modulators (AM and PM) and its brightness is controlled with a variable optical attenuator (VOA). Phase synchronization signals are also produced in the modulators time-multiplexed with the quantum signal, either regularly as in (a) and (b) or randomly as in (c). The signals are injected into the channel and measured with a locally generated local oscillator at Bob. An AM produces local oscillator pulses while a PM randomly switches their phases by π to allow for a random quadrature measurement. Phase and frequency synchronization between LO and signal is attained through DSP of the data produced by the interference between the LO and the reference pulses. Taken from Ref. [578]. c) Transmitter and receiver are to a large extent controlled by software, thereby reducing the complexity of the hardware. At the transmitter, software defines the pulse shape and the modulation pattern (here QPSK), and it ensures that the single side-banded signal - concentrated in a 10MHz band - is upconverted and combined with a pilot-tone which is used for controlling the frequency carrier-frequency offset and the phase noise. At the receiver, the signal is measured with a heterodyne detector using a locally generated, and frequency shifted LO. The output of the detector is demodulated into amplitude and phase quadrature components with a sampling rate of 200MS/s. Carrier-frequency offset, phase noise, clock skew and quadrature imbalance are subsequently corrected in digital-signal-processing, and the output is fed to the post-processing steps for key generation. Taken from Ref. [588]. Figures adapted with permissions from: a) Ref. [581] ©NPG (2013), b) Ref. [578] ©OSA (2015), and c) Ref. [588] ©IEEE (2017).

3. Post-processing

A critical part for the successful completion of CV-QKD is the remaining post-processing protocols which include EC, parameter estimation and PA. The latter scheme is standard for any communication system (and thus will not be discussed further in this review) while the two former schemes are more complicated as they require sophisticated computational algorithms specifically tailored for CV-QKD. Furthermore, the performance of CV-QKD, that is key rate and distance, critically depends on the efficiency of the EC algorithm and the quality of parameter estimation scheme.

Error correction. In long-distance communication, the signal-to-noise ratio (SNR) of the acquired data is usually very low and thus the reconciliation of the Gaussian correlated variables is computationally very hard. Earlier versions of high-efficiency EC protocols for CV-QKD could only handle data with an SNR larger than around 1, thereby inherently limiting the secure communication distance to about 25km corresponding to a small metropolitan sized network. However, in recent years there have been numerous new developments in constructing high-efficiency error-correcting codes operating at very low SNR. New code developments have resulted in a significant improvement of the performance of CV-QKD and was the key stepping stone for realizing long-distance communication. E.g. the work in Ref. [581] performed EC with an efficiency of 96% at an SNR=0.08 as obtained with an 80km link while in Ref. [579] the efficiency was 95.6% at SNR=0.002 corresponding to a 150km fiber link. A rateless reconciliation protocol proposed in Ref. [604] can achieve more than 95% efficiency within the wide range of SNR from -20 to 0 dB, supporting the practical application of long distance CV-QKD.

The key innovation leading to these improved codes is to combine multi-edge low density parity check (LDPC) codes with multidimensional reconciliation techniques [576, 605–609]. A rate-adaptive reconciliation protocol was proposed in Ref. [608] to keep high efficiency within a certain range of SNR, which can effectively reduce the SNR fluctuation of the quantum channel on the system performance. Throughputs of 25Mbit/s [606] and 30Mbit/s [609] have been achieved, which are not yet compatible with high speed system using clock speeds of more than 100 MHz [578]. However, the speed of the LDPC decoder do not currently representing the key bottleneck in extending the distance of QKD. One of the main limiting factors in extending the distance is the efficiency and quality in estimating the parameters of the system.

Parameter Estimation. The quality of practical parameter estimation is crucial for the reliable extraction of secret keys for long-distance communication. In addition to the estimation of the phase and frequency differences for LO adjustments as discussed above, it is important also to estimate the transmitter's modulation variance μ, the channel transmittance η and the variance of the excess noise ε. The two variances are expressed in shot noise units and thus a careful calibration of the shot noise level is also required. Once all parameters are estimated, they are used to compute the bounds on the Eve's information. However, the reliability in warranting security strongly depends on the precision in estimating the parameters. Very large data block sizes are often required to reduce the finite-size effects to a level that is sufficiently low to claim security (see also Sec. IX). As an example, in Ref. [581], a secret key was generated by using blocks of size 10^9 for a 80km channel but by reducing the block size to 10^8, no key could be extracted as a result of the finite-size effect. Likewise in Ref. [579] a block size of 10^{10} was used to enable secret key generation over 100km. To extend the distance further, even larger data blocks are required. This places more stringent demands on the stability of the system to allow for longer measurement series, and it calls for an increase in the measurement rate realized by a larger clock rate and higher detector bandwidth.

Practical key rate: Within a certain data block, half of the data are used for sifting (if homodyne detection is used), a subset is used for parameter estimation and another subset is used for phase synchronization of the local oscillator. The remaining data are then used for secret key generation and thus undergo EC with efficiency ξ and PA. In a stable system it is also possible to perform EC first, using the SNR estimate from the previous round, and then use all the data for parameter estimation. If the clock rate is given by C and the fraction of data used for key extraction is f, the final practical key rate in RR is given by

$$R_{\text{prac}} = fC(\xi I_{AB} - \chi_{BE}) \tag{152}$$

where I_{AB} is Alice-Bob mutual information and χ_{BE} is Eve's Holevo information on Bob's variable. The fastest system of today produces secret keys of 1Mbps (for 25km) while the longest distance attained is 150km with a key rate of 30kbps. Both realizations are secure against collective attacks and include finite-size effects.

C. Implementation of advanced CV-QKD

The point-to-point coherent state protocol discussed above is by far the most mature CV-QKD scheme developed, and furthermore, since it is reminiscent of a coherent classical communication system, it is to some extend compatible with the existing telecom networks. However, the point-to-point scheme might in some cases be vulnerable to quantum hacking attacks and it possess some limitations in speed and distance. To circumvent some of these vulnerabilities and limitations, more advanced CV-QKD protocols have been proposed and experimentally tested in proof-of-principle type experiments using bulk optical components and often without post-processing. In the following we briefly discuss these demonstrations.

1. Squeezed-state protocols

There have been two main implementations of QKD based on squeezed states. The schemes were discussed in Section VII C, and were shown to be capable of extending the distance of QKD [484] or to enable composable security [610]. In the following we briefly address the experimental details of these realizations.

In both experiments [484, 610], two-mode squeezed states were generated by interfering two single-mode squeezed states on a balanced beam splitter. The squeezed states were produced in cavity-enhanced parametric down-conversion using non-linear crystals, such as periodically-poled potassium titanyl phosphate (PP-KTP), inside high-quality optical cavities [611]. One mode of the two-mode squeezed state was measured with high-efficiency homodyne detection at the transmitter station while the other mode was transmitted in free space to Bob who performed homodyne/heterodyne measurements. The homodyne measurements at Alice's station steered the state at Bob's station into a Gaussian distribution of amplitude or phase quadrature squeezed states and thus the scheme is effectively similar to a single-mode squeezed state protocol. The noise suppression below shot noise of the two-mode squeezed states were measured to be 3.5dB at 1064nm [484] and 10.5dB at 1550nm [610]. The clock rate of the experiments was in principle limited by the bandwidth of the cavity-enhanced parametric amplifiers (21MHz in Ref. [484] and 63MHz in Ref. [610]) but in the actual implementations, the bandwidth was set to a few kHz given by filters in the homodyne detectors.

In such squeezed state systems, the size of the alphabet is often limited to the degree of anti-squeezing and thus it is not possible in practice to maximize the key rate with respect to the modulation depth. However, in Ref. [484] the Gaussian alphabet was further extended by modulating the mode sent to Bob with a pair of modulators. With this approach, the system becomes more robust against excess noise and thus it is possible to extend the distance over which secure communication can be realized. The squeezed state experiment in Ref. [610] was used to demonstrate CV-QKD with composable security. E.g. for a channel loss of 0.76 dB (corresponding to 2.7km fiber), they achieved composable secure key generation with a bit rate of 0.1 bit/sample using a reconciliation efficiency of 94.3%. Furthermore, the system was also used to demonstrate one-sided-device-independent security against coherent attacks.

In a recent work [612], it was experimentally demonstrated that by using squeezed states encoding with a uni-dimensional and small alphabet, it is possible to completely eliminate the information of Eve in a purely lossy channel. This reduces the computational complexity of the post-processing protocols and therefore might be of interest in future CV-QKD schemes despite the limited size of the alphabet. Finally, in this context, it is also worth to mention the recent 50km experiment in optical fiber based on the direct distribution TMSV states [613].

2. CV MDI-QKD

As discussed in Section IV G, MDI-QKD schemes circumvent quantum hacking attacks on the measurement system. A CV version of the MDI-QKD scheme (see Section VII K) has been realized in a proof-of-concept experiment [240]. Here amplitude and phase modulation were applied to CW beams both at Alice's and at Bob's site. The modulated beams underwent free space propagation before being jointly measured in a CV Bell state analyzer. Such an analyzer consists normally of a balanced beam splitter, in which the two incoming beams interfere, followed by two homodyne detectors measuring orthogonal quadratures. In the current experiment, however, the Bell analyzer was significantly simplified by using the carriers of the signals as local oscillators: Through a proper phase space rotation of the carriers enabled by the interference, information about the sum of the amplitude quadratures and the difference of the phase quadratures were extracted by simple direct measurements of the beam splitter output modes followed by an electronic subtraction and summation. Losses of the channels were simulated in the experiments by varying the modulation depths of the modulators, and for an attenuation of respectively 2% and 60% for the two channels, a bit rate of 0.1 secret bits per use was deduced from a measured excess noise of 0.01SNU and an assumed post-processing efficiency of 97%.

IX. THEORETICAL SECURITY ASPECTS

A. Finite-size analysis in QKD

Here, we describe how to lift the security analysis of QKD protocols from more physical considerations to the same level of rigor as found for classical primitives in theoretical cryptography. This is crucial to assure that QKD can be safely used as a cryptographic routine in any type of applications. We have already seen the general structure of QKD protocols and discussed the precise composable security criterion in Section II. Here we describe in detail how to give mathematically precise finite key security analyzes. We emphasize that such finite key analyzes are crucial to understand the security properties of any practical quantum hardware, just as every distributed key will have finite length and will only be approximately secure.

We start by reviewing the different known methods for finite key analyzes in Section IX B and then describe in more detail the state-of-the-art approach based on entropic uncertainty relations with side quantum information (Section IX C). As we will see, the security intuitively follows from the two competing basic principles of quantum physics: the uncertainty principle and entanglement.

We then discuss CV protocols in Section IX D and end with an outlook Section IX E, commenting on extensions to device-independent QKD.

B. Finite-size statistical analysis

It is natural to split the finite-size statistical analysis into two steps, and in fact most security proofs respect that structure. In the first step of PA, discussed in Subsection IX B 1, we explain how the criterion for composable security (introduced in Subsection II D) can be satisfied as long as we can guarantee a sufficiently strong lower bound on a quantity called the *smooth min-entropy* $H_{\min}^{\varepsilon}$ of Alice and Bob's corrected raw key conditioned on Eve's side information. The second step, discussed in Subsection IX B 2 is then to find such lower bounds.

1. Privacy amplification (PA)

PA is a procedure that allows Alice and Bob, who are assumed to share a random bit string (called the raw key) about which the eavesdropper has only partial information, to extract a shorter random bit string (the secret key) that is guaranteed to be uncorrelated with the eavesdropper's information. To make this more precise, we first need to define what *partial information* about the raw key means. Since we are interested in finite-size effects, it turns out that the proper way to measure the eavesdropper's information is by assessing its probability of guessing the random bit string. This is done using the *smooth min-entropy* [86]. The higher the smooth min-entropy of the eavesdropper on the raw key, the more secret key can be extracted using the PA scheme.

A simple way of extracting Alice's secret key is by applying a random hash function to her raw bit strings (technically, the random hash function must form a two-universal family). This was shown to work even when the eavesdropper has a quantum memory by Renner [86] who provided a quantum generalization of the so-called *Left-over Hashing Lemma*. This method has the advantage that the random seed used to decide on the hash function is independent of the resulting random bit string (i.e. the extractor is strong) and hence the seed can be published over the public channel to Bob. This way both Alice and Bob can apply the same hash function, and since their initial bit strings agreed their final strings will too. Thus, we end up with Alice and Bob both holding bit strings that are independent of the eavesdropper's information — and thus a secret key between them has been successfully established.

Therefore, as long as we can guarantee some lower bound on the min-entropy of the raw key, PA can be invoked to extract a secret key.

2. Guaranteeing large smooth min-entropy

There are a plethora of techniques available to analytically show that the smooth min-entropy of the raw key is indeed large given the observed data but it is worth summarizing the most important ones. We give a more detailed exposition of one of the most powerful techniques, based on entropic uncertainty relations, in Section IX C. We restrict our attention here to finite-dimensional quantum systems and discuss CV protocols in Section IX D.

a. Asymptotic equipartition and exponential de Finetti [86]. Under the i.i.d. assumption where the total state of the system after the quantum phase has product form, the smooth min-entropy can be bounded by the von Neumann entropy of a single measurement, using the so-called quantum asymptotic equipartition property [614]. This von Neumann entropy can in turn be estimated using state tomography, performed on the quantum state shared between Alice and Bob. This approach often works directly when we only consider individual or collective attacks, as the state after the distribution phase then usually admits an i.i.d. structure. However, with general coherent attacks such a structure can no longer be guaranteed. Nonetheless, Renner [86], in his seminal work establishing the security of BB84 for finite length keys, uses an exponential de Finetti theorem to argue that, in a suitable sense, the general case can be reduced to the i.i.d. setting as well. This comes at a significant cost in extractable key, however.

b. Asymptotic equipartition and post-selection [615]. In particular the latter reduction, using the exponential de Finetti theorem, leads to large correction terms that make the security proof impractical. It can be replaced by a significantly tighter method (based on similar representation-theoretic arguments), the so-called post-selection technique [615].

c. Virtual entanglement distillation [97, 616]. This technique can be traced back to one of the early security proofs by Shor and Preskill [97] and has been adapted to deal with finite key lengths by Hayashi and Tsurumaru [616]. The basic idea is to interpret part of the raw key as a syndrome measurement of a Calderbank-Shor-Steane (CSS) code and use it to virtually distill entanglement on the remaining qubits. The crucial point is that this can be done after measurement (hence virtual) so that no multi-qubit quantum operations are required. The correctness and secrecy of Alice and Bob's key then follows directly from the fact that they effectively measured a close to maximally entangled state.

d. Entropic uncertainty relations with side quantum information [90, 617]. This approach is based on an entropic uncertainty relation [618] that allows us to directly reduce the problem of lower bounding the smooth min-entropy of the raw key conditioned on the eavesdropper's information with a different, more tractable problem. Namely, instead of bounding the min-entropy we need only ensure that the correlations between Alice's and Bob's raw keys are strong enough in an appropriate

sense, which can be done by a comparably simple statistical tests. This reduction naturally deals with general attacks and gives tight bounds for finite keys.

The intuition and some of the details behind this approach will be discussed in detail in the next section. The proof technique has recently been reviewed in detail and in a self-contained way in [619].

e. Entropy accumulation [620]. A recent proof technique uses entropy accumulation [213] to argue that the smooth min-entropy accumulates in each round of the protocol. This security proof naturally deals with the so-called device independent setting (see Section IV). The bounds, while still not as strong as the ones that can be achieved using the last two methods discussed above, have recently been improved in [228].

C. Uncertainty principle versus entanglement: an intuitive approach to QKD security

One of the basic principles of quantum physics that is intuitively linked to privacy is Heisenberg's uncertainty principle [621]. In its modern information-theoretic form due to Maassen-Uffink [622] it states that for any two measurements X, Z with eigenvectors $|x\rangle, |z\rangle$, respectively, we have

$$H(X) + H(Z) \geq -\log_2 \max_{x,z} |\langle x|z\rangle|^2, \tag{153}$$

where $H(X) = -\sum_x p_x \log_2 p_x$ denotes the entropy of the post-measurement probability distribution. Importantly, the bound on the right-hand side is independent of the initial state and the first ideas of directly making use of this uncertainty principle for security proofs can be traced back to [623, 624].

It turns out, however, that when taking into account the most general coherent attacks, the adversary might have access to a quantum memory and with that to the purification of the state held by the honest parties. Now, when starting with a maximally entangled bipartite state Φ_{AB} and applying measurement X or Z on the A-system, then it is easily checked that there always exists a measurement on the B-system that reproduces the measurement statistics on A, independent if X or Z was measured! This phenomenon was first discussed in the famous EPR paper [625] and in terms of entropies it implies that

$$H(X|B) + H(Z|B) = 0, \tag{154}$$

where $H(X|B) := H(XB) - H(B)$ denotes the conditional von Neumann entropy of the post-measurement classical-quantum state. We emphasize that this is in contrast to classical memory systems B, for which the left-hand side of (154) would always respect the lower bound from (153).

Luckily, entanglement turns out to be monogamous in the sense that for tripartite quantum states ABC the more A is entangled with B the less A can be entangled with C (and vice versa). Moreover, it is now possible to make this monogamy principle of entanglement quantitatively precise by showing that the Maassen-Uffink bound is recovered in the tripartite setting [617]

$$H(X|B) + H(Z|C) \geq -\log_2 \max_{x,z} |\langle x|z\rangle|^2. \tag{155}$$

It is this type of entropic uncertainty relation with quantum side information that is employed for deducing the security of QKD. (Entropic uncertainty relations with and without quantum side information as well as their applications in quantum cryptography are also reviewed in [626].) Note that there is now no need to distinguish between individual, collective, and coherent attacks but rather (155) directly treats the most general attacks. This is crucial for not ending up with too pessimistic estimates for finite secure key rates.

To continue, we actually need an entropic uncertainty relation suitable for the finite key analysis. This is in terms of smooth conditional min- and max-entropies, taking the form [618]

$$H^{\varepsilon}_{\min}(Y^n|E\Theta^n) + H^{\varepsilon}_{\max}(Y^n|\hat{Y}^n) \geq n, \tag{156}$$

where Y^n is Alice's raw key (of length n bits), $\hat{Y}^n$ is Bob's raw key, E denotes Eve's information and Θ^n labels the basis choice of the measurements made in the n rounds by the honest parties (e.g., for BB84 if X or Z was chosen in each round). An information reconciliation protocol can then be used to make sure that Alice and Bob hold the same raw key. Taking into account the maximum amount of information that gets leaked to the eavesdropper in this process, denoted leak_{EC}, this yields the bound

$$H^{\varepsilon}_{\min}(Y^n|E\Theta^n) \geq n - H^{\varepsilon}_{\max}(Y^n|\hat{Y}^n) - \text{leak}_{\text{EC}}. \tag{157}$$

Therefore, it only remains to statistically estimate $H^{\varepsilon}_{\max}(Y^n|\hat{Y}^n)$, which can be done by calculating the number of bit discrepancies between Alice and Bob on a random sample of the raw keys [90].

D. Composable security of CV-QKD protocols

For CV protocols, two methods are known to obtain finite-size, composable security proofs, against general attacks: 1) entropic uncertainty relations and 2) the Gaussian de Finetti reduction. Note that entropic uncertainty relations apply to protocols where a TMSV state is distributed between Alice and Bob, who then locally measure by homodyne detection. On the other hand, the Gaussian de Finetti reduction (or post-selection method) is for protocols where Alice and Bob measure their local mode by heterodyne detection: this is equivalent to Alice sampling coherent states from a Gaussian distribution of amplitudes, which are then sent to Bob.

1. Entropic uncertainty relations

For protocols based on the transmission of TMSV states measured via homodyne detection (therefore squeezed-state protocols), the proof principle via entropic uncertainty applies as well, leading to a tight characterisation [91, 92]. This follows the intuition from the early work [623] and is based on the entropic uncertainty relations with side quantum information derived in [627, 628].

Importantly, the analysis does not directly work with continuous position and momentum measurements but rather with a binning argument leading to discretized position and momentum measurements. Namely, a finite resolution measurement device gives the position Q by indicating in which interval $\mathcal{I}_{k;\delta} := \big(k\delta, (k+1)\delta\big]$ of size $\delta > 0$ the value q falls ($k \in \mathbb{Z}$). If the initial state is described by a pure state wave function $|\psi(q)\rangle_Q$ we get $\{\Gamma_{Q_\delta}(k)\}_{k\in\mathbb{Z}}$,

$$\Gamma_{Q_\delta}(k) = \int_{k\delta}^{(k+1)\delta} \big|\psi(q)\big|^2 \, \mathrm{d}q \tag{158}$$

with entropy

$$H(Q_\delta) := -\sum_{k=-\infty}^{\infty} \Gamma_{Q_\delta}(k) \log_2 \Gamma_{Q_\delta}(k). \tag{159}$$

For these definitions we then recover a discretized version of the of Everett-Hirschman [629, 630] entropic uncertainty relation

$$\begin{aligned} H(Q_\delta) + H(P_\delta) \geq \log_2(2\pi) \\ - \log_2 \left[\delta_q \delta_p \; S_0^{(1)} \left(1, \frac{\delta_q \delta_p}{4}\right)^2 \right], \end{aligned} \tag{160}$$

where $S_0^{(1)}(\cdot,\cdot)$ denotes the 0th radial prolate spheroidal wave function of the first kind [631]. Extending this to quantum side information we find similarly as in the finite-dimensional case that [627]

$$\begin{aligned} H(Q_{\delta q}|B) + H(P_{\delta p}|C) \geq \log_2(2\pi) \\ - \log_2 \left[\delta_q \delta_p \; S_0^{(1)} \left(1, \frac{\delta_q \delta_p}{4}\right)^2 \right]. \end{aligned} \tag{161}$$

Extending this to the smooth min-entropy then allows for the same security analysis as in (155).

2. Gaussian de Finetti reduction

For infinite-dimensional systems, finite-key approaches based on exponential de Finetti or post-selection unfortunately fail [632]. The post-selection method exploits the symmetry of the protocol under permutation of the signals sent from Alice to Bob. The methods allows us to obtain the security against general attacks from the security against collective attacks, which are invariant under permutation of the signals. This generalization is obtained at the cost of increasing the security parameter of the protocol (and thus decreasing the security) by a multiplicative factor. Such a multiplicative factor is proportional to the dimension of the symmetric subspace.

If the information carriers live in a d-dimensional Hilbert space, the dimension of the symmetric space for n signals is upper bounded by $(n+1)^{d^2-1}$. As long as d is finite (and small) this overhead is sustainable as it increases polynomially with n. Obviously the method fails if one attempts to apply it directly to CV protocols, as the Hilbert space of each single signal state has infinite dimensions. The introduction of a cutoff in the Hilbert space, following from a suitable energy constraint does not solve this problem, and leads to rather pessimistic finite-key rate estimates [87].

A security proof for a certain class of CV protocols has been recently obtained by applying a modified post-selection method, where the permutation symmetry is replaced by a more specific symmetry that reflects the peculiar features of these protocols [93, 499, 633, 634]. In CV protocols based on heterodyne detection, the relevant symmetry group is a suitable Fock-space representation G of the group $\mathrm{U}(n)$ of $n \times n$ unitary matrices [93]. Denote as $\mathcal{P}$ the CV QKD protocol. We say that the protocol is covariant under the action of the symmetry group if, for any $g \in G$, there exists a (trace non-increasing) completely positive map $\mathcal{K}_g$ such that [93]

$$\mathcal{P} \circ g = \mathcal{K}_g \circ \mathcal{P}. \tag{162}$$

By extending the post-selection proof method, it is then possible to prove that the composable finite-size security under a general coherent attack follows from the composable finite-size security against collective Gaussian attacks. More precisely, if protocol $\mathcal{P}$ is secure against collective Gaussian attacks with a security parameter ϵ, and it is also covariant under the symmetry group, then the protocol is also secure against general attacks, with security parameter $\epsilon' = \frac{K^4}{50}\,\epsilon$, where K is a suitable parameter. See Appendix B for more details.

E. Extensions and Outlook

Going forward from a theoretical viewpoint some of the main challenges in the security analysis of quantum key distribution schemes are:

- To refine the mathematical models on which the security proofs are based to more accurately match the quantum hardware used in the actual implementations. This is of crucial importance to decrease the vulnerability to quantum hacking, which is typically based on side channel attacks exploiting weaknesses of the quantum hardware [204]. Intensified collaborations of theorists and experimental-

ists should help to close this gap between realistic implementations and provable security.

- Device independent QKD makes fewer assumptions on the devices used and hence naturally takes care of issues with imperfect hardware. However, it still remains to determine the ultimate finite key rates possible in device-independent QKD. The state-of-the-art works are based on entropy accumulation [213, 620] and have recently been improved [228]. In contrast to the tightest device dependent approach based on entropic uncertainty relations with side quantum information (as presented in Section IX C), the lower bounds on the smooth min-entropy are achieved in a device independent way by ensuring that there is enough entanglement present. The details are beyond the scope of this review but the open question is then to determine if the same experimentally feasible trade-off between security and protocol parameters is available as in the device dependent case.

- From a more business oriented perspective it is crucial to argue that QKD schemes not only offer security in an abstract information-theoretic sense but are actually more secure in practice compared to widely used classical encryption schemes. That is, it is important to realize that in typical every day use cases no cryptographic scheme is absolutely secure but instead the relevant question is how much security one can obtain for how much money. Given the ongoing development around post-quantum or quantum-secure-cryptography [635] we believe that there is still significant territory to conquer for QKD.

X. QUANTUM HACKING

A practical implementation of QKD protocols is never perfect and the performance of protocols depends on the applicability of the security proofs and assumptions to the real devices [636], as well as on numerous parameters, including post-processing efficiency and the level of noise added to the signal at each stage (including the noise added due to attenuation). Broadly speaking, quantum hacking [637] encompasses all attacks that allow an eavesdropper to gain more information about messages sent between the trusted parties than these parties assume to be the case, based on their security proofs. Since security proofs are constructed on physical principles, this can only be the case if one or more of the assumptions required by the security proof does not hold [638]. If this is the case, the proof will no longer be valid, and Eve may be able to gain more information about the message than Alice and Bob believe her to have. These assumptions include the existence of an authenticated channel between Alice and Bob, the isolation of the trusted devices (i.e. that Eve cannot access Alice and Bob's devices) and that the devices perform in the way that they are expected to. Certain forms of quantum hacking have already been mentioned in this review, such as the photon-number splitting (PNS) attack against DV-QKD protocols.

Exploitable imperfections in the trusted parties' devices that allow quantum hacking are called side-channels. These could take the form of losses within the trusted devices that could potentially contribute to Eve's information about the signal, or added noise within the devices that could be partially controlled by Eve, in order to influence the key data. Such partially controllable losses and noises constitute threats to the security of QKD protocols, if overlooked. Quantum hacking often serves one of two purposes: to directly gain information about the secret key or to disguise other types of attack on a protocol, by altering the trusted parties' estimation of the channel properties. To restore security, the trusted parties can either incorporate the side-channels into their security analysis, in order to not underestimate Eve's information, or can modify their protocol to include countermeasures. In this section, we will discuss some common side-channel attacks, and how their effects can be mitigated. It is clear that the study of quantum hacking is an important aspect for the real-life security of QKD implementations; it is central to the ongoing effort for the standardization of QKD by the European Telecommunications Standards Institute. See the recent white paper on the topic [637].

A. Hacking DV-QKD protocols

The security proofs for many DV protocols, such as BB84 [639] and B92 [113], assume the use of single-photon sources. However, real QKD implementations often use strongly attenuated laser pulses, rather than true single-photon sources, which will send some pulses with multiple photons [640]. The existence of such pulses allows the use of the (previously mentioned) PNS attack. This is where Eve beamsplits off all but one of the photons from the main quantum channel. Since Bob is expecting to receive a single-photon pulse, and since this pulse will be undisturbed (if Eve does not carry out any other attack), the trusted parties will not detect any additional error on the line. Eve can then store the photons she receives in a quantum memory until after all classical communication has been completed. She can then perform a collective measurement on her stored qubits, based on the classical communication, to gain information about the secret key, without revealing her presence to the trusted parties. For instance, in BB84, she will know all of the preparation bases used by Alice, after the classical communication is complete, and so will be able to gain perfect information about all of the key bits that were generated by multi-photon pulses.

1. PNS and intensity-based attacks

A method used to counter the PNS attack is the use of decoy states. For instance, the BB84 protocol can be modified into BB84 with decoy states [159–163]. In this protocol, Alice randomly replaces some of her signal states with multi-photon pulses from a decoy source. Eve will not be able to distinguish between decoy pulses, from the decoy source, and signal states, and so will act identically on both types of pulse. In the post-processing steps, Alice will publicly announce which pulses were decoy pulses. Using the yields of these decoy pulses, the trusted parties can then characterize the action of the channel on multi-photon pulses, and so can detect the presence of a PNS attack. They can then adjust their key-rate accordingly, or abort the protocol if secret key distribution is not possible.

Imperfections in Alice's source can give rise to exploitable side-channels, which can allow Eve to carry out the PNS attack undetected. Huang et al [641] tested a source that modulates the intensity of the generated pulses by using different laser pump-currents, and found that different pump-currents cause the pulse to be sent at different times, on average. This means that the choice of intensity setting determines the probability that the pulse will be sent at a given time, and hence it is possible for Eve to distinguish between decoy states and signal states, based on the time of sending. Eve can then enact the PNS attack on states that she determines to be more likely to be signal states, whilst not acting on states that she determines to be likely to be decoy states. This would allow her PNS attack to go undetected by the trusted parties. They then bounded the key rate for BB84 with decoy states, using an imperfect source (for which the different intensity settings are in some way distinguishable).

Huang et al. [641] also tested a source that uses an external intensity modulator to determine the intensity settings (meaning that the intensity is modulated after the laser pulse is generated). They found that such sources do not give a correlation between intensity setting and sending time, giving a possible countermeasure to attacks based on this side-channel. Another option is for Alice to change the time at which the pump-current is applied depending on the intensity setting, in order to compensate for this effect. Eve may be able to circumvent this countermeasure, however, by heating Alice's source using intense illumination. Fei et al. [642] found that if gain-switched semiconductor lasers are heated, the pulse timings of different intensity settings shift relative to each other, so Alice will no longer be able to compensate for the timing differences unless she knows that they have been changed. They also found that heating the gain medium can cause the time taken for the carrier density to fall to its default level between pulses to increase. This could lead to unwanted (by Alice) correlations between pulses, which could compromise the security of the protocol.

2. Trojan horse attacks

Another form of hacking that can be used against DV-QKD protocols is the Trojan horse attack (THA) [643–645]. This encompasses a variety of different types of attack that involve sending quantum systems into one or both of the trusted parties' devices in order to gain information. For instance, Vakhitov et al. [645] considered the use of large pulses of photons to gain information about Alice's choice of basis and about Bob's choice of measurement basis, in BB84 and B92. The information is gained by sending a photon pulse into the trusted device via the main channel and performing measurements on the reflections. Considering the case in which the qubit is encoded via a phase shift, if Eve is able to pass her pulse through Alice's phase modulator, measuring the resulting pulse will give some information about the signal state. This is possible because Alice's phase modulator operates for a finite amount of time (rather than only being operational for exactly long enough to modulate the signal state), giving Eve a window in which to send her own pulse through, to be modulated similarly to the signal pulse. The process of Eve gaining information about the basis choice via reflectometry is described in some detail by Gisin et al. [643].

The information may be partial, giving only the basis used, or may directly give the key bit. Even in the case in which only the basis can be obtained, the security of the protocol is still compromised, as Eve is now able to always choose the same measurement basis as Alice, for an intercept and resend attack, gaining complete information about the key without introducing any error. Alternatively, Eve may be able to target Bob's device. For B92 or SARG04, it is sufficient to know Bob's measurement basis in order to gain complete information about the key. In BB84, if Eve is able to ascertain the measurement basis that Bob will use prior to the signal state arriving at his device, she can carry out an undetectable intercept and resend attack by choosing the same basis as him. Vakhitov et al. [645] also note that even if Eve only gains information about Bob's basis after the signal state has been measured, this can help with a practical PNS attack, since it reduces the need for a quantum memory (Eve can carry out a measurement on the photons she receives immediately, rather than having to wait until after all classical communication is completed). This does not aid an eavesdropper who is limited only by the laws of physics, but it could help one who is using current technology.

A number of methods of protecting against THAs have been proposed. Vakhitov et al. [645] suggested placing an attenuator between the quantum channel and Alice's setup, whilst actively monitoring the incoming photon number for Bob's setup. Gisin et al. [643] calculated the information leakage due to a THA, assuming heavy attenuation of the incoming state, and suggested applying phase randomization to any outgoing leaked photons. Lucamarini et al. [646] calculated the key rates for BB84,

with and without decoy states (in the without case, assuming an ideal single-photon source), in the presence of a Trojan horse side-channel, parameterized by the outgoing photon number of the Trojan horse state. They then proposed an architecture to passively limit the potential information leakage via the Trojan horse system (without using active monitoring). This was done by finding the maximum incoming photon number in terms of the Laser Induced Damage Threshold (LIDT) of the optical fibre, which can be treated as an optical fuse. The LIDT is the power threshold over which the optical fibre will be damaged. The minimum energy per photon, which depends only on the frequency of the photons, is lower-bounded using an optical fibre loop, which selects for frequency (photons of too low a frequency will not totally internally reflect, and so will leave the loop). The maximum time for Eve's pulse is also known and bounded by the time it takes Alice's encoding device to reset between signals. Hence, the maximum number of photons per pulse can be upper-bounded. By correctly setting the attenuation of incoming photons, Alice can then upper-bound and reduce the information leakage due to any THA.

Jain et al. [644] considered using THAs at wavelengths lower than the signal pulse in order to reduce the risk of detection by the trusted parties. This could reduce the efficacy of active monitoring of the incoming average photon number, as detectors often have a frequency band at which they are most sensitive, and so may not detect photons outside of this band. It could also lead to reduced attenuation of the Trojan state by passive attenuators, as the transmittance of a material is frequency-dependent. Sajeed et al. [647] carried out experimental measurements on equipment used in existing QKD implementations at a potential THA wavelength as well as at the wavelength used by the signal state, and found that the new wavelength (1924 nm) reduced the probability of afterpulses in Bob's detectors, which could alert the trusted users to the attack. This came at the cost of increased attenuation and a lower distinguishability, due to the phase modulator being less efficient at the new wavelength. Jain et al. [644] suggest the use of a spectral filter to prevent attacks of this type. Further, the optical fibre loop in the setup proposed by Lucamarini et al. [646] would help prevent attacks at low wavelengths.

Eve could also use a THA to target the intensity modulator, used by Alice to generate decoy states. If Eve can distinguish between decoy pulses and signal states, she can carry out a PNS attack without being detected, by ignoring decoy pulses and only attacking multi-photon signal states. Tamaki et al. [648] created a formalism for bounding the information leakage from the intensity modulator in terms of the operation of the modulator (i.e. the unitaries enacted by the modulator for each intensity level). They also develop the formalism for calculating the information leakage due to a THA against the phase modulator. Using these, they then calculated the key rate for BB84 with various types of THA (different assumptions about the details of the attack, and hence about the outgoing Trojan state), for fixed intensity of the outgoing Trojan horse mode.

Vinay et al. [649] expanded on the work by Lucamarini et al. in [646], and showed that coherent states (displaced vacuum states) are the optimal Trojan horse state, amongst the Gaussian states, for Eve to use in an attack on BB84, assuming attenuation of the Trojan mode and a limited outgoing photon number. Based on a calculation of the distinguishability (a measure of the information leakage of a THA), they showed that adding thermal noise to both the signal state and the Trojan horse mode can provide an effective defence against a THA, greatly increasing the key rate for a given outgoing photon number. They then upper-bounded the distinguishability for THA attacks using different photon number statistics, expanding from the case of Gaussian states to more general separable states (allowing correlations between different Fock states, but assuming no entanglement between the Trojan horse mode and some idler state held by Eve). They found that this upper bound on the distinguishability was higher than the bound found in Ref. [646] but that it could be reduced to below the Lucamarini bound by applying their thermal noise defence. They also proposed the use of a shutter between Alice's device and the main channel, in conjunction with a time delay between the encoding apparatus and the shutter, as a defence that could be used in place of an attenuator. This would work by forcing the Trojan pulse to make several journeys through Alice's encoding apparatus, making it more difficult for Eve to accurately determine the encoded phase.

3. *Backflash attacks*

A different type of side-channel attack is the detector backflash attack, introduced by Kurtsiefer et al. [650]. Detectors based on avalanche photodiodes (APDs) sometimes emit light (referred to as backflash light) upon detecting a pulse. This backflash light can give information to Eve about Bob's measurement outcome in a variety of ways. The polarization of the backflash light can give an indication of which components of Bob's system it has passed through, which could tell Eve which detector it originated from [651]. Alternatively, the travel time of the backflash photons (after entering Bob's detector) or path-dependent alterations to the profile of the outgoing light could also give Eve this information. This could tell Eve which measurement basis was chosen by Bob, and for certain detector setups could even reveal Bob's measurement outcome.

Meda et al. [652] characterized two commercially used InGaAs/InP APDs and found that backflash light could be detected for a significant proportion of avalanche events. Pinheiro et al. [651] then built on this work by characterizing a commercial Si APDs; they also found that the backflash probability was significant, with a backflash probability greater than or equal to 0.065.

Both papers found that the backflash light was broadband, and so could be reduced using a spectral filter. Pinheiro et al. [651] also characterized a photomultiplier tube, and found that it had a much lower backflash probability. They therefore suggested using photomultiplier tubes in place of APDs in Bob's detectors.

4. *Faked states and detector efficiency mismatch*

The security of BB84 (and most DV protocols) is based on Eve and Bob's basis choices being independent. If Eve is able to exploit some imperfection in Bob's device that lets her influence Bob's basis or even choose it for him, this independence would no longer hold, and the security of the protocol may be breached. Makarov et al. [653] proposed a number of schemes that could allow an eavesdropper to control or influence Bob's detector basis or measurement results. These schemes use faked states; this is where Eve does not attempt to gain information without disturbing the signal state, but instead sends a state designed to take advantage of flaws in Bob's detection device to give him the results that she wants him to receive.

Two of the proposed schemes take advantage of Bob's passive basis selection. Receiver implementations can select the measurement basis using a beamsplitter: this will randomly allow a photon through or reflect it onto another path. We call this passive basis selection, and differentiate it from active basis selection, in which Bob explicitly uses a random number generator to select the basis and changes the measurement basis accordingly [654]. If the beamsplitter used is polarization-dependent, Eve can tune the polarization of the pulses she sends such that they go to the basis of her choosing, allowing her to intercept and resend signals whilst ensuring that she and Bob always choose the same basis.

The second scheme proposes a way around the countermeasure of placing a polarizer in front of the beamsplitter. Makarov et al. [653] suggest that imperfections in the polarizer will allow Eve to still choose Bob's basis if she uses sufficiently large pulses (albeit with heavy attenuation due to the polarizer). They also suggest the use of a polarization scrambler as a defence against these two schemes. Li et al. [655] proposed a similar type of attack, in which they exploit the frequency-dependence of the beamsplitter to allow them to choose Bob's basis with high probability.

Makarov et al. [653] proposed two further schemes using faked states. One takes advantage of unaccounted for reflections in Bob's device, which could allow Eve to choose Bob's basis by precisely timing her pulses such that part of them reflects into the detectors in the correct time window for the chosen basis. This would require Eve to have a very good characterisation of Bob's device and carries the risk of detection due to side-effects caused by the part of the pulse that is not reflected. The second attack, briefly introduced in [653] and then expanded on in [656], exploits detector efficiency mismatch (DEM). This is where the detector corresponding to the outcome 0 has a different efficiency to the detector corresponding to the outcome 1 (here we are considering setups in which both bases are measured using the same pair of detectors, with a phase modulator beforehand to determine the basis used; it is also possible to have DEM in a setup in which four detectors are used) for some values of a parameter. This parameter could be time or some other parameter such as polarization, space or frequency.

If Bob's detectors have DEM, a photon with a certain value of the parameter (e.g. a certain polarization) would be more likely to be detected by the detector giving the value 0, if it were to hit it, than to be detected by the detector giving the value 1, if it were to hit that detector (or vice versa). Note, however, that in reality the photon will only hit one of the detectors, depending on what value it encodes. In the attack, Eve intercepts Alice's states and measures them in some basis. She then sends a state to Bob in the opposite basis, with the timing chosen such that Bob is likely to receive no result rather than an error, reducing Bob's error rate at the cost of increasing loss (with the likelihood of this depending on how mismatched the detector efficiencies are). We say that one of Bob's detectors has been blinded, since it is less able to pick up signals.

Lydersen et al. [204] demonstrated the possibility of using faked states to attack commercial QKD systems. They blinded the detectors using a CW laser, exploiting the fact that APDs can be made to operate in linear mode; in this mode, the detectors do not register single photons. Eve sends in pulses to trigger Bob's detectors, and they will only give a result when he chooses the same basis as Eve (with the result in this case being the same as Eve's value). Lydersen et al. [657] showed that the APDs could also be blinded by heating them using bright light. Yuan et al. [658, 659] argued that a properly operated APD would be difficult to keep in linear mode and that faked states attacks of this type could be identified by monitoring the photocurrent. Stipčević et al. [654] showed that detector blinding attacks can be treated as an attack on Bob's random number generator, and suggested that an actively selected basis with a four detector configuration (rather than using the same two detectors to measure both bases) could mitigate the effects of many types of blinding attack. See Refs. [660, 661] for other countermeasures against blinding attacks, e.g., based on intensity modulation.

Qi et al. [662] suggested a different attack based on DEM with the time parameter, which they called the time-shift attack. In this attack, Eve does not attempt to measure the signal state, but simply shifts the time at which it enters Bob's device, such that, if Bob has a detection event, it is more likely to be one value than another. For instance, if the detector corresponding to the outcome 0 has a higher efficiency at some given time than the detector corresponding to the outcome 1, Eve can know that if the time of arrival of the pulse is shifted

such that it arrives at the detector at that particular time, and the pulse is detected by one of the detectors, it is more likely that the outcome was 0 than that it was 1. The greater the DEM, the more information Eve can gain about the key. This attack does not introduce any error in the resulting key bits, and was shown to be practical using current technology by Zhao et al. [663], who carried out the attack on a modified commercial system.

In fact, there is no requirement that the DEM be parameterized by time. The detectors could be mismatched over polarization, frequency or even spatially [664]. Sajeed et al. [665] and Rau et al. [666] both showed that by altering the angle at which pulses enter Bob's device, it is possible to alter the relative sensitivity of the detectors, since the angle of entry will determine the angle at which the light hits the detectors, but small changes in the configuration of the setup could lead to different angles of incidence on each detector. The angle at which the pulse hits the detector determines the surface area of the detector that is hit by the pulse, and hence the sensitivity of the detector.

One proposed countermeasure against attacks exploiting DEM is for Bob to use a four detector configuration, with the mapping of outcomes to detectors randomly assigned each time. However, this configuration is still vulnerable to a time-shift (or other DEM) attack, if the attack is coupled with a THA on Bob's device (which learns the detector configuration after the measurement has been carried out) [667]. A THA of this type is hard for Bob to defend against, and making Bob's device more complicated by adding hardware safeguards risks opening up more vulnerabilities for Eve to exploit, and so it is desirable to find a software solution (i.e. to calculate the key rate accounting for the possibility of DEM attacks).

Fung et al. [664] found a formula for the key rate in the presence of a DEM for a very broad class of attacks, using a proof devised by Koashi [668]. Lydersen et al. [667] generalized this proof slightly. Both formulae require a thorough characterisation of the detector efficiencies over possible values of the DEM parameter. This may be difficult for the trusted parties, especially since they may not always know which parameters of the detector give rise to DEM. Fei et al. [669] calculated the key rate of BB84 with decoy states in the presence of DEM, using a new technique based on treating the detection process as a combination of the case in which there is no DEM and the case in which there is complete DEM (i.e. for some value of the parameter, there is 0% detection efficiency for one detector, but not for the other, and vice versa for some other value of the parameter). They then numerically simulated QKD in this case, and found that DEM decreases the secure key rate.

B. Hacking CV-QKD protocols

The differences between the types of protocols and devices used in DV and CV protocols mean that not all hacking attacks on DV systems are directly applicable to CV systems. Some vulnerabilities, such as attacks on the LO, are specific to CV protocols, whilst some, such as THAs, are analogous to the attacks used on DV protocols. An important practical issue in the implementation of CV-QKD is calibration of the equipment used. The shot-noise must be determined, since it affects the parameter estimation. If this is not carried out accurately, the security of CV QKD may be undermined [670]. During calibration, the phase noise introduced during modulation should be estimated. By taking it into account in the security analysis, the key rate can be increased, since the phase noise added by the modulator can then be treated as trusted noise.

1. Attacks on the local oscillator

To carry out measurements of Alice's signal states, Bob interferes them with a LO. Due to the difficulty of maintaining coherence between Alice's source and Bob's LO, implementations of CV-QKD often send the LO through the quantum channel. Since security proofs of CV-QKD do not account for this (as it is not theoretically necessary to send the LO through the channel), this leaves open some side-channels, which Eve can exploit. Häseler et al. [671] showed that the intensity of the LO must be monitored, in order to prevent Eve from replacing the signal state and LO with squeezed states, in such a way as to disguise an intercept and resend attack, by reducing the error relative to what the trusted parties would expect for such an attack. Huang et al. [672] and Ma et al. [673] proposed an attack on the LO based on the wavelength-dependency of beamsplitters. They found that by exploiting the wavelength-dependence of the beamsplitters in Bob's device, they could engineer Bob's outcomes, whilst preventing Bob from accurately determining the LO intensity. Huang et al. proposed a countermeasure in which a wavelength filter is applied at random, and any difference in channel properties between the cases in which it is applied and not applied is monitored.

Jouguet et al. [674] devised another attack on the LO. This attack uses the fact that Bob's clock is triggered by the LO pulse. By changing the shape of the LO pulse, Eve can delay the time at which the clock is triggered. This can lead to Bob incorrectly calculating the shot-noise, and hence can allow Eve to carry out an intercept and resend attack undetected. As a countermeasure, Jouguet et al. suggest that Bob should measure the shot-noise in real-time by randomly applying strong attenuation to the signal. Huang et al. [675] built on this by showing that an attack exploiting the wavelength-dependence of beamsplitters could be used to defeat Bob's attempt to measure the shot-noise in real-time. However, they found that by adding a third attenuation value (rather than just on or off) to the strong attenuation could prevent their attack. Xie et al. [676]

also found that a jitter effect in the clock signal can lead to an incorrect calculation of the shot noise, and Zhao et al. [677] identified a polarization attack where the eavesdropper attacks unmeasured LO pulses to control and tamper with the shot-noise unit of the protocol.

In order to prevent LO attacks altogether, Qi et al. [597] and Soh et al. [596] proposed and analyzed a way in which Bob could generate the local oscillator locally. Alice regularly sends phase reference pulses, and Bob applies a phase rotation to his results during post-processing, to ensure that they are in phase with Alice's source. Marie et al. [678] improved on this scheme, in order to reduce the phase noise. Ren et al. [679] proposed that even an local LO could be vulnerable to a hacking attack if the trusted parties assume that the phase noise is trusted, and cannot be used by Eve. In this case, Eve can lower the phase noise, by increasing the intensity of the phase reference pulses, and compensate for the reduced phase noise by increasing her attack on the signal states, so that the total noise on Bob's measurements remains the same.

2. *Saturation attacks on detectors*

Qin et al. [680] considered saturation attacks on Bob's homodyne detectors. Such attacks exploit the fact that CV-QKD security proofs assume a linear relationship between the incoming photon quadratures and the measurement results (that the quadrature value linearly corresponds to the measurement result), but in reality, homodyne detectors have a finite range of linearity. Above a certain quadrature value, homodyne detectors will saturate, meaning that the measurement result will be the same whether the quadrature value is at the threshold level or above it. For instance, a quadrature value of 100 shot-noises could give the same measurement result as a quadrature value of 200 shot-noises. Qin et al. considered exploiting this by using an intercept and resend attack and then rescaling and displacing the measured states (multiplying them by some factor and then adding a constant displacement to them). By causing Bob's measurement results to partially overlap with the saturation region, Eve can alter the distribution of measurement results, and so reduce the trusted parties' error estimation.

Qin et al. [680] also proposed some countermeasures, including the use of a Gaussian post-selection filter [681, 682] to try and ensure that the measurement results used for key generation fall within the linear range of the detector and the use of random attenuations of Bob's signal, to test whether the measurement results are linearly related to the inputs. Qin et al. [683] expanded on their previous work, considering a slightly different attack in which an incoherent laser is used to displace Bob's measurement results into the saturated range. They also demonstrated saturation of a homodyne detector experimentally and numerically simulated their attack to show feasibility.

3. *Trojan horse attacks*

CV protocols are also vulnerable to THAs [684]. By sending Trojan states into Alice's encoding device, Eve can try to learn how the signal states have been modulated, without disturbing the signal state itself. Derkach et al. [685] considered a leakage mode side-channel in Alice's device. They modeled this side-channel as a beamsplitter in Alice's device, coupling the signal state to a vacuum state after modulation. They also considered a side-channel allowing Eve to couple an untrusted noise to the signal state prior to detection. They then calculated the resulting key rates for both coherent state and squeezed state protocols, using RR. Derkach et al. suggest some countermeasures to the sender side-channel based on manipulation of the input vacuum state to the beamsplitter, and to the receiver side-channel based on measuring the output of the coupled noise. They then expanded on their earlier work [686], considering two types of side-channel leakage: leakage after modulation of the signal state and leakage prior to modulation, but after squeezing of the signal state (in the squeezed state protocol). They allowed multiple leakage modes from each side-channel. They calculated the key rates for both DR and RR, for side-channels of this type, and optimized the squeezing for post-modulation leakage.

Pereira et al. [687] considered a THA on Alice, in the coherent state protocol, in which Eve is able to send a Trojan state with a bounded average photon number into Alice's box. This state is then modulated in a similar way to the signal state and returned to Eve. The key rate and security threshold are calculated, for RR. Active monitoring of incoming light is suggested as a countermeasure. Ma et al. [688] considered a THA on the two-way protocol, in which Eve sends a state into Alice's device, following Bob's signal state, and then measures this state to gain information about the modulation applied by Alice. They suggest the use of active monitoring to remove the Trojan state.

Part of the noise originating from the trusted parties' devices can be assumed to be trusted and therefore not under the control of an eavesdropper. Such trusted noise could be the noise of the signal states (e.g. thermal noise in thermal-state protocols), noise added by the modulators or the noise of the detection. Trusted noise can have different impacts on CV QKD depending on the reconciliation direction. Trusted noise on the reference side of the protocol can even be helpful due to decoupling Eve's systems from the information shared by the trusted parties. On the other hand, noise on the remote side of reconciliation protocols can be harmful for the protocols, despite being trusted [471].

C. General considerations

A number of more general attacks exist, which can be used against both DV or CV protocols (although much

of the current research has been focused on DV protocols), based on altering the properties of the devices used. These type of attacks can be used to create vulnerabilities even in well-characterized devices.

Jain et al. [689] suggested and experimentally tested an attack that Eve could carry out during the calibration phase of a QKD protocol. The attack targets the system whilst Bob is calibrating his detectors (for a DV protocol) using a line length measurement (LLM). Attacks of this type are implementation dependent; in the system under consideration, Jain et al. found that by changing the phase of the calibration pulses sent by Bob during the LLM, they could induce a DEM (in the time parameter). This would open up the system to other types of attack (such as those previously mentioned), and would be especially problematic, since the trusted parties would not realise that Bob's device was miscalibrated. Building on this, Fei et al. [690] found that by sending faked calibration pulses during the LLM process, they could induce DEM or basis-dependent DEM with high probability. Fei et al. suggest adding a system to allow Bob to test his own device for calibration errors after the calibration process.

Even if an implementation is perfect, it could be possible for Eve to create vulnerabilities, by damaging components of the trusted parties' devices using a laser. Bugge et al. [691] suggested that Eve could use a laser to damage to components such as the detectors or any active monitoring devices, allowing other attacks to be enacted. They showed that APDs could be damaged by intense laser light, reducing their detection efficiency and hence permanently blinding them. This creates loopholes for Eve, without requiring her to continuously ensure that the detectors are kept blinded. Higher laser powers rendered APDs completely non-functional; this could be exploited by Eve if an APD were being used as a monitoring device (e.g. for Trojan pulses). Makarov et al. [692] demonstrated this on a commercial system and then showed that they were able to melt a hole in a spatial filter, meant to protect against spatial DEM.

Sun et al. [693] considered an attack on Alice's source. By shining a CW laser onto Alice's gain medium, Eve is able to control the phase of Alice's pulses. This could open up loopholes for other attacks in both DV and CV systems. Sun et al. suggest monitoring the light leaving Alice's source and the use of active phase randomization. In general, QKD can always be prevented by denial-of-service attacks, where Eve voluntarily introduces an amount of loss and/or noise which makes the communication insecure. Besides blinding attacks, Eve can exploit all sorts of strategies (e.g., in polarization-based DV QKD protocols, she may just apply strong Faraday rotations on the communication line [694]).

D. Device-independence as a solution?

A conceptually different approach to dealing with side-channels is the development of device-independent protocols (DI-QKD), which can prevent a lot of side-channel attacks. As discussed in Section IV, this is a type of QKD that allows for untrusted devices, which could even have been produced by Eve. Schemes for implementing DI-QKD have been designed for both the DV [221] and the CV [695] cases. Where sources can be trusted, measurement device-independent QKD (MDI-QKD) schemes can be used instead. These have also been designed for both the DV [52, 53] and the CV [240] cases. DI- and MDI-QKD protocols are harder to implement and so in general give lower key rates than device-dependent protocols. In spite of improving security, neither are immune to attack. In all protocols there is a requirement that Alice and Bob's devices be isolated from the outside world (in particular from Eve). Even in DI-QKD, if there is a hidden channel that allows Eve to gain access to measurement outcomes, then the key will not be secure. MDI-QKD is also vulnerable to source imperfections, such as the previously-mentioned attack by Sun et al. [693]. Therefore, device-independence cannot be seen as a panacea for side-channels. However, one of the main advantages of device-independent protocols is that they allow users to automatically catch malfunctioning devices.

XI. LIMITS OF POINT-TO-POINT QKD

A. Overview of the main contributions

One of the crucial problems in QKD is to achieve long distances at reasonably-high rates. However, since the proposal of the BB84 protocol [110], it was understood that this is a daunting task because even an ideal implementation of this protocol (based on perfect single-photon sources, ideal detectors and perfect EC) shows a linear decay of the secret key rate R in terms of the loss η in the channel, i.e., $R = \eta/2$. One possible way to overcome the rate problem was to introduce CV QKD protocols. Their ideal implementation can in fact beat any DV QKD protocol at any distance, even though current practical demonstrations can achieve this task only for limited distances due to practical problems related to finite reconciliation efficiency and other technical issues.

One of the breakthroughs in CV QKD was the introduction of the reverse reconciliation (RR) [462], where it is Alice to infer Bob's outcomes β, rather than Bob guessing Alice's encodings α, known as direct reconciliation (DR). This led the CV QKD community to considering a modified Devetak-Winter rate [84] in RR. This takes the form of $I(\alpha : \beta) - \chi(E : \beta)$, where the latter is Eve's Holevo information on Bob's outcomes. In a CV QKD setup, where both the energy and the entropy may hugely vary at the two ends of a lossy communication channel, there may be a non-trivial difference between the two

reconciliation methods. Most importantly, it was soon realized that RR allowed one to achieve much longer distances, well beyond the 3dB limit of the previous CV approaches. At long distances (i.e., small transmissivity η), an ideal implementation of the CV QKD protocols proposed in Refs. [466, 572] has rate $R \simeq \eta/(2\ln 2) \simeq 0.72\eta$. An open question was therefore raised:

- What is the maximum key rate (secret key capacity) achievable at the ends of a pure-loss channel?

With the aim of answering this question, a 2009 paper [44] introduced the notion of reverse coherent information (RCI) of a bosonic channel. This was quantity was previously defined in the setting of DVs [483, 696]. It was called "negative cb-entropy of a channel" in Ref. [696] and "pseudocoherent information" in Ref. [4]; Ref. [483] introduced the terminology of RCI and, most importantly, it showed its fundamental use as lower bound for entanglement distribution over a quantum channel (thus extending the hashing inequality [84] from states to channels). Ref. [44] extended the notion to CVs where it has its more natural application.

Given a bosonic channel $\mathcal{E}$, consider its asymptotic Choi matrix $\sigma_{\mathcal{E}} := \lim_{\mu} \sigma_{\mathcal{E}}^{\mu}$. This is defined over a sequence of Choi-approximating states of the form $\sigma_{\mathcal{E}}^{\mu} := \mathcal{I}_A \otimes \mathcal{E}_B(\Phi_{AB}^{\mu})$, where Φ_{AB}^{μ} is a TMSV state [7] with $\bar{n} = \mu - 1/2$ mean thermal photons in each mode. Then, we define its RCI as [44]

$$I_{\mathrm{RCI}}(\mathcal{E}) := \lim_{\mu} I(A\langle B)_{\sigma_{\mathcal{E}}^{\mu}}, \tag{163}$$

$$I(A\langle B)_{\sigma_{\mathcal{E}}^{\mu}} := S[\mathrm{Tr}_B(\sigma_{\mathcal{E}}^{\mu})] - S(\sigma_{\mathcal{E}}^{\mu}), \tag{164}$$

with $S(\sigma) := -\mathrm{Tr}(\sigma \log_2 \sigma)$ is the von Neumann entropy of σ. Here first note that, by changing Tr_B with Tr_A in Eq. (164), one defines the coherent information (CI) of a bosonic channel [44], therefore extending the definition of Refs. [697, 698] to CV systems. Also note that $I_{\mathrm{RCI}}(\mathcal{E})$ is easily computable for a bosonic Gaussian channel, because $\sigma_{\mathcal{E}}^{\mu}$ would be a two-mode Gaussian state.

Operationally, the RCI of a bosonic channel represents a lower bound for its secret key capacity and, more weakly, its entanglement distribution capacity [44]. A powerful CV QKD protocol reaching the RCI of a bosonic channel consists of the following steps:

- Alice sends to Bob the B-modes of TMSV states Φ_{AB}^{μ} with variance μ.
- Bob performs heterodyne detections of the output modes sending back a classical variable to assist Alice.
- Alice performs an optimal and conditional joint detection of all the A-modes.

The achievable rate can be computed as a difference between the Alice Holevo information $\chi(A:\beta)$ and Eve's Holevo information $\chi(E:\beta)$ on Bob's outcomes. Note that this is not a Devetak-Winter rate (in RR) but rather a generalization, where the parties' mutual information is replaced by the Holevo bound. Because Eve holds the entire purification of $\sigma_{\mathcal{E}}^{\mu}$, her reduced state ρ_E has entropy $S(\rho_E) = S(\sigma_{\mathcal{E}}^{\mu})$. Then, because Bob's detections are rank-1 measurements (projecting onto pure states), Alice and Eve's global state $\rho_{AE|\beta}$ conditioned to Bob's outcome β is pure. This means that $S(\rho_{E|\beta}) = S(\rho_{A|\beta})$. As a result, Eve's Holevo information becomes

$$\chi(E:\beta) := S(\rho_E) - S(\rho_{E|\beta}) = S(\sigma_{\mathcal{E}}^{\mu}) - S(\rho_{A|\beta}). \tag{165}$$

On the other hand, we also write

$$\chi(A:\beta) := S(\rho_A) - S(\rho_{A|\beta}), \tag{166}$$

where $\rho_A := \mathrm{Tr}_B(\sigma_{\mathcal{E}}^{\mu})$ and $\rho_{A|\beta}$ is conditioned to Bob's outcome. As a result we get the following achievable rate

$$R^{\mu}(\mathcal{E}) := \chi(A:\beta) - \chi(E:\beta) = I(A\langle B)_{\sigma_{\mathcal{E}}^{\mu}}. \tag{167}$$

By taking the limit for large μ, this provides the key rate $R(\mathcal{E}) := \lim_{\mu} R^{\mu}(\mathcal{E}) = I_{\mathrm{RCI}}(\mathcal{E})$, so that the secret key capacity of the channel can be bounded as

$$K(\mathcal{E}) \geq I_{\mathrm{RCI}}(\mathcal{E}) \ . \tag{168}$$

In particular, for a pure-loss channel $\mathcal{E}_\eta$ with transmissivity η, Pirandola, García-Patrón, Braunstein and Lloyd wrote the lower bound [44]

$$K(\mathcal{E}_\eta) \geq I_{\mathrm{RCI}}(\mathcal{E}_\eta) = -\log_2(1-\eta). \tag{169}$$

At long distances, i.e., low transmissivities $\eta \simeq 0$, this achievable key rate decays as

$$K(\mathcal{E}_\eta) \gtrsim \eta/\ln 2 \simeq 1.44\eta \ \text{ bits per channel use}, \tag{170}$$

therefore identifying an achievable rate-loss scaling which is linear in the transmissivity, i.e., of the order of η.

With the aim of providing an upper bound to the key rate of CV QKD protocols, in 2014 the TGW bound was proposed by employing the notion of squashed entanglement [699] for a bosonic channel. This is [259]

$$K(\mathcal{E}_\eta) \leq \log_2\left(\frac{1+\eta}{1-\eta}\right), \tag{171}$$

which is $\simeq 2.88\eta$ bits per use at long distances, therefore confirming the linear scaling $O(\eta)$ in Eq. (170). However, by comparing the lower bound in Eq. (169) and the upper bound in Eq. (171), we see the presence of a clear gap, which becomes an unwanted extra factor 2 in the linear scaling at long distances. Unfortunately, this extra factor 2 results into an over-pessimistic evaluation of the actual rate performance of any QKD protocol. For instance, the violation of this larger bound requires an extra 6dB of loss (or 30km in fiber) in a crucial protocol such as the ideal TF-QKD. See Sec. IV H for more details.

This non-trivial gap with the lower bound of Eq. (169) was finally closed in 2015 by Ref. [43] which derived the PLOB upper bound for the pure-loss channel

$$K(\mathcal{E}_\eta) \leq -\log_2(1-\eta). \tag{172}$$

This was done by employing the relative entropy of entanglement (REE) [700–702], suitably extended to quantum channels, combined with an adaptive-to-block reduction of quantum protocols. As a result, Ref. [43] established the secret key capacity of the pure-loss channel to be

$$K(\mathcal{E}_\eta) = -\log_2(1-\eta), \tag{173}$$

which, in turn, completely characterizes the fundamental rate-loss scaling of QKD to be $\simeq 1.44\eta$ bits per channel use at long distances.

This capacity cannot be beaten by any point-to-point QKD protocol at the two ends of the lossy channel. It can only be outperformed if Alice and Bob pre-share some secret randomness or if there is a quantum repeater splitting the quantum communication channel and assisting the remote parties. For this reason, the PLOB bound not only completely characterizes the fundamental rate-loss scaling of point-to-point QKD but also provides the exact benchmark for testing the quality of quantum repeaters.

Note that a weaker version of the PLOB may also be written by explicitly accounting for the overall detector efficiency η_{det} of a protocol. This corresponds to Alice and Bob having a composite channel of transmissivity $\eta_{\text{det}}\eta$, so that the PLOB bound weakens to $-\log_2(1-\eta_{\text{det}}\eta)$. For instance, in the recent experiment of Ref. [267] on the SNS variant of TF-QKD, the authors used 300km of optical fiber with loss rate of 0.19 dB/km (so that $\eta \simeq 1.995 \times 10^{-6}$) and their setup had an overall detection efficiency of $\eta_{\text{det}} \simeq 0.3$. This means that the relative PLOB bound in their experiment corresponds to $\simeq 8.64 \times 10^{-7}$ bits per pulse (use).

Soon after the introduction of the PLOB bound, in early 2016, Ref. [58] (later published as Ref. [59]) established the secret key capacities achievable in chains of repeaters and, more generally, quantum networks connected by pure-loss channels. In particular, in the presence of a single repeater, in the middle between the remote parties and equally splitting the overall pure-loss channel $\mathcal{E}_\eta$ of transmissivity η, one finds the following single-repeater secret key capacity

$$K_{1\text{rep}}(\mathcal{E}_\eta) = -\log_2(1-\sqrt{\eta}). \tag{174}$$

At long distances $\eta \simeq 0$, this rate provides the fundamental rate-loss scaling in the presence of a single repeater/relay. This is given by [59, Supp. Note 1, Eq. (25)]

$$K_{1\text{rep}}(\mathcal{E}_\eta) \simeq 1.44\sqrt{\eta} \text{ bits per repeater use.} \tag{175}$$

It is important to note that the right hand side of Eq. (174) is an upper bound valid for any kind of repeater (i.e., trusted or untrusted). Then, if the repeater is trusted, this bound is achievable by performing key composition via one-time pad. If the repeater is untrusted, the bound is achievable by distributing entanglement and performing entanglement swapping [58, 59].

In Fig. 11 we show the ideal key rates of point-to-point QKD protocols and those of relay-assisted end-to-end QKD protocols (i.e., exploiting an untrusted QKD repeater). These rates are compared with the PLOB bound of Eq. (173) and the single-repeater bound of Eq. (174). By ideal rates we mean the optimal ones that can be computed assuming zero dark counts, perfect detector efficiency, zero misalignment error, as well as perfect EC and reconciliation efficiency. Point-to-point protocols cannot beat the PLOB bound and asymptotically scales as $\simeq \eta$ bits per channel use. This is the case for the BB84 protocol (both with single-photon sources and decoy-state implementation) and one-way CV-QKD protocols. Even though MDI-QKD is relay assisted, its relay is not efficient, which is why DV MDI-QKD is below the PLOB bound. After TF-QKD [54] was introduced, a number of TF-inspired protocols were developed, all able to beat the PLOB bound. The middle untrusted relays of these protocols are therefore efficient (i.e., they are able to 'repeat'). Their key rates cannot overcome the single-repeater bound, but clearly follow its asymptotic rate-loss scaling of $\simeq \sqrt{\eta}$ bits per channel use.

In the following subsections, we provide the main mathematical definitions, tools, and formulas related to the study of the ultimate limits of point-to-point QKD protocols over an arbitrary quantum channel. Then, in subsequent Sec. XII we discuss the extension of these results to repeater-assisted quantum communications.

B. Adaptive protocols and two-way assisted capacities

Let us start by defining an adaptive point-to-point protocol $\mathcal{P}$ through a quantum channel $\mathcal{E}$. Assume that Alice has register $\mathbf{a}$ and Bob has register $\mathbf{b}$. These registers are (countable) sets of quantum systems which are prepared in some state $\rho^0_{\mathbf{ab}}$ by an adaptive LOCC Λ_0 applied to some fundamental separable state $\rho^0_{\mathbf{a}} \otimes \rho^0_{\mathbf{b}}$. Then, for the first transmission, Alice picks a system $a_1 \in \mathbf{a}$ and sends it through channel $\mathcal{E}$; at the output, Bob receives a system b_1 which is included in his register $b_1\mathbf{b} \to \mathbf{b}$. Another adaptive LOCC Λ_1 is applied to the registers. Then, there is the second transmission $\mathbf{a} \ni a_2 \to b_2$ through $\mathcal{E}$, followed by another LOCC Λ_2 and so on (see Fig. 12). After n uses, Alice and Bob share an output state $\rho^n_{\mathbf{ab}}$ which is epsilon-close to some target state ϕ^n with nR^ε_n bits. This means that, for any $\varepsilon > 0$, one has $\|\rho^n_{\mathbf{ab}} - \phi^n\| \leq \varepsilon$ in trace norm. This is also called an $(n, R^\varepsilon_n, \varepsilon)$-protocol. Operationally, the protocol $\mathcal{P}$ is completely characterized by the sequence of adaptive LOCCs $\mathcal{L} = \{\Lambda_0, \Lambda_1 \ldots\}$.

The (generic) two-way assisted capacity of the quantum channel is defined by taking the limit of the asymptotic weak-converse rate $\lim_{\varepsilon,n} R^\varepsilon_n$ and maximizing over

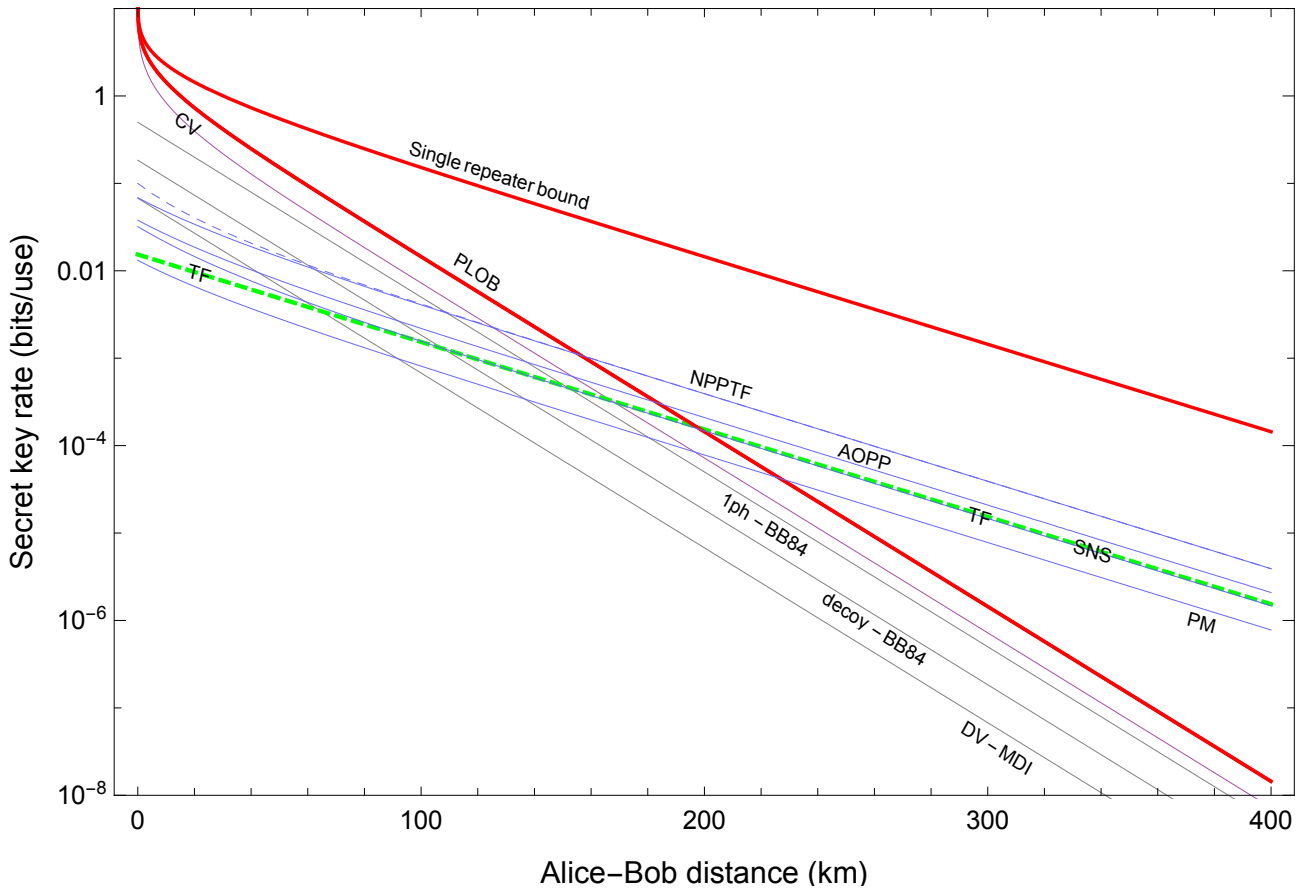

FIG. 11. State of the art in high-rate QKD. We plot the ideal key rates of several point-to-point and relay-assisted end-to-end protocols with respect to the PLOB bound [43] of Eq. (173), having the asymptotic scaling of 1.44η bits per use, and the single-repeater bound [58, 59] of Eq. (174), having the asymptotic scaling of $1.44\sqrt{\eta}$ bits per use. The key rates are expressed in terms of bits per channel use and plotted versus distance (km) at the standard fiber-loss rate of 0.2 dB per km. In particular, below the PLOB bound we consider: (**CV**) The one-way coherent-state protocol with heterodyne detection [466], which coincides with the most asymmetric protocol for CV MDI-QKD [240]. For long distances, the rate scales as 1/2 of the PLOB bound. The same asymptotic scaling is found for the coherent-state protocol with homodyne detection [572]. (**1ph-BB84**) The ideal BB84 protocol, implemented with single-photon sources [110]; according to Eq. (56) this achieves the ideal rate of $\eta/2$ shown in the figure, which can be improved to η (not shown) in the case of the efficient BB84 protocol [132]. (**decoy-BB84**) The BB84 protocol implemented with weak coherent pulses and (infinite) decoy states; according to Eq. (70) this achieves the ideal rate of $\eta/(2e)$ shown in the figure, which can be improved to η/e (not shown) in the case of the efficient decoy-state BB84 protocol. (**DV-MDI**) The ideal implementation of a passive MDI-QKD node [52, 53]. In particular, we plot the ideal rate of decoy state DV MDI-QKD [53] which is $\eta/(2e^2)$ according to Eq. (96). Then, we consider relay-assisted end-to-end protocols able to beat the PLOB bound. In particular: (**TF**) the twin-field QKD protocol [54] scaling as $\simeq 0.01535\sqrt{\eta}$ [see Eq. (102)] and shown as a dashed green line; (**PM**) the phase-matching QKD protocol [247]; (**SNS**) the sending or not sending version of TF-QKD [249] whose rate overlaps with that of the original TF-QKD protocol at long distances; (**AOPP**) the active odd-parity pair protocol [252], which is an improved formulation of the SNS protocol; (**NPPTF**) the no-phase-postselected TF-QKD protocol [253], including the variant of Ref. [257] with improved rate at shorter distances (blue dashed line).

all adaptive protocols $\mathcal{P}$, i.e.,

$$\mathcal{C}(\mathcal{E}) := \sup_{\mathcal{P}} \lim_{\varepsilon} \lim_{n} R_n^{\varepsilon}. \tag{176}$$

The specification of the target state ϕ^n identifies a corresponding type of two-way capacity. If ϕ^n is a maximally-entangled state, then we have the two-way entanglement-distribution capacity $D_2(\mathcal{E})$. The latter is in turn equal to the two-way quantum capacity $Q_2(\mathcal{E})$, because transmitting qubits is equivalent to distributing ebits under two-way CCs. If ϕ^n is a private state [703], then we have the secret key capacity $K(\mathcal{E})$ and we have $K(\mathcal{E}) \geq D_2(\mathcal{E})$, because a maximally-entangled state is a particular type of private state. Also note that $K(\mathcal{E}) = P_2(\mathcal{E})$, where P_2 is the two-way private capacity, i.e., the maximum rate at which Alice may *deterministically* transmit secret bits [704]. Thus, we may write the chain of (in)equalities

$$D_2(\mathcal{E}) = Q_2(\mathcal{E}) \leq K(\mathcal{E}) = P_2(\mathcal{E}). \tag{177}$$

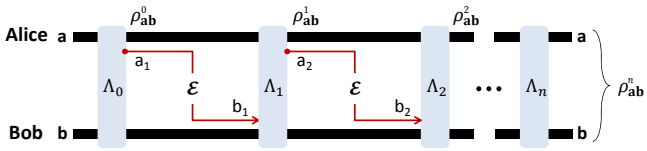

FIG. 12. Point-to-point adaptive protocol. Each transmission $a_i \to b_i$ through the quantum channel $\mathcal{E}$ is interleaved by two adaptive LOCCs, Λ_{i-1} and Λ_i, applied to Alice's and Bob's local registers **a** and **b**. After n transmissions, Alice and Bob share an output state $\rho^n_{\mathbf{ab}}$ close to some target state ϕ^n. Adapted with permission from Ref. [487] ©IOPP (2018).

C. General weak-converse upper bound

The two-way capacity $\mathcal{C}(\mathcal{E})$ [i.e., any of the capacities in Eq. (177)] can be bounded by a general expression in terms of the REE [700–702]. First of all, recall that the REE of a quantum state σ is given by

$$E_{\mathrm{R}}(\sigma) = \inf_{\gamma \in \mathrm{SEP}} S(\sigma||\gamma), \tag{178}$$

where γ is a separable state and S is the quantum relative entropy, defined by [700]

$$S(\sigma||\gamma) := \mathrm{Tr}\left[\sigma(\log_2 \sigma - \log_2 \gamma)\right]. \tag{179}$$

The notion of REE can be extended to an asymptotic state $\sigma := \lim_\mu \sigma^\mu$, which is defined as a limit of a sequence of states σ^μ (e.g., this is the case for energy unbounded states of CV systems). In this case, we may modify Eq. (178) into the following expression

$$E_{\mathrm{R}}(\sigma) := \inf_{\gamma^\mu} \liminf_{\mu \to +\infty} S(\sigma^\mu||\gamma^\mu), \tag{180}$$

where γ^μ is sequence of separable states that converges in trace-norm, i.e., such that $||\gamma^\mu - \gamma|| \overset{\mu}{\to} 0$ for some separable γ, and the inferior limit comes from the lower semi-continuity of the quantum relative entropy (valid at any dimension, including for CV systems [2]).

With these notions in hand, we may write a general upper bound. In fact, for any quantum channel $\mathcal{E}$ (at any dimension, finite or infinite), we have [43]

$$\mathcal{C}(\mathcal{E}) \leq E^{\bigstar}_{\mathrm{R}}(\mathcal{E}) := \sup_{\mathcal{P}} \lim_n \frac{E_R(\rho^n_{\mathbf{ab}})}{n}, \tag{181}$$

where $E^{\bigstar}_{\mathrm{R}}(\mathcal{E})$ is defined by computing the REE of the output state $\rho^n_{\mathbf{ab}}$, taking the limit for many channels uses, and optimizing over all the adaptive protocols $\mathcal{P}$.

To simplify the REE bound $E^{\bigstar}_{\mathrm{R}}(\mathcal{E})$ into a single-letter quantity, we adopt a technique of adaptive-to-block reduction or protocol "stretching" [43, 487, 705]. A preliminary step consists in using a suitable simulation of the quantum channel, where the channel is replaced by a corresponding resource state. Then, this simulation argument can be exploited to stretch the adaptive protocol into a much simpler block-type protocol, where the output is decomposed into a tensor product of resource states up to a trace-preserving LOCC.

D. LOCC simulation of quantum channels

Given an arbitrary quantum channel $\mathcal{E}$, we may consider a corresponding simulation $S(\mathcal{E}) = (\mathcal{T}, \sigma)$ based on some LOCC $\mathcal{T}$ and resource state σ. This simulation is such that, for any input state ρ, the output of the channel can be expressed as

$$\mathcal{E}(\rho) = \mathcal{T}(\rho \otimes \sigma). \tag{182}$$

See also Fig. 13. A channel $\mathcal{E}$ which is simulable as in Eq. (182) can also be called "σ-stretchable". Note that there are different simulations for the same channel. One is trivial because it just corresponds to choosing σ as a maximally-entangled state and $\mathcal{T}$ as teleportation followed by $\mathcal{E}$ completely pushed in Bob's local operations. Therefore, it is implicitly understood that one has to carry out an optimization over these simulations, which also depend on the specific functional under study.

More generally, the simulation can be asymptotic, i.e., we may consider sequences of LOCCs $\mathcal{T}^\mu$ and resource states σ^μ such that [43]

$$\mathcal{E}(\rho) = \lim_\mu \mathcal{E}^\mu(\rho), \quad \mathcal{E}^\mu(\rho) := \mathcal{T}^\mu(\rho \otimes \sigma^\mu). \tag{183}$$

In other words a quantum channel $\mathcal{E}$ may be defined as a point-wise limit of a sequence of approximating channels $\mathcal{E}^\mu$ that are simulable as in Eq. (183). We call $(\mathcal{T}, \sigma) := \lim_\mu (\mathcal{T}^\mu, \sigma^\mu)$ the asymptotic simulation of $\mathcal{E}$. This generalization is crucial for bosonic channels and some classes of DV channels. Furthermore, it may reproduce the simpler case of Eq. (182). Note that both Eqs. (182) and (183) play an important role in quantum resource theories (e.g., see also Eq. (54) of Ref. [706]).

Given an asymptotic simulation of a quantum channel, the associated simulation error is correctly quantified in terms of the energy-constrained diamond (ECD) norm. Consider the compact set of energy-constrained states

$$\mathcal{D}_{\bar{N}} := \{\rho_{\mathbf{ab}} \mid \mathrm{Tr}(\hat{N}\rho_{AB}) \leq \bar{N}\}, \tag{184}$$

where $\bar{N}$ is the total multi-mode number operator. For two bosonic channels, $\mathcal{E}$ and $\mathcal{E}'$, and $\bar{N}$ mean number of photons, we define the ECD distance as

$$\|\mathcal{E} - \mathcal{E}'\|_{\diamond \bar{N}} := \sup_{\rho_{AB} \in \mathcal{D}_{\bar{N}}} \|\mathcal{I}_A \otimes \mathcal{E}(\rho_{AB}) - \mathcal{I}_A \otimes \mathcal{E}'(\rho_{AB})\|_1. \tag{185}$$

This quantity was introduced by Ref. [43, Eq. (98)] for the field of quantum/private communications and by Ref. [707] for the field of quantum metrology. (See also Refs. [708, 709] for a slightly different definition, where the constraint is only enforced on the B part.) The condition in Eq. (183) means that, for any finite $\bar{N}$, we may write the following bounded-uniform convergence

$$\|\mathcal{E} - \mathcal{E}^\mu\|_{\diamond \bar{N}} \overset{\mu}{\to} 0. \tag{186}$$

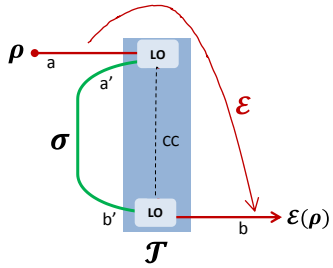

FIG. 13. LOCC simulation of an arbitrary quantum channel $\mathcal{E}$ by means of an LOCC $\mathcal{T}$ applied to the input state ρ and a resource state σ, according to Eq. (182). For asymptotic simulation, we have the approximate channel $\mathcal{E}^{\mu}$ which is simulated by $(\mathcal{T}^{\mu}, \sigma^{\mu})$. We then take the point-wise limit for infinite μ, which defines the asymptotic channel $\mathcal{E}$ as in Eq. (183).

Since the first teleportation-based simulation of Pauli channels introduced in Ref. [710, Section V], the tool of channel simulation has been progressively developed over the years thanks to the contributions of several authors [711–716] and it is still today a topic of improvements and generalizations (e.g., see Table I in Ref. [487]). Here we have presented the most general formulation for the LOCC simulation of a quantum channel at any dimension (finite or infinite) as it has been formalized in Ref. [43]. This formulation enables one to deterministically simulate the amplitude damping channel.

As a matter of fact, today we only know asymptotic simulations for the amplitude damping channel which either involves a limit in the dimension of the Hilbert space or a limit in the number of systems forming the resource state (e.g., implementing port-based teleportation [717–720] over an infinite number of Choi matrices [721]). It is an open problem to find a deterministic and non-asymptotic simulation for this channel, which would provide a better estimate of its secret key capacity, today still unknown. Also note that the tool of conditional channel simulation [722] seems to fail to simulate the amplitude damping channel, while it can easily simulate a diagonal amplitude damping ("DAD") channel or a "dephrasure" channel [723].

Finally, note that the LOCC simulation is also useful to simplify adaptive protocols of quantum metrology and quantum channel discrimination [707]. See Ref. [724] for a review on adaptive quantum metrology and Ref. [725] for a recent review on quantum channel discrimination with applications to quantum illumination [726, 727], quantum reading [728] and optical resolution [729–731].

E. Teleportation covariance and simulability

For some channels, the LOCC simulation takes a very convenient form. This is the case for the "teleportation covariant" channels, that are those channels commuting with the random unitaries of quantum teleportation [24–27], i.e., Pauli operators in DVs [1], phase-space displacements in CVs [7, 8]. More precisely, a quantum channel $\mathcal{E}$ is called teleportation covariant if, for any teleportation unitary U, we may write

$$\mathcal{E}(U\rho U^{\dagger}) = V\mathcal{E}(\rho)V^{\dagger} \ , \tag{187}$$

for another (generally-different) unitary V. This property was discussed in Ref. [715, 716] for DV systems and then in Ref. [43] for systems of any dimension.

Note that this is a wide family, which includes Pauli channels (e.g., depolarizing or dephasing), erasure channels and bosonic Gaussian channels. Thanks to the property in Eq. (187), the random corrections of the teleportation protocol can be pushed at the output of these channels. For this reason, they may be simulated by teleportation. In fact, a teleportation-covariant channel $\mathcal{E}$ can be simulated as

$$\mathcal{E}(\rho) = \mathcal{T}_{\text{tele}}(\rho \otimes \sigma_{\mathcal{E}}), \tag{188}$$

where $\mathcal{T}_{\text{tele}}$ is a teleportation LOCC (based on Bell detection and conditional unitaries) and $\sigma_{\mathcal{E}}$ is the Choi matrix of the channel, defined as $\sigma_{\mathcal{E}} := \mathcal{I} \otimes \mathcal{E}(\Phi)$, with Φ being a maximally entangled state.

For a teleportation-covariant single-mode bosonic channel (e.g., Gaussian), we may write the asymptotic simulation [43]

$$\mathcal{E}(\rho) = \lim_{\mu} \mathcal{T}^{\mu}_{\text{tele}}(\rho \otimes \sigma^{\mu}_{\mathcal{E}}), \tag{189}$$

where $\mathcal{T}^{\mu}_{\text{tele}}$ is a sequence of teleportation-LOCCs (based on finite-energy versions of the ideal CV Bell detection) and $\sigma^{\mu}_{\mathcal{E}} := \mathcal{I} \otimes \mathcal{E}(\Phi^{\mu})$ is a sequence of Choi-approximating states (recall that Φ^{μ} is a TMSV state with $\bar{n} = (\mu - 1)/2$ mean thermal photons in each mode).

When a quantum channel can be simulated as in Eq. (188) or (189) it may be called "Choi-stretchable" or "teleportation simulable". Let us also mention that, recently, non-asymptotic types of teleportation simulations have been considered for bosonic Gaussian channels [705, 732–735]. These simulations remove the limit in the resource state (while the infinite-energy limit is still assumed in the CV Bell detection). However, it has also been found that these simulations cannot provide tight results for quantum and private capacities as the asymptotic one in Eq. (189), unless the energy of the resource state is again sent to infinity [736].

F. Strong and uniform convergence in teleportation simulation

Let us further discuss the topology of the simulation of Eq. (189) for bosonic channels. In 1994, Lev Vaidman proposed an ideal protocol for CV teleportation [737] based on ideal EPR correlations. Later in 1998, Braunstein and Kimble (BK) [25] devised a realistic protocol of CV teleportation based on finite-energy TMSV states (see Ref. [27] for a review). Since its introduction, it

was understood that the BK protocol strongly converges to the identity channel in the limit of infinite squeezing (both in the resource state and in the Bell detection). In other words, for any input state ρ, we may write the point-wise limit

$$\lim_{\mu} \mathcal{T}^{\mu}_{\text{tele}}(\rho \otimes \Phi^{\mu}) = \mathcal{I}(\rho). \tag{190}$$

Because of this, the channel simulation of any teleportation-covariant bosonic channel *strongly* converges to the channel. This condition can equivalently be expressed in terms of the ECD norm, so that for any finite $\bar{N}$ we may write

$$\|\mathcal{E} - \mathcal{T}^{\mu}_{\text{tele}}(\rho \otimes \sigma^{\mu}_{\mathcal{E}})\|_{\diamond \bar{N}} \stackrel{\mu}{\to} 0. \tag{191}$$

It is also well-known that the BK protocol does not converge *uniformly* to the identity channel. In other words, if we consider the standard diamond norm which is defined over the entire set $\mathcal{D}$ of bipartite states, then we have (see Sec. 4.4 of Ref. [487])

$$\|\mathcal{I} - \mathcal{T}^{\mu}_{\text{tele}}(\rho \otimes \Phi^{\mu})\|_{\diamond} \stackrel{\mu}{\to} 2. \tag{192}$$

For this reason, the uniform convergence in the teleportation simulation of bosonic channels is not guaranteed. However, it holds for some specific bosonic Gaussian channels. Recall that a single-mode Gaussian channel transforms the characteristic function as follows [738]

$$\mathcal{G} : \chi(\boldsymbol{\xi}) \to \chi(\mathbf{T}\boldsymbol{\xi}) \exp\left(-\tfrac{1}{2}\boldsymbol{\xi}^T \mathbf{N}\boldsymbol{\xi} + i\mathbf{d}^T\boldsymbol{\xi}\right) \ , \tag{193}$$

where $\mathbf{d} \in \mathbb{R}^2$ is a displacement, while the transmission matrix $\mathbf{T}$ and the noise matrix $\mathbf{N}$ are 2×2 real, with $\mathbf{N}^T = \mathbf{N} \geq 0$ and $\det \mathbf{N} \geq (\det \mathbf{T} - 1)^2$. In terms of mean value $\bar{\mathbf{x}}$ and covariance matrix $\mathbf{V}$, Eq. (193) corresponds to [7, 738–740]

$$\bar{\mathbf{x}} \to \mathbf{T}\bar{\mathbf{x}} + \mathbf{d}, \quad \mathbf{V} \to \mathbf{T}\mathbf{V}\mathbf{T}^T + \mathbf{N}. \tag{194}$$

It is easy to check that the asymptotic simulation of a single-mode Gaussian channel uniformly converges to the channel if and only if $\mathbf{N}$ has full rank.

G. Stretching of an adaptive protocol

By exploiting the LOCC simulation $S(\mathcal{E}) = (\mathcal{T}, \sigma)$ of a quantum channel $\mathcal{E}$, we may completely simplify an adaptive protocol. In fact, the output state $\rho^n_{\mathbf{ab}}$ can be decomposed into a tensor-product of resources states $\sigma^{\otimes n}$ up to a trace-preserving LOCC $\bar{\Lambda}$. In other words, we may write [43, Lemma 3]

$$\rho^n_{\mathbf{ab}} = \bar{\Lambda}\left(\sigma^{\otimes n}\right). \tag{195}$$

For non-asymptotic simulations the proof goes as follows. As shown in Fig. 14, for the generic ith transmission, we replace the original quantum channel $\mathcal{E}$ with a simulation $S(\mathcal{E}) = (\mathcal{T}, \sigma)$. Then, we collapse the LOCC $\mathcal{T}$ into the adaptive LOCC Λ_i to form the composite LOCC Δ_i. As a result, the pre-transmission state $\rho^{i-1}_{\mathbf{ab}} := \rho_{\mathbf{a}a_i\mathbf{b}}$ is transformed into the following post-transmission state

$$\rho^i_{\mathbf{ab}} = \Delta_i\left(\rho^{i-1}_{\mathbf{ab}} \otimes \sigma\right). \tag{196}$$

The next step is to iterate Eq. (196). One finds

$$\rho^n_{\mathbf{ab}} = (\Delta_n \circ \cdots \circ \Delta_1)(\rho^0_{\mathbf{ab}} \otimes \sigma^{\otimes n}). \tag{197}$$

Because $\rho^0_{\mathbf{ab}}$ is separable, its preparation may be included in the LOCCs and we get Eq. (195) for a complicated but single trace-preserving LOCC $\bar{\Lambda}$.

For a bosonic channel with asymptotic simulation as in Eq. (183), the procedure is more involved. One first considers an imperfect channel simulation $\mathcal{E}^{\mu}(\rho) := \mathcal{T}^{\mu}(\rho \otimes \sigma^{\mu})$ in each transmission. By adopting this simulation, we realize an imperfect stretching of the protocol, with output state $\rho^{\mu,n}_{\mathbf{ab}} := \bar{\Lambda}_{\mu}\left(\sigma^{\mu \otimes n}\right)$ for a trace-preserving LOCC $\bar{\Lambda}_{\mu}$. This is done similarly to the steps in Fig. 14, but considering $\mathcal{E}^{\mu}$ in the place of the original channel $\mathcal{E}$. A crucial point is now the estimation of the error in the channel simulation, which must be controlled and propagated to the output state. Assume that, during the n transmissions of the protocol, the total mean number of photons in the registers is bounded by some large but finite value $\bar{N}$. By using a "peeling argument" over the trace distance, which exploits the triangle inequality and the monotonicity under completely-positive maps, we may write the output simulation error in terms of the channel simulation error, i.e., [43, 487, 707]

$$\|\rho^n_{\mathbf{ab}} - \rho^{n,\mu}_{\mathbf{ab}}\| \leq n \, \|\mathcal{E} - \mathcal{E}^{\mu}\|_{\diamond \bar{N}} \ . \tag{198}$$

Therefore, we may write the trace-norm limit

$$\left\|\rho^n_{\mathbf{ab}} - \bar{\Lambda}_{\mu}\left(\sigma^{\mu \otimes n}\right)\right\| \stackrel{\mu}{\to} 0, \tag{199}$$

i.e., the asymptotic stretching $\rho^n_{\mathbf{ab}} = \lim_{\mu} \bar{\Lambda}_{\mu}(\sigma^{\mu \otimes n})$. This is true for any finite energy bound $\bar{N}$, an assumption that can be removed at the very end of the calculations.

Let us note that protocol stretching simplifies an *arbitrary* adaptive protocol over an *arbitrary* channel at *any* dimension, finite or infinite. In particular, it works by maintaining the original communication task. This means that an adaptive protocol of quantum communication (QC), entanglement distribution (ED) or key generation (KG), is reduced to a corresponding block protocol with exactly the same original task (QC, ED, or KG), but with the output state being decomposed in the form of Eq. (195) or Eq. (199). In the literature, there were precursory arguments, as those in Refs. [710, 712–716], which were about the transformation of a protocol of QC into a protocol of ED, over restricted classes of quantum channels. Most importantly, no control of the simulation error was considered in previous literature.

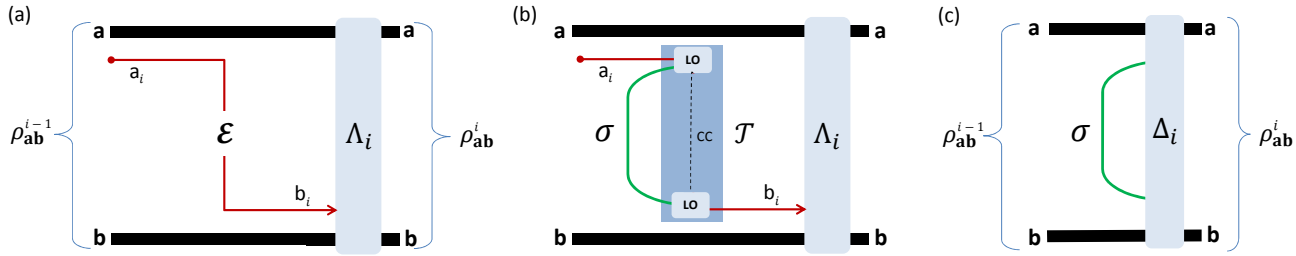

FIG. 14. Stretching of the ith transmission of an adaptive protocol. (a) We depict the original transmission through the channel $\mathcal{E}$ which transforms the register state $\rho^{i-1}_{\mathbf{ab}} := \rho_{\mathbf{a}a_i\mathbf{b}}$ into the output $\rho^{i}_{\mathbf{ab}}$. (b) We simulate the channel by means of an LOCC $\mathcal{T}$ and a resource state σ, as in previous Fig. 13. (c) We collapse $\mathcal{T}$ and the adaptive LOCC Λ_i into a single LOCC Δ_i applied to the tensor product $\rho^{i-1}_{\mathbf{ab}} \otimes \sigma$, as in Eq. (196). Adapted with permission from Ref. [43] ©NPG (2017).

H. Single-letter upper bound for two-way assisted capacities

A crucial insight from Ref. [43] has been the combination of protocol stretching with the REE, so that its properties of monotonicity and sub-additivity can be powerfully exploited. This is the key observation that leads to a single-letter upper bound for all the two-way capacities of a quantum channel. In fact, let us compute the REE of the output state decomposed as in Eq. (195). We derive

$$E_{\mathrm{R}}(\rho^{n}_{\mathbf{ab}}) \overset{(1)}{\leq} E_{\mathrm{R}}(\sigma^{\otimes n}) \overset{(2)}{\leq} nE_{\mathrm{R}}(\sigma) \ , \tag{200}$$

using (1) the monotonicity of the REE under trace-preserving LOCCs and (2) its subadditive over tensor products. By replacing Eq. (200) in Eq. (181), we then find the single-letter upper bound

$$\mathcal{C}(\mathcal{E}) \leq E_{\mathrm{R}}(\sigma) \ . \tag{201}$$

In particular, if the channel $\mathcal{E}$ is teleportation-covariant, it is Choi-stretchable, and we may write

$$\mathcal{C}(\mathcal{E}) \leq E_{\mathrm{R}}(\sigma_{\mathcal{E}}) = E_{\mathrm{R}}(\mathcal{E}) := \sup_{\rho} E_{\mathrm{R}}\left[\mathcal{I} \otimes \mathcal{E}(\rho)\right] , \tag{202}$$

where $E_{\mathrm{R}}(\mathcal{E})$ is the REE of the channel $\mathcal{E}$ [43, Theorem 5].

These results are suitable extended to asymptotic simulations. Using the weaker definition of REE in Eq. (180), the bounds in Eqs. (201) and (202) are also valid for bosonic channels with asymptotic simulations. For a bosonic Gaussian channel $\mathcal{E}$, the upper bound in Eq. (202) is expressed in terms of its asymptotic Choi matrix $\sigma_{\mathcal{E}} := \lim_{\mu} \sigma^{\mu}_{\mathcal{E}}$. By inserting Eq. (180) in Eq. (202), we derive

$$\mathcal{C}(\mathcal{E}) \leq \liminf_{\mu \to +\infty} S(\sigma^{\mu}_{\mathcal{E}} || \tilde{\gamma}^{\mu}) \ , \tag{203}$$

for a suitable converging sequence of separable states $\tilde{\gamma}^{\mu}$. Here $\sigma^{\mu}_{\mathcal{E}} := \mathcal{I} \otimes \mathcal{E}(\Phi^{\mu})$ is Gaussian and also $\tilde{\gamma}^{\mu}$ can be chosen to be Gaussian, so that we are left with a simple computation of relative entropy between Gaussian states.

Related investigations were carried out in Refs. [741, 742]. Ref. [741] found that the weak converse upper bound $E_{\mathrm{R}}(\mathcal{E})$ in Eq. (202) is also a strong converse rate (for Choi-stretchable channels). It also provided several higher-order bounds that describe the inherent trade-off between the transmission rate and the error for finite block lengths n. For bosonic Gaussian channels, these bounds have higher order terms that are positive contributions to the asymptotic key rate: further investigations are therefore needed in order to find tighter bounds (with negative higher-order contributions) so that the finite-size key rate is indeed lower than its asymptotic value (e.g., see preliminary results in Ref. [734] and Appendix B of Ref. [736]). Ref. [742] found that, by replacing the REE in Eq. (202) with the max-relative entropy of entanglement, this becomes a strong converse bound that can be written for any quantum channel (but the resulting bound is generally larger for Choi-stretchable channels).

I. Bounds for teleportation-covariant channels

Because the upper bounds in Eqs. (202) and (203) are valid for any teleportation-covariant channel, they may be applied to Pauli channels and bosonic Gaussian channels. Consider a qubit Pauli channel

$$\mathcal{E}_{\mathrm{Pauli}}(\rho) = p_0\rho + p_1 X\rho X + p_2 Y\rho Y + p_3 Z\rho Z, \tag{204}$$

where $\{p_k\}$ is a probability distribution and X, Y, and Z are Pauli operators [1]. Let us call H_2 the binary Shannon entropy and $p_{\max} := \max\{p_k\}$. Then, we may write [43, Eq. (33)]

$$\mathcal{C}(\mathcal{E}_{\mathrm{Pauli}}) \leq \begin{cases} 1 - H_2(p_{\max}), & \text{if } \ p_{\max} \geq 1/2, \\ 0, & \text{if } \ p_{\max} < 1/2, \end{cases} \tag{205}$$

which can be easily generalized to arbitrary finite dimension (qudits).

Consider now phase-insensitive Gaussian channels. The most important is the thermal-loss channel $\mathcal{E}_{\eta,\bar{n}}$ which transforms input quadratures $\hat{\mathbf{x}} = (\hat{q}, \hat{p})^T$ as $\hat{\mathbf{x}} \to \sqrt{\eta}\hat{\mathbf{x}} + \sqrt{1-\eta}\hat{\mathbf{x}}_E$, where $\eta \in (0,1)$ is the transmissivity and E is the thermal environment with $\bar{n}$ mean photons.

For this channel, we may derive [43, Eq. (23)]

$$\mathcal{C}(\mathcal{E}_{\eta,\bar{n}}) \leq \begin{cases} -\log_2\left[(1-\eta)\eta^{\bar{n}}\right] - h(\bar{n}), & \text{if } \bar{n} < \frac{\eta}{1-\eta}, \\ 0, & \text{if } \bar{n} \geq \frac{\eta}{1-\eta}, \end{cases} \tag{206}$$

where we have set

$$h(x) := (x+1)\log_2(x+1) - x\log_2 x. \tag{207}$$

The thermal-loss channel is particularly important for QKD. From the variance parameter $\omega = 2\bar{n}+1$, we define the so-called "excess noise" ε of the channel $\omega = (1-\eta)^{-1}\eta\varepsilon + 1$,which leads to

$$\varepsilon = 2\eta^{-1}(1-\eta)\bar{n}. \tag{208}$$

This formula of the excess noise (in the currently chosen SNU equal to 1) comes from considering a one-way CV-QKD Gaussian protocol, and writing Alice and Bob's mutual information in SNR form. In the limit of high Gaussian modulation, the equivalent noise χ at the denominator can be broken down into a contribution from the losses χ_{loss} and an extra contribution coming from the thermal noise, i.e., the excess noise.

Then, for a generic QKD protocol, we may write its rate as $R = R(\eta, \varepsilon)$. The security threshold of the protocol is therefore obtained for $R = 0$ and expressed as $\varepsilon = \varepsilon(\eta)$, providing the maximum tolerable excess noise as a function of the transmissivity. An open question is to find the optimal security threshold in CV-QKD. From Eq. (206), it is easy to see that this must be lower than the entanglement-breaking value $\varepsilon_{\text{UB}} = 2$ SNU. In terms of lower bounds, we may consider the RCI which is however beaten by QKD protocols with trusted noise or two-way quantum communication. The highest security thresholds known in CV-QKD are plotted in Fig. 15, where we may also note the big gap between the best-known achievable thresholds and the upper bound (this figure was first presented in Ref. [487] but assuming the different convention of vacuum SNU equal to 1/2).

For a noisy quantum amplifier $\mathcal{E}_{g,\bar{n}}$ we have the transformation $\hat{\mathbf{x}} \to \sqrt{g}\hat{\mathbf{x}} + \sqrt{g-1}\hat{\mathbf{x}}_E$, where $g > 1$ is the gain and E is the thermal environment with $\bar{n}$ mean photons. In this case, we may compute [43, Eq. (26)]

$$\mathcal{C}(\mathcal{E}_{\eta,\bar{n}}) \leq \begin{cases} \log_2\left(\dfrac{g^{\bar{n}+1}}{g-1}\right) - h(\bar{n}), & \text{if } \bar{n} < (g-1)^{-1}, \\ 0, & \text{if } \bar{n} \geq (g-1)^{-1}. \end{cases} \tag{209}$$

Finally, for an additive-noise Gaussian channel $\mathcal{E}_\xi$, we have $\hat{\mathbf{x}} \to \hat{\mathbf{x}} + (z,z)^T$ where z is a classical Gaussian variable with zero mean and variance $\xi \geq 0$. In this case, we have the bound [43, Eq. (29)]

$$\mathcal{C}(\mathcal{E}_\xi) \leq \begin{cases} \frac{\xi-2}{2\ln 2} - \log_2(\xi/2), & \text{if } \xi < 2, \\ 0, & \text{if } \xi \geq 2. \end{cases} \tag{210}$$

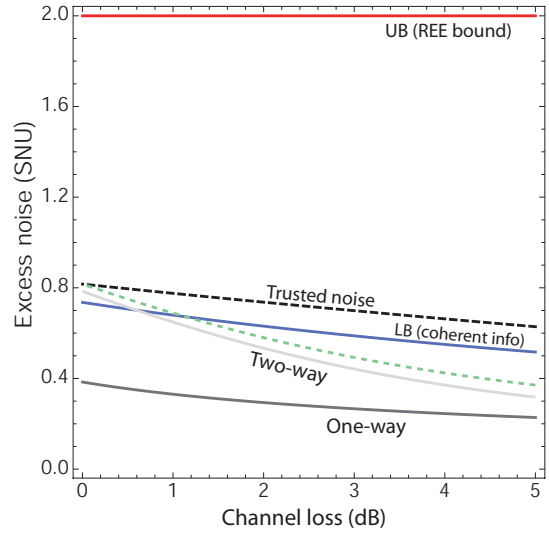

FIG. 15. Best-known security thresholds in CV-QKD expressed as maximum tolerable excess noise ε in terms of SNU (i.e., units of vacuum noise) versus channel loss (dB). Each protocol is secure only below its threshold. The red line corresponds to the upper bound $\varepsilon_{\text{UB}} = 2$ SNU. The blue line is the lower bound ε_{LB} computed from the RCI of the thermal-loss channel [44]. The black dashed line is the best-known security threshold, which is achieved by the one-way trusted noise protocol described in Ref. [487, Sec. VII]. Then, we show the thresholds for the one-way coherent-state protocol with heterodyne detection [466] and the two-way protocols with coherent states [493] (solid line) and largely-thermal states [512] (green dashed line). Reproduced and adapted with permission from Ref. [487] ©IOPP (2018).

Note that this formula slightly differs from Eq. (29) of Ref. [43] due to the different convention for the vacuum SNU that we consider here.

J. Capacities for distillable channels

Within the class of teleportation-covariant channels, there is a sub-class for which the upper bound $E_{\text{R}}(\sigma_{\mathcal{E}})$ in Eq. (202) coincides with an achievable rate for one-way entanglement distillation. These "distillable channels" are those for which we may write

$$E_{\text{R}}(\sigma_{\mathcal{E}}) = D_1(\sigma_{\mathcal{E}}), \tag{211}$$

where $D_1(\sigma_{\mathcal{E}})$ is the distillable entanglement of the Choi matrix $\sigma_{\mathcal{E}}$ via one-way (forward or backward) CC. This quantity is also suitably extended to asymptotic Choi matrices in the case of bosonic channels.

The equality in Eq. (211) is a remarkable coincidence for three reasons:

1. Since $D_1(\sigma_{\mathcal{E}})$ is a lower bound to $D_2(\mathcal{E})$, all the two-way capacities of these channels coincide ($D_2 =$

$Q_2 = K = P_2$) and are fully established as

$$\mathcal{C}(\mathcal{E}) = E_{\rm R}(\sigma_{\mathcal{E}}) = D_1(\sigma_{\mathcal{E}}). \tag{212}$$

2. The two-way capacities are achieved by means of rounds of one-way CC, so that adaptiveness is not needed and the amount of CC is limited.

3. Because of the hashing inequality, we have

$$D_1(\sigma_{\mathcal{E}}) \geq \max\{I_{\rm C}(\sigma_{\mathcal{E}}), I_{\rm RC}(\sigma_{\mathcal{E}})\}, \tag{213}$$

where $I_{\rm C}$ and $I_{\rm RC}$ are the coherent [697, 698] and reverse coherent [44, 483] information of the Choi matrix. Such quantities (and their asymptotic versions) are easily computable and may be used to show the coincidence in Eq. (212).

In this way we can write simple formulas for the two-way capacities of fundamental quantum channels, such as the pure-loss channel, the quantum-limited amplifier, the dephasing and erasure channels (all distillable channels).

In particular, for a bosonic pure-loss channel $\mathcal{E}_\eta$ with transmissivity η, one has the PLOB bound [43, Eq. (19)]

$$\mathcal{C}(\eta) = -\log_2(1-\eta)\ . \tag{214}$$

The secret-key capacity $K(\eta)$ determines the maximum rate achievable by any QKD protocol in the presence of a lossy communication line (see also Fig. 11). Note that the PLOB bound can be extended to a multiband lossy channel, for which we write $\mathcal{C} = -\sum_i \log_2(1-\eta_i)$, where η_i are the transmissivities of the various bands or frequency components. For instance, for a multimode telecom fibre with constant transmissivity η and bandwidth W, we have

$$\mathcal{C} = -W\log_2(1-\eta). \tag{215}$$

Now consider the other distillable channels. For a quantum-limited amplifier $\mathcal{E}_g$ with gain $g > 1$ (and zero thermal noise $\bar{n} = 0$), one finds [43, Eq. (28)]

$$\mathcal{C}(g) = -\log_2\left(1-g^{-1}\right)\ . \tag{216}$$

In particular, this proves that $Q_2(g)$ coincides with the unassisted quantum capacity $Q(g)$ [743, 744]. For a qubit dephasing channel $\mathcal{E}_p^{\rm deph}$ with dephasing probability p, one finds [43, Eq. (39)]

$$\mathcal{C}(p) = 1 - H_2(p)\ , \tag{217}$$

where H_2 is the binary Shannon entropy. Note that this also proves $Q_2(\mathcal{E}_p^{\rm deph}) = Q(\mathcal{E}_p^{\rm deph})$, where the latter was derived in ref. [745]. Eq. (217) can be extended to arbitrary dimension d, so that [43, Eq. (41)]

$$\mathcal{C}(p,d) = \log_2 d - H(\{P_i\})\ , \tag{218}$$

where H is the Shannon entropy and P_i is the probability of i phase flips. Finally, for the qudit erasure channel $\mathcal{E}_{p,d}^{\rm erase}$ with erasure probability p, one finds [43, Eq. (44)]

$$\mathcal{C}(p) = (1-p)\log_2 d\ . \tag{219}$$

For this channel, only Q_2 was previously known [746], while [43, 747] co-established K.

K. Open problems

There are a number of open questions that are currently subject of theoretical investigation. While the secret key capacity has been established for a number of important channels, there are others for which the gap between best-known lower bound and best-known upper bound is still open. This is the case for the thermal-loss channel, the noisy quantum amplifier, the additive-noise Gaussian channel, the depolarizing channel, and the amplitude damping channel. For most of these channels, an improvement may come from refined calculations (e.g., including non-Gaussian states in the optimization of the REE, or by employing the regularized REE). As we already mentioned before, for the amplitude damping channel the problem is also its LOCC simulation, which is not good enough to provide a tight upper bound. Recently this simulation has been improved in the setting of DVs by resorting to the convex optimization of programmable quantum processors [748, 749], e.g., based on the port-based teleportation protocol [717, 721].

For the thermal-loss channel, we also know that the lower bound to the secret key capacity given by the RCI is not tight. There are in fact QKD protocols with trusted-noise in the detectors whose rates may beat the RCI, as shown in Refs. [44, 485]. Similarly, for the noisy amplifier, we know [486] trusted-noise protocols that are able to beat the CI of the channel, which is therefore not tight. The non-tightness of the CI (and RCI) is also a feature in the computation of energy-constrained quantum capacities of bosonic Gaussian channels [750]. An interesting approach to bound the quantum capacities of these channels has been recently pursued in Refs. [751–753] by using the Gottesman-Preskill-Kitaev (GKP) states [754], realizable with various technologies [755–759].

XII. REPEATER CHAINS AND QUANTUM NETWORKS

A. What is a quantum repeater?

In an information-theoretic sense, a quantum repeater or quantum relay is *any type* of middle node between Alice and Bob which helps their quantum communication by breaking down their original quantum channel in two different quantum channels. It does not matter what technology the node is employing, e.g., it may or may not have quantum memories. Quantum repeaters can then be classified on the basis of specific features.

A general classification, which is relevant in QKD, relies on their type of security. As already mentioned in the introduction, the simplest type of repeater is a trusted party, which uses one-time pad to swap keys. This is what we call a trusted QKD repeater (or relay or node). Schemes based on this concept are trusted-relay protocols or trusted-node networks [47–51]. The next type/level is a repeater which may be operated by an untrusted party.

Type of repeater:	Trusted QKD repeater (key composition)	Untrusted QKD repeater (measurement-based)	Untrusted ED/QEC repeater (entanglement-based [55–57])
Relay-assisted protocol:	Trusted-relay QKD protocol	End-to-end QKD protocol	
Examples:	Trusted-node networks [47–51]	MDI-QKD [52, 53, 240] TF-QKD [54]	DI-QKD [114]

TABLE VI. Classification of repeaters in QKD.

Its simplest working mechanism is based on the implementation of some suitable measurement, which is then certified by the remote parties [52–54, 240]. A protocol performed with an untrusted QKD repeater is end-to-end, meaning that security only relies on the two end-users. A stronger but more challenging way to achieve end-to-end security is to consider untrusted repeaters

To be precise, a quantum repeater actually *repeats* only when it is able to beat the performance of any point-to-point protocol, i.e., the PLOB bound [43]. We may call these "active" or "effective" repeaters. Example of effective repeaters are those exploiting phase-randomization and single-photon detection, such as TF-QKD [54, 246] and the related protocols of PM-QKD [247], SNS-QKD [249–252], and NPPTF-QKD [253–258]. Examples of non-effective repeaters are MDI-nodes based on standard Bell detections [52, 53, 240]. In this other classification, the PLOB bound provides the exact benchmark, being exactly the secret key capacity of the lossy communication channel (pure-loss channel), besides its (two-way) entanglement distribution and quantum capacity. According to our definitions above, the proof-of-concept TF-QKD experiment in Ref. [265] represents the first effective untrusted QKD repeater ever implemented. The ideal performances of TF-QKD and other relay-assisted end-to-end protocols are summarized in Fig. 11.

While the violation of the PLOB bound provides an exact criterion for benchmarking quantum repeaters, one also needs to quantify the optimal performance they may achieve. Within the setting of QKD, we would like to determine the maximum secret key rates that can be generated in a chain of quantum repeaters or, more generally, in a multi-hop quantum network. Upper bounds on these key rates have been recently investigated by considering the most general adaptive protocols. Here we report the tightest upper bounds of Refs. [58, 59], which also allow us to exactly establish the secret key capacities of repeater chains and quantum networks when they are connected by fundamental types of quantum channels (subsection XII B). When a chain or network is connected by distillable channels (e.g., pure-loss channels), these upper bounds are in fact achievable: If the repeaters/nodes are trusted, the bounds can be achieved via key composition, while if the repeaters/nodes are untrusted but equipped with quantum memories (ED repeaters) then the upper bounds can be reached via entanglement distillation protocols and entanglement swapping.

In the second part of the section (subsection XII C), that are based on entanglement distribution/distillation (ED) [55–57]. These untrusted ED repeaters typically exploit quantum memories and can be used for various tasks, from DI-QKD to long-distance transmission of quantum information. Equivalently, these tasks can be achieved by untrusted repeaters based on quantum error correction (QEC). See Table VI for a summary.
we will discuss quantum repeaters which are generally designed for the reliable transmission of quantum information. Since this process is strictly connected with the distribution of entanglement, it implies the distribution of secret correlations. The typical working mechanism relies on entanglement distillation, i.e., these correspond to the untrusted ED repeaters discussed above. The ebits distributed in this way can then be transformed into secret key bits by the parties. Another working mechanism relies on QEC for which the use of quantum memories is not necessary (but still entanglement is needed for the construction of the codewords). In this case, the reliable transmission of an arbitrary qubit can be used to transmit part of an ebit, so that a secret bit can again be extracted thanks to the untrusted QEC repeater. Afterwards, we will discuss different designs and models, depending on their modus operandi which may be probabilistic or deterministic.

B. Information-theoretic limits for repeater-assisted quantum communications

1. *Ideal chains of quantum repeaters*

Consider a linear chain of N quantum repeaters (trusted or untrusted), labeled by $\mathbf{r}_1, \ldots, \mathbf{r}_N$. This is characterized by an ensemble of $N+1$ quantum channels $\{\mathcal{E}_i\}$ describing the sequence of transmissions $i = 0, \ldots, N$ between the two end-points Alice $\mathbf{a} := \mathbf{r}_0$ and Bob $\mathbf{b} := \mathbf{r}_{N+1}$ (see Fig. 16). Assume the most general adaptive protocol $\mathcal{P}$, where the generation of the secret key between Alice and Bob is ideally assisted by adaptive LOCCs involving all the parties in the chain. (While this network assistance naturally arises with trusted repeaters, it may also arise in a random protocol with untrusted repeaters.) After n uses of the chain, Alice and Bob will share an output state $\rho^n_{\mathbf{ab}}$ which depends on $\mathcal{P}$. By taking the limit of large n and optimizing over all possible protocols $\mathcal{P}$, we define the repeater-assisted secret

key capacity $K(\{\mathcal{E}_i\})$. This quantity satisfies the bound

$$K(\{\mathcal{E}_i\}) \leq E_R^{\bigstar}(\{\mathcal{E}_i\}) := \sup_{\mathcal{P}} \lim_n E_R(\rho_{\mathbf{ab}}^n). \tag{220}$$

where the REE E_R is defined in Eq. (178) and, more weakly, in Eq. (180) for asymptotic states.

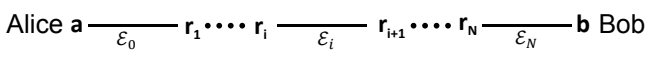

FIG. 16. Chain of N quantum repeaters $\mathbf{r}_1, \ldots, \mathbf{r}_N$ between Alice $\mathbf{a} := \mathbf{r}_0$ and Bob $\mathbf{b} := \mathbf{r}_{N+1}$. The chain is connected by $N+1$ quantum channels $\{\mathcal{E}_i\}$.

In order to bound this capacity, let us perform a cut "i" which disconnects channel $\mathcal{E}_i$ between $\mathbf{r}_i$ and $\mathbf{r}_{i+1}$. We may then simulate channel $\mathcal{E}_i$ with a resource state σ_i, either exactly as in Eq. (182) or asymptotically as in Eq. (183). By stretching the protocol with respect to $\mathcal{E}_i$, we may decompose Alice and Bob's output state as $\rho_{\mathbf{ab}}^n = \bar{\Lambda}_i\left(\sigma_i^{\otimes n}\right)$ for a trace-preserving LOCC $\bar{\Lambda}_i$, which is local between "super-Alice" (i.e., all the repeaters with $\leq i$) and the "super-Bob" (i.e., all the others with $\geq i+1$). This decomposition may be asymptotic for bosonic channels, as specified in Eq. (199).

If we now compute the REE on the output state, we find $E_R(\rho_{\mathbf{ab}}^n) \leq nE_R(\sigma_i)$ for any i and protocol $\mathcal{P}$. By replacing this inequality in Eq. (220), we establish the single-letter bound [58, 59]

$$K(\{\mathcal{E}_i\}) \leq \min_i E_R(\sigma_i) \ . \tag{221}$$

Consider now a chain of teleportation-covariant channels $\{\mathcal{E}_i\}$, so that each quantum channel satisfies the condition in Eq. (187). These channels $\{\mathcal{E}_i\}$ can all be simulated by their (possibly-asymptotic) Choi matrices $\{\sigma_{\mathcal{E}_i}\}$. Therefore, Eq. (221) takes the form

$$K(\{\mathcal{E}_i\}) \leq \min_i E_R(\sigma_{\mathcal{E}_i}) \ . \tag{222}$$

Assume that the quantum channels are distillable, i.e., $E_R(\sigma_{\mathcal{E}_i}) = D_1(\sigma_{\mathcal{E}_i})$ as in Eq. (211), then we have $E_R(\sigma_{\mathcal{E}_i}) = K(\mathcal{E}_i)$ and Eq. (222) becomes $K(\{\mathcal{E}_i\}) \leq \min_i K(\mathcal{E}_i)$. Remarkably, this upper bound coincides with a lower bound. In the case of trusted repeaters, assume that each pair of neighbor repeaters, $\mathbf{r}_i$ and $\mathbf{r}_{i+1}$, exchange a key at their channel capacity $K(\mathcal{E}_i)$ and one-time pad is applied to all the keys to generate an end-to-end key at the minimum rate $\min_i K(\mathcal{E}_i)$. As a result, for distillable chains, we have an exact result for their secret key capacity [58, 59]

$$K(\{\mathcal{E}_i\}) = \min_i K(\mathcal{E}_i) \ . \tag{223}$$

This achievability can also be proven for the case of untrusted ED repeaters: They may distill ebits between neighbors at the (one-way) ED rate $D_1(\sigma_{\mathcal{E}_i}) = K(\mathcal{E}_i)$ and then apply entanglement swapping, so that the minimum common number of ebits is swapped to the end-users. Although in a realistic scenario this optimal procedure would be disadvantageous for Eve, it is still one of the possible protocols that can be implemented (furthermore, the end-users can remotely certify it).

Thanks to the result in Eq. (223), we know the repeater-assisted secret key capacities of chains composed of fundamental channels, such as bosonic pure-loss channels, quantum-limited amplifiers, dephasing and erasure channels. In particular, for a chain of repeaters connected by pure-loss channels with transmissivities $\{\eta_i\}$, we may write the secret key capacity [58, 59]

$$K_{\text{loss}} = -\log_2\left[1 - \min_i \eta_i\right] \ , \tag{224}$$

which is fully determined by the minimum transmissivity in the chain. In particular, consider an optical fiber with transmissivity η which is split into $N+1$ parts by inserting N equidistant repeaters, so that each part has transmissivity $\sqrt[N+1]{\eta}$. Then, we write the capacity

$$K_{\text{loss}}(\eta, N) = -\log_2\left(1 - \sqrt[N+1]{\eta}\right) \ . \tag{225}$$

In a chain connected by quantum-limited amplifiers with gains $\{g_i\}$, we may write [58, 59]

$$K_{\text{amp}} = -\log_2\left[1 - \left(\max_i g_i\right)^{-1}\right] \ . \tag{226}$$

For a chain connected by dephasing channel $\mathcal{E}_i$ with probability $p_i \leq 1/2$, we find [58, 59]

$$K_{\text{deph}} = 1 - H_2(\max_i p_i) \ , \tag{227}$$

where H_2 is the binary Shannon entropy. Finally, for a chain of erasure channels we have $K_{\text{erase}} = 1 - \max_i p_i$ [58, 59].

2. *Quantum communication networks*

The results for repeater chains can be generalized to arbitrary quantum networks by combining methods of channel simulation with powerful results from the classical network theory. Here we do not present the details of this methodology but only an introduction to the main notions and the specific results for pure-loss channels. The reader interested in further details may consult Refs. [58, 59] where they can find a comprehensive treatment and general results for arbitrary quantum channels.

We may represent a quantum communication network as an undirected finite graph $\mathcal{N} = (P, E)$, where P is the set of points (trusted or untrusted) and E is the set of edges. Each point $\mathbf{p}$ has a local ensemble (register) of quantum systems; two points, $\mathbf{p}_i$ and $\mathbf{p}_j$, are logically connected by an edge $(\mathbf{p}_i, \mathbf{p}_j) \in E$ if and only if they are physically connected by a quantum channel $\mathcal{E}_{ij} := \mathcal{E}_{\mathbf{p}_i\mathbf{p}_j}$. Between the two end-points, Alice $\mathbf{a}$ and Bob $\mathbf{b}$, there is an ensemble of possible routes $\Omega = \{1, \ldots, \omega, \ldots\}$. Here

the generic route ω is an undirected path between $\mathbf{a}$ and $\mathbf{b}$, and is associated to a sequence of quantum channels $\{\mathcal{E}_0^\omega, \ldots, \mathcal{E}_k^\omega \ldots\}$. Then, a cut C is a bipartition (A, B) of the points P such that $\mathbf{a} \in A$ and $\mathbf{b} \in B$. The cut-set $\tilde{C}$ of C is the set of edges with one end-point in each subset of the bipartition, i.e., $\tilde{C} = \{(\mathbf{x}, \mathbf{y}) \in E : \mathbf{x} \in A, \mathbf{y} \in B\}$. Given these notions we may define two type of network protocols, which are based either on sequential or parallel routing of the quantum systems.

In a sequential protocol $\mathcal{P}_{\rm seq}$, the network $\mathcal{N}$ is initialized by a network LOCCs, where each point classically communicates with all the others (via unlimited two-way CCs) and each point adaptively performs local operations on its local quantum systems on the basis of the information exchanged. Then, Alice connects to some point $\mathbf{p}_i$ by exchanging a quantum system (with forward or backward transmission depending on the physical direction of the quantum channel). This is followed by a second network LOCC. Then, point $\mathbf{p}_i$ connects to another point $\mathbf{p}_j$ by exchanging another quantum system, which is followed by a third network LOCC and so on. Finally, Bob is reached via some route ω, which completes the first sequential use of $\mathcal{N}$. For the second use, a different route may be chosen. After n uses of $\mathcal{N}$, Alice and Bob's output state $\rho_{\mathbf{ab}}^n$ is ε-close to a private state [703] with nR_n^ε secret bits. Optimizing the rate R_n^ε over all possible protocols $\mathcal{P}_{\rm seq}$ and taking the limit for large n and small ε (weak converse), one defines the single-path secret key capacity of the network $K(\mathcal{N})$.

Note that, similar to repeater chains, network secret key capacities refer to both trusted and untrusted nodes. In the presence of untrusted/unauthenticated nodes, the optimization of the quantum network includes 'good' protocols where the nodes are operated according to an ideal working mechanism (in general, an untrusted node might be operated in a legitimate way and might also involve local quantum operations that are blind to Eve, so that it may be effectively reduced to the performance of a trusted node). Following the theory developed in Refs. [58, 59], a general upper bound may be written for $K(\mathcal{N})$, which takes a particularly simple form for networks of teleportation-covariant channels. Then, for quantum networks connected by distillable channels, the formula for the capacity $K(\mathcal{N})$ can exactly be found. For these networks, the upper bound can be saturated by a sequential protocol where key composition (for trusted nodes) or entanglement distillation (for untrusted nodes) is suitably combined with a classical strategy for finding the best route in the network.

In particular, consider an optical network, so that two arbitrary points $\mathbf{x}$ and $\mathbf{y}$ are either disconnected or connected by a pure-loss channel with transmissivity $\eta_{\mathbf{xy}}$. The single-path capacity of the lossy network $\mathcal{N}_{\rm loss}$ is determined by [58, 59]

$$K(\mathcal{N}_{\rm loss}) = -\log_2(1-\tilde{\eta}), \quad \tilde{\eta} = \min_C \max_{(\mathbf{x},\mathbf{y})\in\tilde{C}} \eta_{\mathbf{xy}}, \quad (228)$$

where $\tilde{\eta}$ is found by computing the maximum transmissivity along a cut, and then minimizing over the cuts.

This result can be also formulated in an equivalent way. In fact, for any route ω of pure-loss channels with transmissivities $\{\eta_i^\omega\}$, we may compute the end-to-end transmissivity of the route as $\eta_\omega := \min_i \eta_i^\omega$. Then the single-path capacity is determined by the route with maximum transmissivity [58, 59]

$$K(\mathcal{N}_{\rm loss}) = -\log_2(1-\tilde{\eta}), \quad \tilde{\eta} := \max_{\omega\in\Omega} \eta_\omega. \quad (229)$$

Finding the optimal route $\tilde{\omega}$ corresponds to solving the widest path problem [760]. Adopting the modified Dijkstra's shortest path algorithm [761], this is possible in time $O(|E|\log_2|P|)$, where $|E|$ is the number of edges and $|P|$ is the number of points.

Consider now a parallel protocol, where multiple routes between the end-points are used simultaneously. More precisely, after the initialization of the network $\mathcal{N}$, Alice exchanges quantum systems with all her neighbor points (i.e., all points she share a quantum channel with). This multipoint communication is followed by a network LOCC. Then, each receiving point exchanges quantum systems with other neighbor points and so on. This is done in such a way that these subsequent multipoint communications are interleaved by network LOCCs and they do not overlap with each other, so that no edge of the network is used twice. The latter condition is achieved by imposing that receiving points only choose unused edges for their subsequent transmissions. This routing strategy is known as "flooding" [762]. Eventually, Bob is reached as an end-point, which completes the first parallel use of $\mathcal{N}$. The next parallel uses of $\mathcal{N}$ may involve different choices by the intermediate nodes. After n uses, Alice and Bob share a private state [703] with nR_n^ε secret bits. Optimizing over all possible flooding protocols, taking the limit for many uses ($n \to \infty$) and the weak converse limit ($\varepsilon \to 0$), one defines the multi-path secret key capacity of the network that we denote by $K^{\rm m}(\mathcal{N})$.

According to Refs. [58, 59], a general upper bound may also be written for $K^{\rm m}(\mathcal{N})$. This simplifies for a network of teleportation-covariant channels and even more if the channels are distillable, in which case the capacity $K^{\rm m}(\mathcal{N})$ is completely established (the upper bound is achieved similarly to the single-path case, but where key composition or entanglement distillation are now combined with an optimal multi-path routing strategy). As an example, consider again a network $\mathcal{N}_{\rm loss}$ composed of pure-loss channels, so that each edge $(\mathbf{x}, \mathbf{y})$ has transmissivity $\eta_{\mathbf{xy}}$. For any cut C, define its total loss as $l(C) := \prod_{(\mathbf{x},\mathbf{y})\in\tilde{C}}(1-\eta_{\mathbf{xy}})$. By maximizing $l(C)$ over all cuts we define the total loss of the network, i.e., $l(\mathcal{N}_{\rm loss}) := \max_C l(C)$. The multi-path capacity of $\mathcal{N}_{\rm loss}$ is therefore given by [58, 59]

$$K^{\rm m}(\mathcal{N}_{\rm loss}) = -\log_2 l(\mathcal{N}_{\rm loss}). \quad (230)$$

The optimal multi-path routing of is provided by the solution of the maximum flow problem, which can

be found in $O(|P| \times |E|)$ time by using Orlin's algorithm [763]. As one may expect, the multi-path capacity $K^{\mathrm{m}}(\mathcal{N}_{\mathrm{loss}})$ outperforms the single-path version $K(\mathcal{N}_{\mathrm{loss}})$. In this regard, Refs. [58, 59] provided the first information theoretic proof that using multi-path routing for distributing entanglement or secret correlations can provide a non trivial advantage in a quantum network. This aspect was further investigated in a subsequent work [67] considering non-ideal repeaters. Finally, note that multi-end generalizations have been also studied [60, 78].

C. Quantum repeaters based on ED and QEC

One of the key features of a future quantum internet [764] is the ability to transfer quantum states reliably from one point to another. As basic as it sounds, this is one of the most challenging implementation tasks that quantum technologies face. There are two main approaches to solving this problem. One relies on using teleportation techniques, which themselves rely on one of the pillars of quantum information science, i.e., entanglement. In this scenario, the state transfer problem reduces to how we can efficiently distribute entanglement across a network [55, 57, 765, 766]. The second solution relies on using QEC techniques to overcome loss and operation errors [767–772]. This is similar to what we have in data communications networks where by adding some redundancy to our message we can correct some of the errors that might be added by the channel. In the quantum case, not only we have to correct the bit flip errors, but also phase flip and erasure errors in possibly a fault-tolerant way. This approach will then require advanced quantum computing modules.

Both above solutions are considered to be part of an underlying platform that enables quantum networks to operate at any distance. From the point of view of QKD, both solutions would enable us to construct a secure QKD network with untrusted repeaters (i.e., an end-to-end QKD network) which is also potentially scalable to an arbitrary number of nodes. It is true that scalability can also be achieved by means of trusted QKD nodes, but losing the well-desired end-to-end property. On the other hand, it is unclear whether untrusted QKD nodes based on measurements, like MDI- and TF-nodes, could also be exploited in some scalable way, without involving the help of other types of repeaters (e.g., trusted or entanglement based).

Original proposals on quantum repeaters were based on ED and relied on the use of entanglement swapping in a nested way [55]. Suppose you have distributed and stored a Bell state between nodes A and B at distance L_0 in a network. Suppose node B also shares a Bell state with node C farther apart by L_0. Then, by performing a Bell-state measurement (BSM) on the two subsystems in node B, we can entangle the systems in node A and C. That means that if we can distribute entanglement over distance L_0, by using entanglement swapping, we

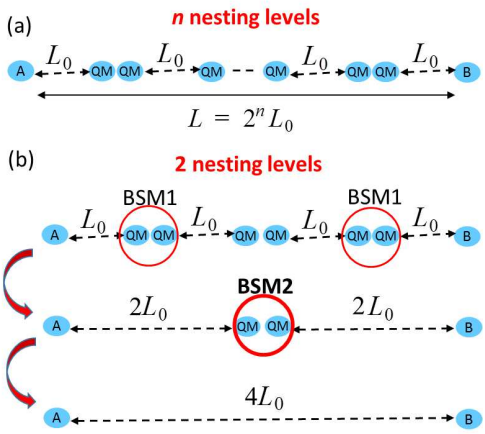

FIG. 17. Typical working mechanism of an ED repeater. Here QM denotes a quantum memory. (a) A quantum repeater link with nesting level n. (b) An example of quantum repeater link with nesting level 2. BSM1 operations extend the entanglement over $2L_0$. BSM2 would then extend it further to $4L_0$. Note that if BSM operations are probabilistic, BSM2 should not be done until the middle node learns about the success of BSM1 operations. This requirement slows down the process and makes the coherence time requirements on the memories more demanding. Reproduced from Ref. [773] under permission of the IOPP.

can extend it to $2L_0$. By using this technique n times, in a nested way, we can then in principle cover entanglement over a distance $L = 2^n L_0$, where n would be the nesting level for our repeater system; see Fig. 17. Looking at this from a different angle, what we have basically done is that in order to distribute entanglement over distance L, we have divided the entire distance into 2^n segments, distributed and stored entanglement over elementary links with distance L_0, and then applied BSMs on the middle nodes to extend the entanglement over distance L. The entanglement distribution rate over distance L would then scale with $\exp(-\alpha L_0)$ instead of $\exp(-\alpha L)$, where α is proportional to the channel attenuation parameter.

The above discussion makes some idealistic assumptions on the system components. In practice, we should also account for the imperfections in the setup. For instance, the distributed state over elementary links may not be a maximally entangled states, in which case, by every BSM, we deviate further from the ideal state. The measurement operations may also not be error free or deterministic to begin with. These issues require us to apply certain entanglement distillation techniques to improve the quality of distributed entangled states [710, 774]. But, that would add to the quantum computational cost of the system and makes its implementation even more challenging. Depending on the state of the art on quantum computing, we can then envisage several different stages of development for quantum repeaters [773, 775]. In the following, we review three such classes, or generations [776], of quantum repeaters.

1. Probabilistic ED repeaters

Since the introduction of the ED-based quantum repeaters, a lot of research has been directed into devising quantum memory units that can interact efficiently with light and can store quantum states for a sufficiently long time. The interaction with light is necessary for such devices as it would allow us to use photonic systems for both distribution and swapping of entanglement. Photon-based systems are, however, fragile against loss and that could result in probabilistic operations, which, in turn, require us to repeat a certain procedure until it succeeds. These problems led to consider probabilistic ED repeaters which are those that rely on probabilistic techniques for entanglement distribution and entanglement swapping. This class of repeaters has been at the center of experimental attention in the past 20 years.

There are different ways of distributing entangled states between quantum memories of an elementary link. In some proposals [765], entangled photons are generated at the middle of the link and sent toward quantum memories located at the two end of the elementary link. If these photons survive the path loss and can be stored in the memories in a *heralding* way we can then assume that the two memories are entangled. This technique requires us to have a verification technique by which we can tell if the storing procedure has been successful. Alternatively, in some other proposals, we start with entangling a photon with the memory and either send it to the other side for a similar operation or swap entanglement in the middle between two such memories. The most famous proposal of this type is that of Duan, Lukin, Cirac, and Zoller [57], known as DLCZ, whose many variants [766] have been proposed and partly demonstrated in practice [777, 778].

The BSM operation in probabilistic ED repeaters is typically done by first converting the state of quantum memories back into photonic states and then use linear optics modules to perform the BSM. Such linear optics modules can, however, be inefficient and face certain limitations in offering a full BSM [779]. There are certain tricks [780–783] by which their performance can be improved, but, in the end, the chance of success in most practical settings would remain below one. An implication of a probabilistic BSM is that we cannot perform BSMs in a certain nesting level until we have learned about the results of the BSMs in the previous nesting level. That requires exchanging data between intermediate nodes, which can not be done faster than the transmission delay between such nodes. This would result in requiring long coherence time and a low entanglement generation rate for probabilistic repeaters.

One remedy to the above problems is the multiple-memory configuration in Fig. 18. In this setup, instead of one quantum memory in each site, we use a bank of N memories. In each round of duration $T_0 = L_0/c$, with c being the speed of light in the classical channel, we attempt to entangle as many elementary links as possible. We then mix and match entangled pairs across

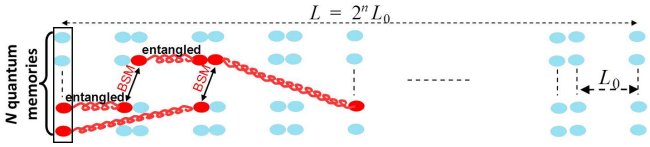

FIG. 18. A probabilistic ED repeater with multiple memories per node. In each round, entanglement distribution is attempted on all available elementary links. BSMs, at different nesting levels, will also be performed by matching as many entangled pairs as possible [784] Reproduced from Ref. [773] under permission of the IOPP.

two neighboring links and perform as many BSM operations as possible. As we continue doing informed BSMs and, at the same time, refilling available elementary links with fresh entangled states, we get to a steady state that in every period we roughly generate $NP_S P_M^n$ entangled states, for $N \gg 1$, between the far two ends of the network [784]. Here, P_S is the success probability for the employed entanglement distribution scheme for elementary links and P_M is the success probability for the BSM operation. Moreover, it roughly takes $T = L/c$ to generate an entangled pair, which minimizes the requirements on the memory coherence time. Multi-mode structures for quantum memories have also been proposed and implemented to improve the performance in repeater setups [785–787].

Probabilistic ED repeaters are the simplest repeater technology to be implemented in practice, with recent investigations in the setting of DI-QKD [73]. Even the simplest setup, when there is only one repeater node in the middle, can offer certain advantages for QKD applications. These setups, known as memory-assisted QKD [788, 789], can soon offer better rate-versus-distance scaling than most conventional QKD systems in operation by using existing quantum memory technologies [790–795]. Over long distances, however, probabilistic ED repeaters would suffer from a low rate, or require a large number of memories to perform well [796–798]. Part of the reason for such low key rates is the use of probabilistic BSM modules. We next see what can be achieved if we have a deterministic BSM unit.

2. Deterministic ED repeaters

The original theoretical proposal for an ED repeater relied on *deterministic*, but possibly *erroneous*, gates for BSM, or similar, operations [55]. In this protocol, the authors assumed that the initial entanglement distribution and storage have already taken place, and one needs to manipulate a number of entangled quantum memories in such a way that we end up with a high quality entangled state between the two remote end-users. In Sec. XII C 1, although we assumed that the BSM operation may succeed probabilistically, we did not account

for possible errors that may be caused by BSM modules. Further, we assumed that the initial entanglement over the elementary links was of the ideal form of a maximally entangled state, e.g., Bell states. Ref. [55] looked at the latter two issues by assuming that BSMs can directly be applied to the quantum memories in a deterministic way. The immediate advantage is that P_M would become 1, which increases the rate and also reduces the waiting time caused by the probabilistic events and their corresponding transmission delays. Once one accounts for errors, however, other problems arise.

In reality, it is very challenging to generate and distribute truly maximally entangled states. In practice, we should often allow for deviations from this ideal case, which can be measured in different ways. For instance, for two pairs of entangled states in a Werner state with parameter p, a BSM on the middle memories would leave the remote memories in a Werner state with parameter $2p$ [55]; that is, the error, or the deviation from the ideal state, has been doubled. In a quantum repeater link as in Fig. 17(a), such an error will get doubled, even if we have perfect deterministic BSM gates, for every nesting level. The danger is that after a certain number of nesting levels the quality of the resulting entangled states is so low that it may not be of any use for quantum applications. If we include the possible errors in the gates, the situation would become even worse.

The solution suggested in [55] is based on the use of purification, or, entanglement distillation, techniques. In short, the idea is that if we are given M pairs of non-ideal entangled states, we can use some LOCCs to come up with $N < M$ entangled states of higher quality, for instance, higher fidelity. Depending on the type of distillation techniques used, we may end up with different rate behaviors. Original distillation schemes relied on performing CNOT gates on pairs of memories [799] and then measuring one of them.

An alternative solution is to use QEC schemes to distil entanglement [800–802]. In essence, we can think of the M non-ideal entangled states that we wish to distil to have been obtained by hypothetically starting with N ideal entangled states, adding $M - N$ redundant states to this batch, and sending all M pairs through an error-prone channel. In such a setting, one can, in principle, use QEC techniques to get the original N pairs back. This can be done with a high probability if the ratio N/M is chosen properly with respect to the expected amount of error in the system. It turns out that, if we want to do this in an error resilient way, we need quantum gates with error rates on the order of 0.001–0.01 or below.

Using the above techniques, one can design quantum repeaters with a modestly high key rate. The limitation is mainly coming from the original requirement for entangling elementary links (which is intrinsically a probabilistic process) and the trade-off between having more nesting levels, and, therefore, higher P_S, versus fewer nesting levels, hence less accumulated error and distillation. Next we show that if we allow for sophisticated quantum operations to be used in quantum repeaters, we can further improve the rate by relaxing the requirement on entangling elementary links.

3. *Memory-less QEC repeaters*

The most advanced protocols for quantum repeaters leave as little as possible to probabilistic schemes. In such schemes, loss-resilient QEC techniques are used to make sure that the *quantum* information carried by photonic systems can be retrieved at each intermediate node. This can be achieved in different ways. The common feature of all these schemes is that we no longer need quantum memories for storage purposes, although we may still need them for quantum processing.

Here, we explain one example that relies on QEC for loss resilience. This idea was first proposed in Ref. [768] and then further work followed up to also account for not only the loss in the channel, but also possible errors in the system [770, 771]. In Ref. [768], a quantum state $\alpha|0\rangle + \beta|1\rangle$ is encoded as

$$|\Psi\rangle^{(m,n)} = \alpha|+\rangle_1^{(m)} \cdots |+\rangle_n^{(m)} + \beta|-\rangle_1^{(m)} \cdots |-\rangle_n^{(m)}, \tag{231}$$

where n is the number of logical qubits and m is the number of physical qubits in each logical qubit. Here, $|\pm\rangle^{(m)} = |0\rangle^{\otimes m} \pm |1\rangle^{\otimes m}$. This encoding has the property that the original quantum state can be recovered provided that at least (1) one photon survives in each logical qubit, and (2) one logical qubit, with all its m constituent photons, is fully received. The authors showed that, for sufficiently short channels, one can find appropriate values of m and n such that a high key rate on the order of tens of MHz can, in principle, be achieved. The requirements are, however, beyond the reach of current technologies.

Refs. [803, 804] designed a linear-optics version of the original scheme of Ref. [770]. This version entirely removes any complicated gates such as CNOT gates and only requires one-way communication (both quantum and classical). Furthermore, no feedforward is needed for the error correction steps (but feedforward and switching may be needed for the local state preparation if it is also based on linear optics). More recently, Ref. [805] has generalized these results to linear-optics logical Bell measurements on QEC codes.

In general, memory-less QEC repeaters, while offering a substantial improvement in the key rate, require a set of demanding properties for their required elements. In particular, we need operation errors as low as $10^{-4} - 10^{-3}$, large cluster states of photons, whose generation may require a series of other advanced technologies (e.g. high-rate efficient single-photon sources), and a large number of intermediate nodes. The latter may cause compatibility problems with existing optical communications infrastructure, in which, at the core of the network, nodes are rather sparsely located. That said, such advanced tech-

nologies for quantum repeaters would perhaps be one of the latest generations of such systems, by which time sufficient improvement in our quantum computing capabilities as well as other required devices and technologies may have already happened. For such an era memoryless repeaters offer a solution that is of an appropriate quality for the technologies that rely on the quantum internet [764, 806, 807].

4. Other studies on quantum repeaters

Our review is clearly not exhaustive of all the possible studies on ED-based or QEC-based quantum repeaters. This is a very active field with so many contributions aimed at sustaining long-distance of various quantum tasks. There is an increasing number of CV schemes for entanglement (and key) distillation based on non-Gaussian elements, such as photon subtraction, quantum catalysis, quantum scissors, symmetric photon replacement, purifying distillation, etc. [477, 808–813]. There are also several proposal for CV repeaters [814–817] besides models of hybrid DV-CV repeaters [818–824].

XIII. QKD AGAINST A BOUNDED QUANTUM MEMORY

A. Introduction

Quantum cryptography is usually defined under the assumption that a potential eavesdropper (Eve) has access to unlimited technology. For example, Eve may have a universal quantum computer with unlimited computational power, as well as a perfect quantum memory of unbounded capacity and measurement apparatuses. While these strong assumptions put quantum cryptography on a solid theoretical ground, they may be considered unrealistic given the present stage of development of quantum technologies. Such strong assumptions create a disproportion between the technology that will be deployed in future and what already available to Eve.

A different scenario is defined by assuming that Eve can only access limited quantum technology. Here we first review the bounded quantum storage model (BQSM), in which Eve is assumed to be able to store only a limited number of qubits [825, 826]. The BQSM is a special case of a more general model in which the adversary quantum memory is noisy [827]. Then we consider the application of quantum data locking (QDL) for QKD within these memory-constrained models. Note that, unlike Alice and Bob, Eve is granted access to a universal quantum computer with unbounded computational power and can perform ideal quantum measurements. Entropic uncertainty relations [626, 828] play a major role in security proofs against an adversary with constrained quantum memory.

We remark that, with suitable constraints in the adversary quantum memory, one obtains provable security for every two-party cryptography, i.e., for protocols involving two users who do not trust each other [829–831]. Examples are bit commitment, oblivious transfer, and secure identification. These protocols are otherwise known to be insecure if there is no constraint on the adversary quantum storage capacity. For applications in QKD, BQSM yields an increased robustness to noise. In particular, applications of QDL within the BQSM substantially boost the QKD rate [832].

B. Entropic uncertainty relations for multiple observables

Entropic Uncertainty Relations EURs [626, 828] have already been discussed in Section IX. Here we focus on EURs involving multiple observables. Consider a collection of k observables in a Hilbert space of dimensions d. On a given state ρ, a measurement of the j-th observable outputs a random variable X_j, taking values in the alphabet $\{x_j\}$ with probability $p_{X_j}(x_j)$. An EUR is then expressed by an inequality quantifying the uncertainty in the measurement outcomes. For example, in terms of the Shannon entropy, an EUR is an inequality of the form

$$\frac{1}{k}\sum_{j=1}^{k} H(X_j) \geq c\,, \tag{232}$$

where $H(X_j) = -\sum_{x_j} p_{X_j}(x_j)\log_2 p_{X_j}(x_j)$ is the post-measurement Shannon entropy, and c is a state-independent constant that only depends on the set of measurements considered.

Given a collection of k observables, one can always find a state ρ such that $H(X_j) = 0$ for a given j. Therefore the constant c in Eq. (232) cannot be larger than $\left(1-\frac{1}{k}\right)\log_2 d$. An EUR that saturates this bound is said to be maximally strong. The Maassen-Uffink EUR [622], which is defined for $k = 2$ observables, is a maximally strong EUR if the observables are mutually unbiased. To find maximally strong EUR for multiple observables is a non-trivial task, as a set of $k > 2$ mutually unbiased observables does not in general define a maximally strong EUR. An almost maximally strong EUR is obtained for a maximal choice of $k = d+1$ mutually unbiased observables, in which case the constant $c_{\mathcal{M}}$ in Eq. (232) equals $\log_2 \frac{d+1}{2}$ [833].

Random observables asymptotically satisfy maximally strong EURs in a high dimensional Hilbert space. Ref. [834] showed that a random choice of k random observables (distributed according to the unitary invariant measure) satisfies a maximally strong EUR with probability arbitrary close to 1, provided that d is large enough and k grows at least logarithmically in d (see also Refs. [829, 835]). Recently, Ref. [836] showed that this property holds for large d at any fixed value of k.

Uncertainty relations can be expressed not only in terms of the Shannon entropy. For example, fidelity uncertainty relations have been defined in Ref. [837], and metric uncertainty relations have been introduced in Ref. [835]. For cryptographic applications one requires EURs for the min-entropy. These are all stronger forms of uncertainty relations, in the sense that they always imply an EUR, while the contrary does not necessarily hold.

C. QKD in the bounded quantum storage model

In this section we briefly review some basic notions regarding the BQSM. To make things more concrete, we consider a one-way protocol in which the sender Alice encodes a variable X of cardinality d into a d-dimensional Hilbert space. The protocol is specified by a collection of k mutually unbiased observables. Alice randomly selects one of the observables and then encodes the classical random variable X by using the corresponding eigenvectors as code words. On the receiver side, Bob independently selects one of the observables and perform the corresponding projective measurement. For example, the BB84 protocol can also be realized within the BQSM, with n photon transmissions and $d = 2^n$. After the quantum part of the protocol, in which n states are prepared, transmitted, and measured, the users proceed with the sifting phase, in which they select only the signal transmissions for which they have made the same choice of bases. The protocol then concludes with EC and PA. The difference with standard QKD is that in the BQSM the eavesdropper is assumed to be capable of storing only a relatively small number of qubits. More specifically, it is assumed that Eve can keep no more than q qubits in her quantum memory after n quantum signal transmissions and before sifting. Therefore, all remaining quantum states intercepted by Eve have been already measured before the sifting phase takes place.

A fundamental estimate of the number of secret bits (excluding sifting) that can be extracted from such a protocol (in DR) is given by

$$\ell^\epsilon \simeq H^\epsilon_{\min}(X^n|ZE) - H_{\max}(C)\,, \tag{233}$$

where ϵ is a security parameter, $H^\epsilon_{\min}(X^n|ZE)$ is the smooth min-entropy [107, 546] conditioned on Eve's side information for n signal transmissions, and $H_{\max}(C)$ is the number of bits publicly exchanged for EC. Under the assumptions of the BQSM, Eve's side information comprises a quantum part E and a classical part Z. Furthermore, since Eve's quantum memory has capacity below q qubits, we have

$$\ell^\epsilon \gtrsim H^\epsilon_{\min}(X^n|Z) - q - H_{\max}(C)\,. \tag{234}$$

It remains to bound the (classical) conditional smooth min-entropy $H^\epsilon_{\min}(X^n|Z)$. For example, it has been shown in Ref. [825] that if the set of k bases employed in the protocol satisfies an EUR as in Eq. (232), then for any $\lambda \in (0, 1/2)$

$$H^\epsilon_{\min}(X^n|Z) \geq (c - 2\lambda)n\,, \tag{235}$$

with

$$\epsilon = \exp\left[-\frac{\lambda^2 n}{32(\log_2(kd/\lambda))^2}\right]. \tag{236}$$

For pair of mutually unbiased bases we can apply the Maassen-Uffink EUR and obtain, for sufficiently small λ

$$H^\epsilon_{\min}(X^n|Z) \gtrsim \frac{n}{2}\log_2 d\,. \tag{237}$$

Later works have obtained tighter and tighter bounds on the min-entropy [838, 839].

In general, the BQSM yields improved resilience to noise in a QKD protocol, but the rate is not expected to improve dramatically compared to an unbounded quantum-capable eavesdropper. We conclude by noting that the number of secret bits in Eq. (233) must be multiplied by a factor $1/k$ to account for the probability that Alice and Bob chose the same observable: therefore the number of observables should be kept small in practical protocols. Experimental demonstrations of protocols of oblivious transfer in the QBSM were presented in Refs. [840, 841].

D. Quantum data locking

A substantial boost in the QKD rates can be obtained within the BQSM by exploiting maximally strong EURs for multiple observables. If the number k of observables is large but much smaller than the Hilbert space dimensions, Alice and Bob can agree *a priori* and in secret on which observable to use to encode and decode information. This allows them to get rid of the $1/k$ reduction in the key rate due to the sifting phase [825]. This plan is made possible by the phenomenon of QDL, which implies the existence of (almost) maximally strong EURs with a number of observables much smaller than the Hilbert space dimensions.

The first QDL protocol was discussed in Ref. [842]. Such a protocol is analogous to BB84, with the fundamental difference that now Alice and Bob share 1 secret bit at the beginning of the protocol [842]. While in BB84 Alice and Bob randomly select their local basis, and only later reconcile their choice in the sifting phase, in QDL they use the 1 bit of information they secretly share to agree on the choice of the basis in which encode (and decode) information. Therefore, according to this secret bit, Alice encodes n bits into n qubits, using either the computational or the diagonal basis, and Bob measures the received qubits in the same basis. We follow the original presentation of Ref. [842] and assume a noiseless channel from Alice and Bob. The security analysis is performed under the assumption that Eve intercepts the n signal qubits.

Consider the joint state representing the classical n-bits sent by Alice together with the quantum state intercepted by Eve. Such a classical-quantum state reads

$$\rho_{XE} = \sum_{x^n=0}^{2^n-1} 2^{-n} |x^n\rangle\langle x^n| \otimes \frac{1}{2} \sum_{j=0,1} U_j^n |x^n\rangle\langle x^n| U_j^{n\dagger}\,, \tag{238}$$

where X denote the classical variable sent by Alice, U_0 is the identity transformation and U_1 is the unitary that maps the computational basis into the diagonal one. Notice that this expression reflects the fact that Eve does not know which basis has been used for the encoding. For the sake of presentation, and to emphasize the link with EURs, consider Eve's accessible information

$$I_{\rm acc}(X:E)_\rho = \max_{M_{E\to Z}} I(X:Z) \tag{239}$$

$$= \max_{M_{E\to Z}} H(X) - H(X|Z) \tag{240}$$

$$= n - \min_{M_{E\to Z}} H(X|Z)\,, \tag{241}$$

where the maximum is over all possible measurements $M_{E\to Z}$ performed by Eve on n qubits. A straightforward calculation yields [842]

$$I_{\rm acc}(X:E)_\rho = n - \min_{M_{E\to Z}} H(X|Z) \tag{242}$$

$$\leq n + \max_\phi \frac{1}{2} \sum_{j,x^n} |\langle\phi|U_j|x^n\rangle|^2 \log_2 |\langle\phi|U_j|x^n\rangle|^2\,. \tag{243}$$

Notice that the last term on the right hand side is bounded by an EUR. In particular, here we can apply Maassen-Uffink EUR [622] and obtain

$$I_{\rm acc}(X:E)_\rho \leq \frac{n}{2}\,. \tag{244}$$

In summary, being ignorant of one single bit of information, Eve is able to access only $n/2$ bits of information about the n bits of information communicated from Alice to Bob. This holds for all values of n. As a matter of fact, to obtain robust security guarantee we need the accessible information to be arbitrarily small. This has been shown in later works that exploited EURs for multiple observables [834].

From a broader perspective, a QDL protocol is defined by a set of $k \ll d$ different bases in a Hilbert space of dimensions d. For an eavesdropper that does not have which-basis information (i.e., $\log_2 k$ bits) the accessible information is smaller than δ. Therefore, EURs for k bases in a d-dimensional space can be applied to obtain a corresponding QDL protocol. Ref. [834] has shown that a random choice of the $k = (\log_2 d)^3$ bases (sampling according to the distribution induced by the Haar measure) in a d-dimensional Hilbert space will yield a QDL protocol with $\delta = \epsilon \log_2 d + O(1)$, as long as d is large enough. The probability that a random choice of bases yield a QDL protocol with these feature is bounded away from 1 if $\log_2 d > \frac{16}{C''\epsilon} \ln \frac{20}{\epsilon}$, with $C'' = (1760 \ln 2)^{-1}$. As $\log_2 d$ grows faster than linearly in $1/\epsilon$, this implies that QDL is obtained only for asymptotically large values of d. For example, putting $\epsilon = 10^{-1}$ one gets the condition $\log_2 d \gtrsim 10^6$. A typicality argument shows that as long as k is sufficiently smaller than d, these bases are with high probability approximate mutually unbiased [835]. Interestingly enough, a collection of (exact) mutually unbiased bases does not necessarily yield QDL [828].

A major advance in QDL was provided by the work of Fawzi et al. [835], which has introduced the notion of metric uncertainty relations. Exploiting this powerful tool they have been able to obtain strong QDL protocols with $\delta = \epsilon \log_2 d$ and $\log_2 k = 4 \log_2 (1/\epsilon) + O(\log_2 \log_2 (1/\epsilon))$, for any $\epsilon > 0$ and for d large enough. While these protocols are for random unitaries (which cannot be simulated efficiently), they also demonstrated QDL with a set of unitaries that can be simulated efficiently on a quantum computer. We remark that these results still require asymptotically large values of d. The QDL protocols of Ref. [835] were the first to allow for an arbitrary small accessible information. As for Ref. [834], the protocols succeed only for asymptotically large values of d.

We remark that QDL represents one of the main differences between classical and quantum information theory. In fact, it is well known that the only way to encrypt a string of n bits in a provable secure way is to use a secret key of the same length [843]. By contrast, QDL shows that, when information is encoded in a quantum information carrier, one can obtain provable secure encryption with a much smaller key.

Whereas QDL was historically introduced in terms of the accessible information, it can also be expressed in terms of stronger security quantifiers, e.g., the total variation distance via Pinsker inequality [844]. This in turn allows one to express the security of a QDL in terms of smooth min-entropy with classical side information. The metric uncertainty relations of Ref. [835] and the fidelity uncertainty relations of Ref. [837] also yield QDL with a stronger security quantifier.

E. Quantum data locking for communication: the quantum enigma machine

QDL was considered for the first time in a communication scenario in Refs. [845, 846]. The authors of Ref. [846] considered a noisy communication channel from Alice to Bob (notice that previous works only considered a noiseless channel). Two scenarios were analyzed: in strong QDL Eve is able to access the input of the channel; in weak QDL she has access to the output of the complementary channel from Alice to Bob. Notice that weak QDL is analogous to the familiar wiretap channel model. Strong QDL is instead closer to the original formulation of QDL. The notion of weak and strong QDL capacities were introduced and in part characterized. In analogy to the notion of private capacity of quantum channel, the (weak and strong) QDL capacities are de-

fined as the maximum asymptotic rate at which Alice and Bob can communicate through the quantum channel with the guarantee that Eve has no information about the exchanged messages. The difference with the notion of private capacity is that to achieve the QDL capacities we assume that Eve is forced to make a measurement as soon as she obtains a train of n signals (then n is made arbitrary large to obtain an asymptotic rate).

Since it is defined accordingly to a weaker security definition, the weak QDL capacity is never smaller than the private capacity. A consequence of the results of Ref. [835] is that the identity qubit channel has unit strong QDL capacity. Entanglement breaking channels and Hadamard channels are instead shown having vanishing weak QDL capacity [846]. Ref. [847] provided explicit examples of quantum channels with a large gap between the private capacity and the weak QDL capacity.

A quantum optics device that exploits QDL for secure communication was dubbed a quantum enigma machine (QEM) by Lloyd [845]. In fact, the protocol of QDL can be seen as a quantum generalization of poly-alphabetic ciphers, among which one of the most famous examples was the Enigma machine. Ref. [845] put forward two architectures for a QEM, using either unary encoding of a single photon over n modes (this would be a direct application of the QDL protocols in Refs. [834, 835]) or using encoding in coherent states. Ref. [846] showed that a weak QDL protocol with coherent state cannot surpass the private capacity by more than $\log_2 e \simeq 1.44$ bits per bosonic mode, and an almost matching lower bound was obtained in Ref. [848].

F. Practical quantum data locking

The QDL protocols of Refs. [834, 835] require coherent control over large (actually asymptotically large) Hilbert space. For this reason there is little hope that these protocols may be ever realized experimentally, not even as a proof-of-principle demonstration. In order to make an experimental realization of QDL feasible, one needs to solve two problems: 1) to design QDL protocols that require control over Hilbert space of reasonably small dimensions; 2) to design protocols that are robust in the presence of a noisy channel from Alice to Bob. Step forwards towards the solution of these two problems were made in Ref. [849]. The authors of this work considered a collection of n d-dimensional systems, where d is supposed to be a small integer and n is large. Instead of considering random unitaries in a large Hilbert space, they considered local random unitaries in the small d-dimensional systems. This model can be physically realized by a train of n photons, each living in the space defined by a discrete collection of d bosonic modes (spanning, for example, spatial, temporal, frequency, or angular momentum degrees of freedom).

Unlike other QDL protocols that exploit EURs, QDL with local unitaries is obtained from a different upper bound on the accessible information, i.e.,

$$I_{\rm acc}(X:E) \leq n \log_2 d - \min_\phi H[Q(\Phi)]\,, \tag{245}$$

where

$$H[Q(\Phi)] = -\sum_{x^n} Q_{x^n}(\phi) \log_2 Q_{x^n}(\phi)\,, \tag{246}$$

and

$$Q_{x^n}(\phi) = \frac{1}{k}\sum_{j=1}^{k} |\langle\phi|U^n|x_n\rangle|^2\,. \tag{247}$$

The quantity $\min_\phi H[Q(\Phi)]$ is then bounded by exploiting the fact that $Q_{x^n}(\phi)$ typically concentrates around $1/d^n$ (a similar approach was used in Ref. [850] to obtain QDL with a set of commuting unitaries). Exploiting this approach, Ref. [849] demonstrated strong QDL protocols for QKD through generic memoryless qudit channels, and Ref. [851] obtained weak QDL protocols for direct secret communication. The price to pay to deploy QDL with local unitaries is that the amount of pre-shared secret key bits is no-longer exponentially smaller than the message but grows linearly with the number of channel uses, with an asymptotic, constant, rate of 1 bit per use of the channel. This implies that non-zero rates can only be obtained for $d > 2$, yet any value of d equal or larger than 3 can yield a non-zero rate of QKD or direct communication.

A model of quantum enigma machine that encodes information using multiple photons has been proposed and analysed in Ref. [852]. In this scheme, $\log_2 \binom{m}{n}$ bits are encoded using n photons over m optical modes (with maximum 1 photon per mode). The encryption is then obtained using a set of random linear optics unitaries. Compared with the single-photon encoding, this scheme provides a more efficient use of resources and a higher rate of bits per mode. This encryption schemes exploits the same physics of Boson Sampling [853], yet unlike Boson Sampling does not require $m \gg n^2 \gg 1$ and it is therefore experimentally feasible with current technology.

G. Experimental demonstrations

The first experimental demonstrations of QDL appeared in 2016. Ref. [854] realized the original QDL protocol [842] with encoding in heralded single photon polarization. Ref. [855] realized the QDL protocol of Ref. [849] using pulse-position modulation. In Ref. [855] a lens was used to implement a Fourier transform and an array of 128×128 spatial light modulators (SLM) was applied to generate random phase shifts. This transformation provides QDL given that at the receiver end a trusted user applies the inverse phase shift and inverse Fourier transform to decode [849]. Finally, Ref. [856] presented an on-chip array of programmable ring resonators that can be naturally applied to QDL with encoding in time of arrival degree of freedom.

XIV. QUANTUM RANDOM NUMBER GENERATION

A. Introduction

Generating random numbers is an important task: most cryptographic protocols rely on them, they are used in simulations, in lotteries, in games and numerous other places. However, in spite of their usefulness, random number generators (RNGs) are difficult to construct and the use of poor-quality random numbers can be detrimental in applications. For instance, in Ref. [857] public RSA keys were collected from the web and a significant number were found to share a prime factor, posing problems for the security of those running the algorithm. In general, problems can arise whenever something that is assumed to be chosen randomly is in fact not [858].

A typical way to make random numbers is to use a pseudo random number generator, in which a short random seed is expanded into a longer string. The idea is that this string is sufficiently random for the application it will be used in. However, a pseudo random number generator is a deterministic algorithm, so, in spite of its length, the output contains no more randomness than the input. It must therefore contain subtle correlations that in principle could be detected and exploited. Given a powerful enough computer, a long enough output sequence could be used to find the seed and hence all of the remaining purportedly random numbers.

Since classical physics is deterministic, RNGs based on classical effects can never be fundamentally random. Instead classical RNGs rely on a lack of knowledge making the numbers appear random. Whether this is good enough for a particular application is a matter of faith, and an undesirable property of such RNGs is that it can be difficult to detect if they are functioning badly. Indeed, while statistical tests are able to attest (beyond reasonable doubt) to particular shortcomings of a candidate RNG, there is no set of tests that can take the output from a candidate RNG and eliminate all shortcomings.

To understand this, it is helpful to define what we mean when we say that a particular string is random. Note that, although the string S will always be classical, we want it to appear random even to an adversary holding quantum information and hence the definition is phrased in terms of quantum states. This definition is related to the definition of a secure key (cf. Section II D). If a random number generation protocol outputs an n bit string S, we would like it to be uniform and unknown to any other party, i.e., independent of any side information E held. Mathematically, for S to be a high quality random string we would like that

$$D(\rho_{SE}, \frac{1}{n}\mathbb{1}_n \otimes \rho_E) \tag{248}$$

is small and we say that a protocol is secure if

$$p(\bar{\perp})D(\rho_{SE}, \frac{1}{n}\mathbb{1}_n \otimes \rho_E) \tag{249}$$

is small, where $p(\bar{\perp})$ is the probability that the protocol does not abort (note the similarity with the secrecy error, $\varepsilon_{\text{secr}}$, from Section II D). As before, this means that whenever there is a high probability of not aborting, the output is close to perfect randomness, i.e., $\rho_{SE} \simeq \frac{1}{n}\mathbb{1}_n \otimes \rho_E$. Unlike in key distribution, there is no second string that the first one needs to be perfectly correlated with, so there is no analogue of the correctness error.

From this definition, it is evident that no amount of statistical testing on the output can verify that S is a high quality random string: statistical tests on S can only increase confidence that $\rho_S \simeq \frac{1}{n}\mathbb{1}_n$, but cannot say anything about whether $\rho_{SE} \simeq \frac{1}{n}\mathbb{1}_n \otimes \rho_E$, i.e., whether another party could already know the string S. (For some applications, it may not be a problem for another party to know the string, provided that it is statistically random; here we focus on the stronger form of randomness.) Whether a string is random or not is ultimately not a property of the string itself, but on how it is generated.

Like in the case of QKD, we can divide QRNGs into two types depending on whether or not the users trust the apparatus they use (there are also hybrids, not discussed here, in which certain features are trusted and others not, e.g., semi-device-independent QRNGs [859]). Both types work by exploiting the fundamental randomness of certain quantum processes, but with trusted devices, it is more straightforward to do so. We briefly mention one example here. A simple trusted-device QRNG can be based on a 50:50 beamsplitter and two detectors, one for the reflected arm and the other for the transmitted arm. If a single photon is incident on the beamsplitter, then with probability half it will go to one detector and with probability half the other. In principle this is a source of quantum random numbers.

However, building such a QRNG is not as straightforward as it sounds. Generation and detection of single photons is challenging, and it is difficult to ensure that the beamsplitter is perfect. Furthermore, correlations may be brought into the string by other factors such as fluctuations in the power supply, asymmetries in the detector responses and dead times. The standard way to account for such difficulties is to try to quantify these effects, estimate the min-entropy of the outputs and then use a classical extractor to compress the imperfect raw string into arbitrarily good randomness.

One issue that needs to be considered when doing this is that extraction of randomness typically requires a seed, i.e., an independent random string. Fortunately, this seed can act catalytically if a strong extractor is used, i.e., the seed randomness remains random and virtually independent of the output randomness so is not consumed in the process. Nevertheless, the need for this seed means that QRNG protocols should more accurately

be described as *quantum randomness expansion* (QRE) protocols. In order to have a good rate of expansion, randomness extractors requiring a short seed should be used. Note also that to have full security guarantees, *quantum-proof* randomness extractors should be used.

For the type of QRNG mentioned above the security relies on the accuracy of the model used to describe it. Like in the case of QKD, various additional advantages can be gained by moving to device-independent protocols (see Section IV A). These shift reliance away from the model: that the output string is random is checked on-the-fly and relies on the correctness and completeness of physical laws (note that correctness and completeness of quantum theory are related [860, 861]). The idea has been described earlier in the review where DI-QKD was introduced (see Section IV B). In essence, if we have some number of separate systems whose correlations violate a Bell inequality, then their outcomes must contain some min-entropy, even conditioning on an adversary holding arbitrary side information (for instance a quantum system entangled with those being measured). This min-entropy can be lower bounded and an extractor applied leading to arbitrarily good randomness output.

To use this idea, some initial randomness is required, so we need to ensure that the protocol outputs more randomness than it requires giving genuine expansion. This can be achieved using a protocol analogous to the spot-checking CHSH QKD protocol from Section IV D 2.

B. Protocols for DI-QRE

1. The setup for DI-QRE

The setup is different from that for DI-QKD because there is only one honest party (Alice) in this protocol, and, because the protocol is for randomness expansion, we do not give an unlimited supply of random numbers to Alice. These are the assumptions:

1. Alice has a secure laboratory and control over all channels connecting her laboratory with the outside world. For any devices in her labs, Alice can prevent unwanted information flow between it and any other devices.

2. Alice has a reliable way to perform classical information processing.

3. Alice has an initial seed of perfectly random (and private) bits, known only to her.

Like for DI-QKD, security is proven in a composable way (cf. Section II D) allowing the protocol's output to be used in an arbitrary application. The remarks made in the last paragraph of Section IV D 1 all apply to QRE as well. However, mitigating the device-reuse problem is easier for QRE than in QKD because QRE does not involve public communication during the protocol [220].

2. The spot-checking CHSH QRE protocol

There are many possible types of protocol; we will describe a specific protocol here, based on the CHSH game with spot-checking. The protocol has parameters $\alpha \in (0,1)$, $n \in \mathbb{N}$, $\beta \in (2, 2\sqrt{2}]$, $\delta \in (0, 2(\sqrt{2}-1))$, which are to be chosen by the users before it commences.

1. Alice uses her initial random string to generate an n-bit string of random bits T_i, where $T_i = 0$ with probability $1-\alpha$ and $T_i = 1$ with probability α.

2. Alice uses a preparation device to generate an entangled pair. She sends one half to one measurement device and the other half to another such device. (As in the case of DI-QKD, although this step refers to the generation of an entangled state, security does not rely on this taking place correctly.)

3. If $T_i = 0$ (corresponding to no test) then Alice makes fixed inputs into each measurement device, $A_i = 0$ and $B_i = 0$ and records the outcomes, X_i and Y_i. These inputs are made at spacelike separation and each device only learns its own input.
   If $T_i = 1$ (corresponding to a test) then Alice uses her initial random string to independently pick uniformly random inputs $A_i \in \{0,1\}$ and $B_i \in \{0,1\}$ to her devices and records the outcomes, X_i and Y_i.

4. Steps 2 and 3 are repeated n times, increasing i each time.

5. For all the rounds with $T_i = 1$, Alice computes the average CHSH value (assigning $+1$ if $A.B = X \oplus Y$ and -1 otherwise). If this value is below $\beta - \delta$, she aborts the protocol.

6. If the protocol does not abort, for the rounds with $T_i = 0$ the outputs X_i are fed into a randomness extractor whose seed is chosen using Alice's initial random string. The EAT can be used to compute how much randomness can be extracted, depending on the value of β.

The ideal implementation of this protocol is as for the CHSH QKD protocol in Section IV D 2 (except that $B_i = 2$ is not needed) and the intuition for its operation is the same. The completeness error is again exponentially small in n. By taking n sufficiently large, this protocol can output at a rate arbitrarily close to $H(X|E)$ from (89) (see Section IV C). This rate is the amount of randomness output per entangled pair shared. We make a few remarks about the protocol.

1. The protocol aims for randomness expansion, so it is important to use as little randomness as possible to implement it. Since each test round consumes two bits of randomness, we would like α to be chosen to be small. This also helps reduce the amount of randomness required to choose the test rounds,

since generating a string of n bits with bias α requires roughly $nH_2(\alpha)$ bits of uniform randomness from Alice's initial random string, where H_2 is the binary entropy which drops away steeply for small α. The value of α can be chosen such that in the large n limit, the randomness required to choose it is negligible.

2. If a strong extractor is used in the last step then randomness is not consumed for this. Nevertheless, it is helpful to use an extractor with a small seed, e.g., Trevisan's extractor, so as to reduce the randomness required to initiate the expansion.

3. In the case of the CHSH QKD protocol the aim is to generate an identical key shared by Alice and Bob. Here the aim is to generate randomness, so there is no need for the ideal implementation to lead to the same outcomes for both devices in the case of no test. This allows randomness expansion rates that go beyond that of the QRE protocol given above, while still using maximally entangled qubit pairs (see [217] for a robust protocol giving up to two bits of randomness per entangled pair). Like in the case of DI-QKD, finding tight bounds on the min-entropy in terms of the observed correlations for general protocols is an open problem.

4. As the number of rounds, n, increases the classical computation required by the protocol (e.g., to perform the randomness extraction) may become prohibitively slow.

C. Historical remarks and further reading

The use of non-local correlations for expanding randomness without trusting the devices used goes back to Ref. [862] and the ideas there were developed in Ref. [863]. The idea was developed experimentally in Ref. [864] and security proofs against classical adversaries were presented in Refs. [865, 866]. The first work covering quantum adversaries was Ref. [867], although this lacked tolerance to noise. Quantum security with error tolerance was proven in Ref. [225] and improved in Ref. [868], where it was shown that any Bell violation can be used to generate randomness.

Most recently, using the EAT [213] the expansion rate was improved [212] so as to be asymptotically optimal and a recent experiment has been performed based on these recent techniques [869].

Note that several review articles devoted to the topic of (quantum) random number generation have appeared in the last few years [870–872]. These go beyond the scope of the present review and provide a useful resource for further reading on the topic.

D. Implementations

DI-QRE suffers from some of the same drawbacks as DI-QKD, the most significant being the difficulty of performing a Bell experiment while closing the detection loophole. For DI-QRE this is slightly easier to do because there is no need for the two measurement devices to be distant from one another. Instead, they only need to be far enough apart to enable sufficiently shielding to ensure they cannot communicate during the protocol. (In particular, each device should make its output independently of the input of the other device on each round of the protocol.) Nevertheless, it remains challenging to do this. While the first DI-QRE experiment ran at a very low rate [864], recent state-of-the-art experiments achieve reasonable rates [869] and even close the locality loophole as well as the detection loophole. Such a demonstration could be turned into a future randomness beacon, but is still far from being built reliably into a small scale device that could reasonably be included in a desktop computer or mobile phone.

One possible way to implementation is to use RNGs that rely on a detailed model of how the device operates (see, e.g., Ref. [873]). To ensure such RNGs work as intended, it will be important to make increasingly sophisticated models of them and to diagnose and patch any weaknesses as and when they are identified. Furthermore, the performance of a RNG may change with time and if and when it degrades, it is important that this is noticed before the purportedly random outputs are used. A problem such as this can be mitigated by combining the outputs of several random number generators (in an appropriate way) to give the random string to be used.

E. Randomness amplification

As we saw in the last section, in order to generate randomness in a device-independent way we require some seed randomness to start the process. This is necessary: to constrain a device based only on its input-output behavior we use the violation of a Bell inequality, and random numbers are needed to choose the inputs when verifying such a violation.

However, while random numbers are required for this task, the protocol given above assumes these are perfectly random. The task of randomness amplification concerns whether a source of imperfect randomness can be used to generate perfect randomness. (This should not be confused with the related task of randomness extraction, where an additional perfect seed is available.) Like randomness expansion, this task is impossible classically in the following sense: given a particular type of imperfect source of randomness, a Santha-Vazirani source [874], and no other source of randomness, there is no classical protocol can generate perfectly random bits [874].

A Santha-Vazirani source is a way of modeling a source of bad randomness. It has the property that each bit

given out can be biased towards either 0 or 1 within some limits which are specified by a parameter $\varepsilon \in [0, 1/2]$. More precisely, call the outputs S_i, and let W_i be a random variable representing arbitrary additional information available that could not be caused by S_i. The sequence of bits S_i in a Santha-Vazirani source with parameter ε if

$$\left| P_{S_i|S_{i-1}=s_{i-1},\ldots,S_1=s_1,W_i=w}(0) - \frac{1}{2} \right| \leq \varepsilon \ \forall s_{i-1}, \ldots, s_1, w \,. \tag{250}$$

In other words, even given the entire prior sequence and any other information that could not be caused by S_i, the probability of 0 and 1 each lie between $1/2 - \varepsilon$ and $1/2 + \varepsilon$.

It turns out that such a source of randomness can be amplified with a quantum protocol. The first proof of this appeared in Ref. [875] where the task was introduced. There it was shown that for $\varepsilon \leq 0.058$ a single source of ε-free bits can be used to generate bits that are arbitrarily close to uniform. Subsequently it was shown that this bound on ε could be extended to cover all $\varepsilon < 1/2$, i.e., any source of partially random bits can be amplified, no matter how small the randomness [876]. These initial protocols gave important proofs of principle, but were impractical due to low noise tolerance or the need for large numbers of devices, a problem addressed in [877]. The current state of the art can be found in [878], which includes a protocol with two devices that tolerates noise and works for all $\varepsilon < 1/2$.

Further works considered other types of imperfect randomness, in particular, min-entropy sources which take as input a single string with an assumed lower bound on its min-entropy conditioned on arbitrary side information, and no further assumptions about the structure of the randomness. A security proof in this scenario is given in [879].

It is worth noting that while all of the above works prove security of randomness amplification against quantum adversaries, several also show security against a post-quantum adversary whose power is only limited by the impossibility of signalling. Protocols that work against arbitrary no-signalling adversaries tend to lack efficiency. One reason for this is the difficulty of extracting randomness against a no-signalling adversary [880, 881].

Another noteworthy property of many of the above protocols (all except the protocol of [877]) is that they can work using a public source of randomness as a seed. This is relevant in the context of randomness beacons. If a user suspects that the output of the beacon is imperfect in some specified way, they may be able to use a randomness amplification protocol to increase their trust in the output randomness.

XV. QUANTUM DIGITAL SIGNATURES

A. Introduction

Digital signature is a cryptographic primitive that ensures that a digital message was (i) created by the claimed sender (authenticity), (ii) that the message was not altered (integrity) and (iii) that the sender cannot deny having sent this message (non-repudiation). It is the digital analogue of handwritten signatures but comes with a higher level of security guaranteed by cryptographic means. Digital signatures play a very different role than encryption in modern communications, but this role is of no less importance. Ronald Rivest, one of the inventors of public-key cryptography, stated in 1990 that "the notion of digital signature may prove to be one of the most fundamental and useful inventions of modern cryptography". This prediction has been fulfilled, since nowadays it is a necessary tool for a huge range of applications, from software distribution, financial transactions, emails to cryptocurrencies and e-voting.

Here we review the research on quantum digital signatures (QDS) that demonstrate how using simple quantum communications we can achieve digital signature schemes that are more secure than most of the commonly used digital signatures algorithms. We start in Section XV B with definitions and security properties of digital signatures and motivate the use of quantum means in Sections XV C and XV D. We present the seminal Gottesman-Chuang scheme, and identify the practical limitations it has in Section XV E. In Section XV F we describe how one-by-one these restrictions were lifted, making QDS a currently realizable quantum technology. In Section XV G we describe a generic practical QDS protocol. A reader interested in quickly catching-up with the current state-of-the-art for QDS, could read this section directly after the introduction. In Section XV H we give theoretical and in Section XV I experimental recent developments. Finally, in Section XV J we give a (fully classical) alternative to QDS that requires point-to-point secret keys (potentially obtained via QKD) and then we conclude in Section XV K.

B. Definitions and security properties

A QDS scheme involves multiple parties: one sender and (potentially many) receivers. It consists of three phases each described by a corresponding algorithm $Gen, Sign, Ver$.

(Gen) Key generation algorithm. This sets and distributes the "keys" to be used in the subsequent interactions. (It is also known as the "distribution phase".) A private key (sk) that is given to the sender, and (possible multiple) public key(s) (pk) given to the receivers are selected. In protocols where the public key of different receivers is not

the same, a subscript will indicate which receiver refers to e.g. pk_i.

($Sign$) Signing algorithm. The sender chooses a message m and uses her private key sk to generate a signature $\sigma = Sign(m)$ and then send the pair $(m, Sign(m))$ to the desired receiver.

(Ver) Verifying algorithm. A receiver has as input a message-signature pair (m, σ) and the public key pk and checks whether to accept the message as originating from the claimed sender or not. In certain types of signatures (including the QDS), there are multiple levels of "accepting" a message, depending on what confidence the receiver has that this message would also be accepted if forwarded to other receivers.

An important property of digital signatures schemes is that after the Gen phase, the actions of the parties are determined without further (classical or quantum) communication, i.e. they sign and decide to accept or reject a message-signature pair, based solely on the keys sk and pk respectively, that were distributed during the Gen phase. This is precisely how hand-written signatures are used, where one signs and accepts/reject a signature "locally". Let us define the correctness and security notions for a digital signature scheme:

- A digital signature scheme is correct if a message-signature pair signed with $Sign$ algorithm using the correct private key sk is accepted by the Ver algorithm with unit probability.
- A digital signature scheme is secure if no adversary without access to the private key sk can generate a signature that is accepted by the Ver algorithm with non-negligible probability.

These definitions, along with the guarantee that the private key sk is not leaked and that all parties share the same (correct) public key pk, lead to three important properties: unforgeability, non-repudiation and transferability. We will see that ensuring parties received the same and correct public key becomes a non-trivial task when the keys are quantum. Instead of using the above security definitions, for analyzing QDS schemes, we will instead aim to ensure that the following three properties are satisfied:

1. Unforgeability: A dishonest party cannot send a message pretending to be someone else.
2. Non-repudiation: A sender cannot deny that she signed a message.
3. Transferability: If a receiver accepts a signature, he should be confident that any other receiver (or judge) would also accept the signature.

Firstly, we need to clarify how the words "cannot" and "confident" are used. The meaning is that, for any adversary allowed (which, depending on the setting, may or may not have restrictions in his computational power), the probability of the protocol failing can be made arbitrarily small with suitable choices of parameters. The exact magnitude of how small is determined by the level of security requested by the use of the given scheme, and is characterized by a small positive number ϵ. In other words, formally we should write ϵ-unforgeability, etc. Secondly, we note that non-repudiation and transferability are very closely related. Not being able to deny a signature typically depends on the way one resolves a dispute, i.e., if Alice refuses that she signed a contract, who will decide whether the contract had her signature or not. In most cases this is the same as asking if a signature accepted by one receiver would also be accepted by a judge or other receivers, and this is exactly the transferability property. Here we will identify non-repudiation with transferability, while keeping in mind that this may not be the most general treatment, if one chooses a different (less natural) "dispute-resolution" mechanism.

For simplicity, in the following we will refer to the sender as Alice, the received as Bob and when a second receiver is required (e.g. for transferability of messages), he will be referred to as Charlie.

C. What is a *quantum* digital signature scheme and why it is useful?

There are various things that one could call QDS, but in this review we present the research that started with Gottesman's and Chuang's seminal work [882] and deals with: signing a classical message and using quantum communication (and computation) in order to provide information-theoretic security (ITS), so that the signatures generated are "one-time" in the sense that when a message is signed the corresponding private/public keys cannot be reused for signing other messages. Other uses of the term include: signing a *quantum* message, "blind" quantum signatures, arbitrated quantum signatures, classical signatures secure against quantum computers [883], quantum tokens for signatures [884], etc.

The most common digital signature schemes are RSA-based, the digital signature algorithm (DSA), the elliptic curve DSA, and ElGamal. The security of all these schemes is based on the assumption that the adversaries have limited computational power and that, in particular, it is hard for them to solve the discrete logarithm or factoring problems. While these problems are still believed to be hard for classical computers, since Shor's algorithm [885] we know that an efficient quantum algorithm exists. In other words, if a large quantum computer is built, then it could solve these problems efficiently and break the security of all these signature schemes. This provides a compelling argument in favor of solutions that provide ITS, which is the strongest type of security, hold-

ing irrespectively of the computational resources that an adversary has.

Here it is important to stress that while the most commonly used classical digital signatures schemes (mentioned above) would break, this is not the case for all classical digital signature schemes. There exist many (less practical) classical signature schemes, that appear to remain secure against quantum computers (post-quantum secure), possibly after small modifications in the security parameters (e.g. by doubling the key-lengths). Examples of such schemes are the Lamport [886], Merkle [887], Ring-Learning-With-Errors [888], CFS [889], etc.

Having said that, there is another strong argument for ITS (and thus QDS). The research in quantum algorithms is not as mature as in classical algorithms, therefore the confidence we have on the hardness of problems still changes. For example, in a recent result [890] one of the best candidates for post-quantum cryptography, the learning-with-errors (LWE) problem, was proven to be equivalent to the dihedral-coset problem, for which there is a sub-exponential quantum algorithm. While this algorithm still would not fully break the security of LWE, it certainly weakens its security and one may wonder whether we should base the security of our communications on such computational assumptions.

D. The Lamport one-time signature scheme

QDS schemes were inspired by Lamport's one-time signatures [886] and for this reason we present here a high-level description of this scheme. Assume that we have a (classical) one-way function f. For such a function, it is simple to evaluate $f(x)$ given x. However, given $f(x) = y$ it is hard to find the pre-image, i.e. invert the function to get the value x. Of course, we can already see that this definition (hardness of inverting) assumes (i) limited computational resources (otherwise one could "brute-force" by trying all x's until he finds the pre-image or a collision) and (ii) the function is such that it is not efficiently invertible. In other words any scheme based solely on the above cannot offer ITS.

Alice chooses two random inputs x_0, x_1 and evaluates $f(x_0), f(x_1)$. She then publicly broadcasts the pairs $(0, f(x_0))$ and $(1, f(x_1))$ which will be the public keys pk, while she keeps the values x_0, x_1 secretly stored (private key sk). This completes the Gen algorithm. Then to $Sign$, Alice simply sends the message b along with her stored corresponding secret key x_b. The receivers, to accept/reject (Ver algorithm) they evaluate $f(x_b)$ and check if it agrees with their public key in order to accept.

The intuition why this is secure comes from the fact that the function is hard to invert. Therefore an adversary with access only to the public keys (images) cannot find the secret key (pre-image) for any message, in order to provide a valid (forged) signature. At the same time, if anyone receives a valid signature (with respect to the publicly available public key), they are convinced that it came from Alice (non-repudiation), even if she claims it does not, because nobody else could have generated such signature.

Finally, at the end of such scheme, all used and unused keys are discarded (thus one-time signatures). Such protocol has been modified using Merkle trees [887] to allow the signing multiple messages.

E. The Gottesman-Chuang QDS

In 2001, Gottesman and Chuang [882] proposed the first QDS protocol, that we may briefly call GC-QDS. The central idea was to use the fact that non-orthogonal states cannot be distinguished perfectly so as to realize a "quantum one-way function", where the inability to invert is not based on computational assumptions but guaranteed by the laws of quantum mechanics. The basic idea is that if we have a quantum state $|f(x)\rangle$, where $f(x)$ represents the classical description of the state, and the set of possible states are non-orthogonal, no-one should be able to determine the classical description of the state, with high probability, unless they already know it (otherwise they could also copy/clone the state). Moreover, the amount of information obtained is bounded by the Holevo theorem [83]. In other words, we have the classical description of the state to play the role of the secret key sk, while the quantum state itself is the public key $|pk\rangle$. Such "one-way function", by construction, cannot be broken even if one has unlimited computational power.

1. *The protocol*

A function f is chosen and is made public. This function takes input x and returns $f(x)$ that is the classical description of a quantum state. For example, x can be a two-bit string and $f(x)$ denotes one of the four BB84 states. There is no need for this function to be one-way, since what replaces the one-wayness of classical protocols is that one cannot obtain the classical description of a quantum state with certainty. In GC-QDS some choices of functions were made, but this is not crucial for the general description. Let us analyze the various steps.

a. Key generation. For the private key, Alice chooses pairs of bit-string $\{x_0^i, x_1^i\}$, where $1 \leq i \leq L$. The x_0's will be used to sign the message 0 and the x_1's to sign the message 1. The number of pairs L is determined by the security level requested.

For the public key Alice generates multiple copies of the state $\{|f(x_0^i)\rangle, |f(x_1^i)\rangle\}$. Since only Alice knows the secret keys, and unknown quantum states cannot be copied, she generates all the copies. Then she distributes to each potential receiver the corresponding states, along with the label for which message they correspond.

In a digital signature scheme, *all* parties may be dishonest (not simultaneously though). When the public key is classical, parties could easily check that they have

the same public keys. This is far from trivial in our case. Gottesman and Chuang proposed to use multiple copies (of each public key for each party) and they interact by performing SWAP tests (see Fig. 19). This is a test that gives always affirmative answer without disturbing the state, when two states are identical, while fails probabilistically otherwise. This comes with considerable cost, since each copy of the public key (quantum state) circulated makes easier the task for an adversary to recover the classical description (secret key) and therefore to forge a message. Finally, all receivers store the public key into a quantum memory until they receive a signed message.

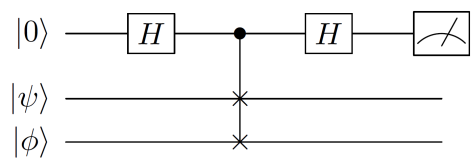

FIG. 19. The SWAP test. If $|\psi\rangle = |\phi\rangle$ then it gives always 0, otherwise the result 1 is obtained with probability that depends on the overlap $|\langle\psi|\phi\rangle|$.

b. Signing. To sign a message, Alice simply chooses the message value $b \in \{0,1\}$ and sends (b, x_b^i) to the desired receiver. This is a completely classical phase.

c. Verification. In order to confirm whether the message-signature pair is valid, the receiver uses the classical description: for each x_b^i he generates the corresponding quantum state $|f(x_b^i)\rangle$ and checks if it is consistent with his stored public key. Then he counts the fraction of incorrect keys s_t (out of the L keys). At this point QDS deviates from standard digital signature schemes. The verification algorithm takes three answers (rather than the usual two accept/reject). The receiver can return REJ when convinced that the message-signature pair is not valid, can return 0-ACC if he is certain that is valid but is uncertain if this signature would also be accepted by other receivers when forwarded (or by a judge), and return 1-ACC if he is certain that is valid and will also be accepted by other receivers or judges. The reason for this modification is subtle and is explained below in the section on the intuition of the security. Depending on the details of the protocol, there are two parameters $0 < s_a < s_v < 1$ that determine what Ver outputs. If $s_t > s_v$ the receiver REJ. If $s_v > s_t > s_a$ the receiver 0-ACC and if $s_t < s_a$ the receiver 1-ACC.

2. Security intuition

Unforgeability is guaranteed by the fact that, given an unknown quantum state, one cannot guess its classical description with certainty, even if the state is from within a known (non-orthogonal) set. A potential forger has in his disposal all the copies of the quantum public keys, and, if colluding with other receiver, may even have extra copies. We assume that the forger performs a minimum-error (or minimum-cost in general) quantum measurement to obtain his best guess, with an associated probability p_f of failure. Provided that this probability is higher than an accepting threshold $p_f > s_v$, a forger cannot mimic a valid signature, at least not with probability higher than a decreasing exponential $e^{-c(p_f - s_v)^2 L}$ for some constant c. This argument is similar in all QDS protocols, where calculating p_f and c varies on the details (number of copies circulated, form of the quantum states sent, method to measure/identify errors in the key, etc).

To prove non-repudiation is even more subtle. Alice is not forced to send identical quantum public keys to Bob and Charlie. As outlined above, they communicate quantumly and perform a number of SWAP tests on copies of the public keys. The result of these tests succeeds probabilistically. If there was a single verification threshold s_v, then Alice could tune the public key she sends to Bob and Charlie to have (expected) $s_v L$ errors. Since the number of errors is determined by a normal probability distribution with mean at $s_v L$, the probability that one of them finds more than $s_v L$ errors is exactly 1/2. This means that with probability 1/4 one of them will practically detect more than $s_v L$ errors while the other less than $s_v L$ errors, and therefore they would disagree on whether this signature is valid or not.

This is why Gottesman and Chuang introduced a second threshold s_a and used both s_a and s_v. Now to repudiate, Alice needs to generate a signature that the first receiver accepts as message that can be forwarded while the second receiver completely rejects. In other words we need the errors of Bob to be below $s_a L$ while those of Charlie to be above $s_v L$. We can see that, similarly with the forging case, this probability decays exponentially if $s_a < s_v$ with a rate $e^{-c'(s_a - s_v)^2 L}$.

Finally, in any realistic setting, even an honest run would result to certain errors due to the noise and imperfections in the quantum communication and quantum memory. This could lead to honest signatures being rejected, which again is undesirable. (This is known as correctness, soundness or robustness in different places in the literature.) We denote the fraction of those honest errors as p_e and once again we see that the protocol does not reject honest signatures if $p_e < s_a$, so that the probability of honest rejection decays as $e^{-c''(p_e - s_a)^2 L}$.

To summarize, we have $0 < p_e < s_a < s_v < p_f$. The parameter p_e is determined by the system, noise, losses, etc, while p_f is theoretically computed as the best guess/attack. The two parameters s_a, s_v should be suitably chosen within the gap $g = p_f - p_e$, and approximately in equal distances so that we have minimum probability that something undesirable (forging, repudiation, honest-reject) happens.

3. Remarks

Let us note that exact calculation of the above parameters for GC-QDS was not done since there were many

practical limitations to actually implement such protocol. It served more as an inspiration for later works.

Then note that this protocol involves multiple parties (at least when considering transferability/non-repudiation) and any one of them could be malicious. This is one of the most crucial differences compared to QKD. The adversaries in QDS are legitimate parties in the (honest) protocol (while Eve in QKD is an external party). This means that even when we are guaranteed that all quantum communications are done as the sender wishes, there are still potential attacks. It is exactly this type of attacks that we have so-far considered. Receivers using their legitimate quantum public key to make a guess of the private key and forge; or a sender sending different quantum public key to each receiver in order to repudiate.

In [882] and in the first few works on QDS, to simplify the security analysis, it was assumed that these are essentially the only possible attacks. This formally was described as having an authenticated quantum channel between the parties. However, to actually have such a channel (or to have quantum-message-authentication-codes [891]), there is a considerable cost. Subsequent works lifted this assumption.

Finally, while we have described QDS as a public-key cryptosystem, strictly speaking this is not quite precise. The "public key" is a quantum state, thus it cannot be copied or broadcasted as classical keys. Therefore to properly ensure that the public key is the same, point-to-point (quantum) communication is required, while parties that have not participated in the *Gen* phase, cannot enter later (i.e., it lacks the "universal verifiability" of classical public key cryptosystems). Whether these issues are crucial or not, it depends on the use/application that the digital signatures are required (e.g., how important is the security) and the efficiency of the QDS protocol after having taken into account the above issues.

4. *Practical limitations of GC-QDS*

The GC-QDS scheme highlighted the possibility of a beyond-QKD quantum cryptographic primitive, but it did not trigger a wide research burst immediately. The reason that it took more than 10 years to have the wider research community following these steps was, mainly, because the original protocol was highly impractical to be actually implemented and used. The three major practical restrictions were:

1. The quantum public key is a quantum state received during the *Gen* phase and then later used again during the *Ver* phase. However, in normal practise, the acts of establishing the possibility of digital signatures and actually signing and even later verifying (or forwarding) a signature can be separated by long periods of time (days or even months). Storing quantum information for even seconds is hard and is one of the major restrictions in building scalable quantum computers.

2. In order to test that receivers obtained the same quantum public key, they need to communicate and have multiple copies of the key, then test whether they are the same using a comparing mechanism such as the SWAP test, send copies to other parties and re-use the SWAP test between their public key and the one received from other parties. This involves extra quantum communication and, more importantly, using ancillae and controlled SWAP gates on each qubit. These operations are operations sufficient for a universal quantum computation and adding the quantum memory requirement, it appears that all parties should have a full universal quantum computer to participate in GC-QDS. This is in sharp contrast with QKD, that requires minimal quantum technologies, for example preparing and measuring single qubits.

3. In the analysis of GC-QDS we have assumed that the quantum states that parties want to send, arrive to the desired party correctly, i.e., they have an authenticated quantum channel. While quantum-message-authentication-codes do exist [891], they bring extra cost. Alternatively, one could modify a QDS protocol to be secure even when there is no guarantee about the quantum channel(s) used.

F. Practical QDS: Lifting the limitations

Since the appearance of the GC-QDS protocol there were four major developments, which we outline here. These lifted all the aforementioned limitations transforming QDS from a theoretical idea to a practical quantum communication primitive, technologically as mature as QKD. Further improvements (in the security proofs/guarantees, performance and realizations) will be summarized in the subsequent sections.

1. *Simplifying state comparison*

Andersson et al. [892] introduced a practical quantum comparison for coherent states (here expressed in the photon number basis)

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \tag{251}$$

Provided that the quantum public key of a QDS protocol consists of coherent states, this practical test can replace the SWAP-test in both its uses. First to ensure that the quantum public keys are identical and thus Alice is not attempting to repudiate. Second, to check the validity of a signature by checking that a quantum public

key matches its classical description (given when a signed message is received).

In Ref. [892], the quantum public key consists of two states ($b = 0$ for signing message 0 and $b = 1$ for message 1) whose form $|\psi^b_{pk}\rangle$ corresponds to a string of coherent states $||\alpha|e^{i\theta}\rangle$ with the same (known) amplitude $|\alpha|$ and phase chosen randomly from the angles $\theta \in \{2\pi\frac{1}{N}, 2\pi\frac{2}{N}, \ldots, 2\pi\frac{N-1}{N}\}$, for suitable N. The classical description of this string (the choice of phase for each coherent state in the string) is the private key sk.

The main idea of the coherent-state quantum comparison is depicted in Fig. 20, where we can see that the "null-ports" measure the phase difference between the two incoming coherent states (and is the vacuum when they are identical). Note, that this comparison is very simple technologically, since all that is needed is beam splitters, mirrors and photon detectors. This is why this set-up is a considerable advancement compared to the SWAP-test used in GC-QDS.

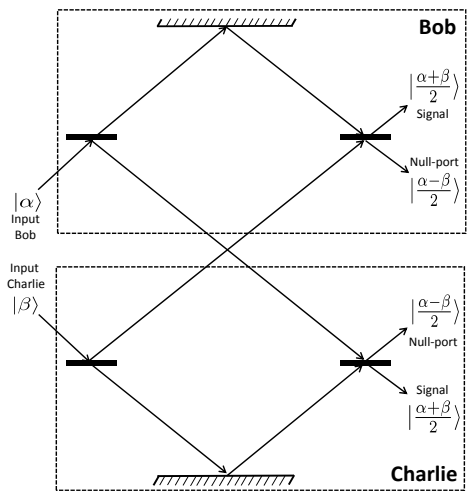

FIG. 20. Coherent-state quantum comparison introduced in Ref. [892]. If $|\alpha\rangle = |\beta\rangle$ then only the signal port of Bob and Charlie detects photons. Otherwise, the null-port detects photons too. Adapted with permission from Ref. [893] ©APS (2014).

Since this comparison should be performed for the quantum public keys that receivers (Bob and Charlie) have, the multiport of Fig. 20 is placed between different locations (Bob's and Charlie's labs). This has two consequences, one practical and one theoretical. The practical is that being in a distance, ensuring path lengths are identical is not trivial, while extra losses occur, since not only the quantum public key needs to go from Alice to Bob/Charlie, but then it needs to go through this comparison process. The theoretical issue is that Alice, in principle, could also tamper the quantum states communicated between Bob and Charlie, something that complicates the (full) security proof. Such proof was only completed for some modified protocols much later.

To sign a message Alice sends the corresponding message b along with the string of phases corresponding to ψ^b_{pk}. Bob (Charlie) to accept, reconstruct the state $|\psi^b_{pk}\rangle$ and use state-comparison with their stored state. They count the number of positions in the string that the null-port clicks and compare the fraction with the thresholds (s_a, s_v) and decide to accept as original (1-ACC), as forwarded (0-ACC) or to reject the message.

2. *No quantum memory requirement*

As we have already stressed, in GC-QDS the public key is a quantum state and one needs to store it until the Ver phase, something that makes impractical such scheme. Dunjko et al. [893] constructed a QDS protocol that does not require a quantum memory. The central idea is to replace the quantum public key (which needs to be stored coherently) with a classical "verification key", which is no longer the same for all receivers.

The protocol builds on Refs. [892, 894] and starts with Alice distributing a "quantum public key" being two strings of coherent states, where for simplicity, the possible phases of each state are two, i.e., the strings are of the type $|\alpha\rangle|-\alpha\rangle|\alpha\rangle\cdots|-\alpha\rangle$ (if Alice is honest). Bob and Charlie use the multiport scheme of Fig. 20 to ensure that Alice was (mostly) honest. Then they directly measure each coherent state pulse, using unambiguous state discrimination (USD) [895–897]. With this measurement, Bob and Charlie know with certainty the classical description of some positions in the string(s) of coherent states that Alice sent, while they have no information about other positions.

This information (position in string and value measured) are stored by Bob and Charlie and will be their verification key. (Note that the verification key of Bob and Charlie is different, even in the honest case. This is because for which positions a USD gives conclusive outcome is probabilistic and happens independently for the copy that Bob and Charlie have.) When Alice sends a signature, she needs to return the classical description for *all* the string corresponding to the message b she wants to sign. Bob and Charlie count the fraction of mismatches that the string that Alice has with their stored verification key(s) s_t and they reject, 0-ACC or 1-ACC comparing these mismatches with the thresholds s_v an s_a.

The important detail that makes such scheme secure, is that Alice does *not* know for which positions Bob and Charlie know the state and for which they do not. It is therefore impossible for her to send a classical description that agrees with all the possible verification keys unless she sends the honest private key.

Note that, to achieve ITS encryption, one uses quantum communication (QKD) to achieve a shared secret key and then uses the fully classical one-time-pad protocol to encrypt a message. Similarly, here, we use quantum communication to achieve correlations between the classical information of the parties involved in the signature scheme (their private/verification keys). Then after

establishing these correlations, a fully classical signing and verifying algorithm follows and achieves the digital signature functionality.

3. QDS from QKD technology

After removing the quantum memory requirement, the only remaining difficulty making QDS harder than QKD is the mechanism to ensure that the same quantum public key was sent to different receivers (ensuring non-repudiation), whether this mechanism is the SWAP-test or the much simpler coherent-state comparison (using a spatially separated multiport).

A crucial observation is that both the SWAP-test and the coherent-state comparison accept symmetric states. In other words, if the states compared are in the global state $\frac{1}{\sqrt{2}}(|\psi\rangle|\phi\rangle+|\phi\rangle|\psi\rangle)$, both tests would always accept. While this may appear as a problem, it turns out that Alice is unable to repudiate by sending such symmetric states. In fact, since the state is symmetric, Alice is unable to make Bob accept (with the lower error threshold s_a) and in the same time make Charlie rejects (with the higher error threshold s_v used for forwarded messages). It is the symmetry of the state and the gap $g = (s_v - s_a)$ that ensures non-repudiation.

Starting from this observation, Wallden et al. [898] replaced the comparison test with a "symmetrizing" step and proposed three protocols. This extra step ensures that, even if Alice did not distribute identical quantum public keys, the classical verification keys that Bob and Charlie store will be symmetric and thus Alice is unable to make them disagree. All protocols given in [898] can be performed with BB84 states. Here we outline one of these protocols to demonstrate these ideas.

Alice selects two strings of BB84 states (one for each future message b), and she generates two copies of these strings and send them to Bob and Charlie. For each qubit, Bob (Charlie) either forwards it to Charlie (Bob) or keeps it and measures it in either $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ basis. Similarly, he measures the forwarded qubit that he received from Charlie (Bob). Depending on the result, he rules-out one of the possible states. For example if for the nth qubit he obtains the outcome "+", Bob stores that the nth qubit is *not* $|-\rangle$ (something he can know with certainty). Bob (Charlie) stores the sequence of eliminated states, the position in the string, and whether he received it directly from Alice or as forwarded from Charlie (Bob). This classical information will be Bob's (Charlie's) verification key.

As usual, Alice to sign sends the message and the classical description of the corresponding string of qubits. Bob checks for positions that the declaration of Alice contradicts his stored verification key (i.e. places that Alice sends the state that Bob has ruled-out). Then the fraction of this mismatches is compared to the two thresholds s_a, s_v and Bob rejects or 0-ACC or 1-ACC.

4. Insecure quantum channels

One major assumption made so far was that the quantum channels used were authenticated, i.e., the quantum states sent during the quantum communication part of the protocol were the same as the one received. While there are general (costly) methods to achieve this, an intuition why this may not be necessary was already given. One can imagine "sacrificing" part of the communicated qubits to test (and bound) the tampering that third parties performed. This is exactly what parameter estimation in QKD achieves. In Refs. [899, 900] the authors made this intuition precise. As part of the interaction that leads to a private key for Alice and (partial information) for Bob (Charlie), they included a parameter estimation phase. As far as the experiment is concerned, it is now a normal QKD protocol, that stops before EC and PA. The way to bound forging and repudiation is very different and depends on the specific protocol.

In Ref. [899] there was another change. The quantum states (quantum public key) that Alice sends to Bob and Charlie were no longer the same. Since the only condition that secures Bob and Charlie against repudiation is the symmetrization procedure, whether Alice sends initially the same or different states makes no essential difference. The only practical difference is that Alice's private key is now composed from the classical description of both the different strings sent to Bob and Charlie. On the other hand, by sending different quantum states, Alice limits the potential forging attacks, since forgers have no longer copies of the full legitimate quantum public key.

Finally, a very interesting observation is that the (channel) error rates for which QDS was possible in [899] were higher than those for QKD. This means that by using this QDS scheme, one may be able to perform QDS in a setting where QKD is not experimentally feasible.

G. A generic modern QDS protocol

1. Description

We can now give a description of a generic modern QDS protocol, i.e., one that does not require quantum memory, that can be realized with the same technology as QKD and that makes no assumption on the quantum channels used. The description below is restricted to three parties, but can be generalized to more parties.

a. Key generation. We start with (any) QKD system as basis. Alice performs the first part of a QKD protocol (separately) twice with Bob and twice with Charlie. The QKD protocol is completed up to obtaining the raw key (i.e., before EC and PA). As a result, Alice has four bit strings $A_0^B, A_1^B, A_0^C, A_1^C$, Bob has two strings K_0^B, K_1^B and Charlie has K_0^C, K_1^C. By the properties of a (non-aborted) QKD protocol, the correlation between, say, A_0^B and K_0^B is greater than the correlation of A_0^B and a string that any other party can produce.

The private key sk that Alice uses to sign a message in the future is the concatenation of the two corresponding strings $sk = (A_0^B||A_0^C, A_1^B||A_1^C)$. During this process, the error rates of the channels are estimated, and values for s_a, s_v are chosen such that $0 < p_e < s_a < s_v < p_f < 1$, and s_a, s_v are "placed" equally separated within the gap $p_f - p_e$. Here, p_e is the estimated ("honest") error rate between Alice-Bob using their quantum channel, while p_f is the minimum error rate that Eve makes trying to guess Alice's string.

Bob and Charlie perform a symmetrization by exchanging secretly half of their strings (e.g., using another full QKD link). The new strings for Bob S_0^B, S_1^B (and similarly for Charlie S_0^C, S_1^C) are each composed from half of the string initially sent to Bob and half of that to Charlie, but which part from Bob's initial string and which part from Charlie's is unknown to Alice (since the symmetrization was performed secretly). The verification keys for Bob and Charlie are $pk_B = (S_0^B, S_1^B)$ and $pk_C = (S_0^C, S_1^C)$. (Note that we no longer call them public keys, being different for Bob and Charlie.)

b. Signing. In order to sign a message m, Alice sends $(m, A_m^B||A_m^C)$ to Bob.

c. Verification. To accept a message coming directly from Alice, Bob checks the mismatches rate p_t^B between the signature received $A_m^B||A_m^C$ and his stored verification key S_m^B, for each part of the signature separately (i.e. mismatches in the part he obtained directly from Alice and mismatches in the part he obtained from Charlie during the symmetrization). If $p_t^B < s_a$ he accepts for both cases, i.e. 1-ACC. Charlie receives a message with Alice's signature, but from Bob. He checks the mismatches rate p_t^C similarly to Bob, and if $p_t^C < s_v$ for both parts, he accepts the message as coming originally from Alice.

2. *Security intuition and performance*

Forging is not possible because any potential forger, even a legitimate party (e.g. Charlie), cannot guess the part of the Alice's private key that was not directly send to him, at least not with any probability significantly better than p_f. His forging probability actually scales at best as $e^{-c(p_f-s_a)^2 L}$ which vanishes for sufficiently large length of string L. Similarly, non-repudiation is guaranteed by the fact that Alice is ignorant on which part of K_m^B, K_m^C is in S_m^B and which is in S_m^C, she is therefore unable to make Bob accept and Charlie to reject, and her probability of succeeding in this scales as $e^{-c'(s_v-s_a)^2 L}$. Finally, an honest abort is unlikely, since we chose $s_a > p_e$ which leads to the honest abort occurring with probability at most $e^{-c''(p_e-s_a)^2 L}$.

A QDS protocol performance is judged by the time taken to distribute the verification key(s) among the parties, but also the distance that the parties could be separated. (The signing algorithm and verification algorithm are both assumed to be much quicker and thus we judge the protocols, essentially, on the time required for the key generation.) In most cases, we consider single-bit message and assume linear scaling, however there may exist more efficient ways to sign longer messages (e.g. [901] for a classical ITS scheme). The time taken to distribute the verification key(s) depends on the clock-rates (how many pulses are sent per second) and on how long strings L are required to achieve a desired level of security. In other words, what L and other choices should be made, so that the probability of something going wrong (forging, repudiation, honest-abort) is below ϵ – the desired level of security.

To jointly minimize the probabilities of forging, repudiation and honest-abort, we first need to determine the values p_e, p_f. The estimated honest-error rate p_e is obtained from the specific channel/experimental set-up used, and can be thought as a practical constraint. It is easy to see that p_e increases with the distance between parties, therefore there is a trade-off between speed of distributing verification key(s) and distance. We should keep this in mind when comparing different implementations. The best forging error attempt p_f is theoretically evaluated for example by considering the minimum-cost quantum measurement that adversaries can perform. Once these two are given, optimal choices for s_a, s_v are calculated to jointly minimize the probabilities of forging, repudiation and honest abort. Typically we require equal separation between the intervals $(s_a - p_e), (s_v - s_a), (p_f - s_v)$, since they all appear in similar form in the exponential decay of the expressions of honest-abort, repudiation and forging, respectively.

H. Extending QDS: Multiple parties, longer messages, and MDI

The QDS schemes we presented considered the case of three parties, the smallest number sufficient to illustrate the transferability property. In that setting, only one party at a time can be an adversary. In real practise however, multiple parties would be involved as potential receivers.

A potentially-important disadvantage of QDS compared with classical schemes is the way the communication required in the *Gen* phase scales as a function of the number of parties involved. For most QDS protocols, a quadratic number of communication channels is required. Moreover, when multiple parties are involved, the issue of colluding parties (including sender colluding with some receivers) should be considered, while also the issue of multiple transfers of a signed message (and the corresponding honest parties fraction thresholds) need to be considered. In Ref. [902] the general framework for multiple-party QDS, certain generic properties, and the concept of multiple levels of transferability (and verification) were introduced, along with a multi-party generalization of one protocol. In Ref. [903] the three-party protocol of [899] was also extended to multiple parties.

Most of the research on QDS is focused on signing single-bit messages, and it is usually stated that a simple iteration can be used for longer messages. While this is mostly true, there are two issues that require attention. First, as analyzed in Ref [904], there are attacks on longer messages impossible to be addressed from single-bit signatures, e.g. tampering with the order of the bits. The second issue is that of efficiency. In classical schemes, using hash functions one can reduce the extra cost from being linear in the size of the message (as in simple iterations) to being logarithmic [901]. It is worth exploring QDS schemes that could improve the scaling with the message size.

As with QKD, many QDS protocols are vulnerable to side-channel attacks [905], with the best known side-channel attacks exploiting measurement-device/detector vulnerabilities (e.g. the "blinding attack"). For this reason, MDI protocols for QDS where first introduced in Ref. [906]. The analysis follow closely that of QKD and of Ref. [899] and we omit further details. One interesting thing to note is that the extra security guarantee (against some side-channel attacks) comes at no (or low) cost in terms of practicality, unlike the fully device-independent protocols. Moreover, the MDI setting that contains untrusted mediating parties is suitable for QDS (where there are multiple parties and each party can be adversarial). It allows us to consider optimization of routing of quantum information in quantum networks, i.e. consider different (or even flexible) connectivity of parties to optimize the multiparty versions of QDS schemes.

I. Experimental QDS realizations

Since 2012, a number of experiments implementing QDS protocols has been performed, and from the first proof-of-principle experiments we now have fully secure, long-distance QDS implementations on existing quantum networks, suitable for real life applications. As mentioned in Section XV G and similarly to QKD, there is a trade-off between the distance that parties can be separated and the speed that verification keys for fixed length messages are distributed. The distances mentioned below are the maximum distances that QDS could run, while it is understood that for smaller distances the "rate"/performance would improve.

1. *Proof-of-principle*

The first QDS experiment by Clarke et al. [894] was based on the QDS protocol outlined in Ref. [892], where the coherent-state comparison (see Fig. 20) was introduced in order to replace the SWAP-test [882]. The simplest case of three-parties was implemented, where each coherent-state pulse $|\alpha\rangle = ||\alpha| \exp(2\pi i\phi)\rangle$ had its phase randomly chosen from eight possible choices ($\phi = k/8$ for $k \in \{0, \ldots, 7\}$). Different mean-photon numbers $|\alpha|^2$ were examined. As explained in the end of Section XV G, one needs to jointly minimize the forging, repudiation and honest-abort probabilities. Too high $|\alpha|$ makes p_f small (and forging simple since the states approach classical states and can be copied), while too low $|\alpha|$ makes p_e large (dark counts are a larger fraction of detections, making honest-abort more likely) so an optimal value for $|\alpha|$ should be sought.

The experiment was meant to be a proof of principle. Firstly, the parties were all located within small distance (same lab). Secondly, the signing and verifying happened immediately (no quantum state stored). In particular, instead of Bob regenerating the quantum state of the signature from Alice's signature (classical description), and then compare it with his stored states, Bob obtained directly the sequence of the qubits from Alice (that used a beam-splitter before sending the quantum public key) and compared it with the hypothetically stored quantum public key.

A second QDS experiment was performed by Collins et al. [907], based on the QDS protocol of Ref. [893] that does not require quantum memory. Because of this property, the only unrealistic assumption was the separation of the parties (still within the same lab), while the signing and verifying happened in arbitrary later time. The protocol used a generalization of the unambiguous discrimination measurement, namely unambiguous elimination measurement. Again it involved three parties, sharing strings of phase-encoded coherent states, where this time there were four $N = 4$ possible phases.

2. *Kilometer-range and fully-secure QDS*

Subsequently, based on the idea that one can replace the state comparison with symmetrization [898], two experiments [908, 909] were performed that had parties able to be separated by a distance of the order of kilometer. Callum et al. [909] was also the first QDS protocol that used CVs (heterodyne detection measurements) and the first experiment to be performed through a free-space noisy 1.6 km channel (in Erlangen).

Following [899, 900], the last unrealistic assumption was removed, i.e., authenticated quantum channels. The use of decoy states, and other theoretical but also technical improvements, resulted in protocols with far superior performance, having the parties separated by tens to hundred kilometers [910, 911]. This brings QDS in par with QKD in terms of practicality. Finally, MDI-QDS protocols, addressing measurement-device side-channel attacks, have been implemented over a metropolitan network [912] and at high rates by using a laser seeding technique together with a novel treatment of the finite-size effects [913].

J. Classical unconditional secure signatures

The type of digital signatures that are achieved by QDS offer ITS, but are one-time (cannot be reused) and require a fixed number of parties all participating during the key generation phase. Only those parties can sign and verify in the future messages and, if one wanted to extend the participating parties, new interactions would be required between (many) parties. In contrast, classical public-key signatures can be verified by anyone with access to the public key (that can be obtained later than the Key Generation phase).

This specific type of signatures that QDS achieve, was actually first considered by Chaum and Roijakkers [914] and were termed unconditionally secure digital signatures (USS). In order to achieve USS, all parties needed to share (long) secret key pairwise, while another assumption was also necessary (an authenticated broadcast channel or anonymous channels). Only a few papers followed this work [915–918]. The main reason for the limited interest was probably because such protocols were seen as impractical, specifically because they require point-to-point shared secret keys. Then, the extra security offered (information theoretic) was not viewed as necessary. Both of these issues have been revisited with the recent advances in quantum technologies since: (i) sharing long secret keys can be achieved with QKD, and (ii) advances in quantum computers make realistic the prospect of large scale quantum computers that could break existing cryptosystems in the medium term. Therefore, it appears likely that interest for this type of protocols could increase.

In a parallel direction, inspired by QDS, a classical USS protocol was proposed in Ref. [898], where only pairwise secret keys were required. This scheme was generalized to multiple parties in Ref. [902]. Subsequently, in Ref. [901], a USS protocol that scales much better for longer messages was obtained using universal hashing (it requires key-sizes that scale logarithmically with the message length). All these protocols require only point-to-point secret keys and neither authenticated broadcast channel nor anonymous channels or trusted third parties were assumed. Because no further assumptions were made, these protocols prove a "reduction" of the task of USS to that of point-to-point secret keys and thus to standard QKD.

K. Summary and outlook

QDS is a type of digital signatures that offers information theoretic security, a very attractive feature, that the progress in building quantum computers has made even more timely. The "trade-off" is that this type of digital signatures that QDS achieve is missing some of the elements that made digital signatures such an important functionality (e.g. the universal verifiability).

In this review we described the research that transformed QDS from a theoretical interesting observation to a practical possibility. In Sections XV E and XV F we presented the developments and choices made in a historical order, while in Section XV G we gave a description and brief analysis of a generic modern QDS protocol. Latest state-of-the-art developments were subsequently mentioned briefly, referring the reader to the original works for further details.

Possibly the biggest challenge for QDS is how do they compare with the classical digital signature schemes that offer ITS. In Section XV J we presented those classical protocols and noted that all of them require point-to-point (long) secret keys between the participants. Indeed, it appears that the classical scheme given in Ref. [901] (inspired by QDS) offers similar guarantees and cost with QDS while being more efficient for long messages, i.e., exponentially better with respect to the size of the message signed.

However, there are at least three directions (and reasons) that further research in QDS is still very promising.

1. Firstly, it is likely that a QDS protocol with better scaling for long messages can be developed. So far, the majority of research in QDS focused on the single-bit message case and the possibility of better scaling for longer messages has not been sufficiently examined.

2. Secondly, classical protocols require communication between *all* parties, i.e., quadratic in the number of participants and number of communication channels. In contrast, with QDS it is possible to achieve linear scaling with respect to the quantum channels. The QDS scheme given in Ref. [900] is an example that offers such feature. This particular protocol would not scale so well with more parties for different reasons (sensitive in forging probability), but it demonstrates the possibility of using quantum resources to reduce the communication channels.

3. Thirdly, in Ref. [899] a QDS protocol was given that could be secure even when the noise in the channels was too high for QKD, again demonstrating the possibility that fundamentally quantum protocols are possible when the "classical" ones (that in any case require QKD) are impossible.

Finally, the so-called "classical" ITS protocols, such as the one given in Ref. [901], require point-to-point secret keys, and those keys can only be practically achieved using QKD. In this sense we can view even these schemes as *quantum* digital signature schemes. While the theory of classical ITS protocols involves little or no new quantum research, their development makes stronger the case for building a quantum communication infrastructure and thus increases the impact of quantum cryptography by offering further functionalities.

In particular, digital signatures are useful when they involve many (potential) parties, which means that QDS

could be useful for real applications only if the corresponding infrastructure is in place, i.e., a large quantum network. While this infrastructure is not currently available, the possibility of QDS (including the USS protocols given above) offers greater value to quantum networks and thus makes the argument for developing such infrastructure more compelling.

XVI. POST-QUANTUM CRYPTOGRAPHY

A. Overview

Quantum computers (when large, fault-tolerant devices are available) will lead to speed-ups in various problems. The exact magnitude of the quantum speed-up varies with the task, from exponential (e.g., in factoring) to quadratic (unstructured search) and even smaller (e.g., in collision-finding). This means that whether a specific (classical) computationally-secure cryptosystem breaks completely, needs to be modified or is not affected at all, depends crucially on the details of the cryptosystem. While most of the widely used cryptosystems are based on factoring and discrete log (e.g. RSA and elliptic curve cryptography) and are expected to completely break with quantum computers, there are numerous older and newer alternatives (all of them less efficient and therefore barely employed) that are not expected or known to be broken by quantum computers. These protocols are characterized by a (conjectured) computationally intractable task, irrespective of whether the protocols are for encryption, signatures or other tasks.

There are mainly five categories of such classical protocols: lattice-based, code-based, hash-based, multivariate and supersingular-isogeny. The body of research in this field is big and is beyond the scope of this review to list it [919]. The National Institute of Standards and Technology (NIST) has an active competition for post-quantum secure cryptosystems where one can find numerous candidates [635]. Here we just give the hardness assumptions of each category, while we conclude with analyzing the complementary role that post-quantum cryptography (PQC) has to QKD and stress the essential quantum expertise that is needed for carrying proper security analysis against quantum attackers. Note that secret-key encryption, e.g., block-ciphers with prominent example the AES encryption algorithm [920], is also not known to break with quantum computers (beyond a modification to requiring to double the key-size for the same security level due to Grover's algorithm). However, there is very little research on symmetric-key quantum cryptanalysis [921].

B. Lattice-based protocols

This category includes problems whose security is based on problems involving lattices in large dimensions (which are given using one of the many equivalent basis vector sets). The most important hard problem for cryptography in lattices is the Shortest-Vector-Problem (SVP) [922]. It requires to approximate the smallest Euclidean length of a non-zero vector, and it is believed to be hard (even in its approximate version) for both classical and quantum computers. The actual problem appearing in most cryptosystems of this type is the Learning-with-Errors problem (LWE) [923], which is the problem of inverting a linear matrix when instead of being given exact values, one is given samples that are perturbed by random noise (with known distribution). The reason that this problem is used is that it was proven that the average instance of this problem is as hard as the worst-case instance of the SVP problem, and it is known that the SVP problem is (worst-case) hard. It is important to note here that a good problem for public-key cryptography not only needs to be believed to be hard, but also needs to be hard for average instances and not only for worst-case instances. (Complexity theory characterises the problems with respect to their worst-case instances, so saying that a problem is NP-complete only means that in the worst-case it is hard, but it may be that the average case is not hard.)

C. Code-based protocols

This category uses families of error-correcting codes, that can correct up to t errors. The code is chosen at random from a certain family of codes (e.g. McEliece codes [924] or Goppa codes [925]), and the decoding algorithm is kept secret. The hard problems used in these cryptosystems are: (i) maximum-likelihood decoding and (ii) minimum distance problem. These problems are classically hard, and there are also no known quantum algorithms to solve them. However, we are less confident on the true quantum-hardness of these problems, since there is no reduction of this problem to other, hard-for-quantum-computers, problems (as in the lattice-based case). What has been shown, is that these cryptosystems are resistant to attacks using Shor's algorithm and its variations.

D. Hash-based protocols

This category is based on the assumption that there exist good approximations of cryptographic hash functions. The current standard is the secure hash algorithm 3 (SHA-3) [926]. There is no strong theoretical argument (neither for classical nor for quantum case) why such functions are indeed hard to invert or to hard to find collisions. The security proofs are typically done in the *random oracle model*, where one models/replaces the real hash function, such as SHA-3, with an ideal random function. Existing cryptosystems have been analysed in the *quantum random oracle model* [927], where the input

and outputs of this idealised box can be quantum states (superposition). This type of attacks admit quantum speed-ups of the type of Grover's algorithm (quadratic). The existing candidate protocols in the NIST competition have their security parameters tuned to be robust against this type of attacks.

E. Other categories of protocols

In multivariate protocols, the hard problem is to find a solution to a system of quadratic equations, in many variables, over a finite field [928]. Most cryptosystems of this type, use structured systems, but assume that the (classical or quantum) attacker cannot exploit this structure. In supersingular-isogeny protocols, the hard problem is instead to find a rational map that preserves the structure between elliptic curves [929]. The security of such protocols is related to collision finding, but there is no formal reduction proving this. It is a new approach and more study is needed to establish confidence.

F. Can quantum cryptography fully replace classical (public-key) cryptography?

While, as argued extensively, QKD and quantum cryptography in general can offer invaluable extra security in (parts) of our communications, claiming that they can fully replace public-key cryptography is not equally well justified, at least currently, for various reasons.

- First, QKD cannot be used (directly) to practically replace encryption with no extra assumption. Even if quantum communication networks are developed, we are still very far from having every single device connected, and it is arguably not very realistic to envision that all devices will have quantum capabilities (e.g. all devices in the Internet of Things).
- The bandwidth that can be achieved, even in the most optimistic scenario, is too low currently for certain applications and there are also theoretical bounds putting restrictions in the possibility for improvements. For example, for live-streaming or in the proof-of-principle teleconference between Austria and China [79] , a classical block-cipher was used to expand the quantumly obtained secret key.
- An essential assumption for QKD is the existence of a classical authenticated channel. While this can be achieved if a pre-shared (small) key exist (in which case we can view QKD as information-theoretic key expansion protocol), frequently parties that have never met need to communicate with secrecy (e.g. in internet commercial transactions). In that case, establishing the key for authenticated communication can only happen using public-key cryptography and infrastructure.
- QKD and similar quantum communication protocols may not be able to replace all functionalities. For example we have seen that only a specific type of one-time-signatures without the universal verifiability property could be established using quantum communications. For many applications, this type of signature may not be suitable or practical (e.g. for networks with variable number of parties participating, such as in blockchain protocols).

From the above, it is evident that the role that quantum cryptography and post-quantum cryptography are going to play for securing our communications, in the medium-term, is likely to be complementary rather than competing.

G. Further issues and essential quantum research

It is clear that a necessary condition for a classical cryptosystem to be secure against quantum attackers, is to not rely on computational assumptions that change with the development of quantum computers (e.g. hardness of factoring). However, this not the only type of concern in proving the post-quantum security of a cryptosystem. New type of attacks (e.g. superposition attacks [930]) and changes in the security proof techniques (e.g. quantum rewinding [931]) and definitions need to be considered (see also Ref. [932]). This type of research goes far beyond the classical cryptography expertise, since it involves modelling adversaries as general quantum systems.

One of the major problems with using post-quantum cryptosystems and establishing standards, is that it is essential that the security is based on a problem that is not only believed to be (asymptotically) hard, but also that there are no significant improvements in the best possible algorithms (attacks). The latter is essential, because the security parameters (key-lengths, etc) are determined by the best known attack. Even a moderate improvement in the optimal algorithm may result in making a specific implementation of a cryptosystem insecure, and changing the implementation takes time and (considerable) cost, while there may be security breaches in the meantime.

Therefore, before one can establish reliable standards for post-quantum cryptography, it is essential that the corresponding hard problems are attacked by quantum algorithms researchers, from multiple groups, for sufficient time that the optimal quantum algorithms become quite stable. This is another research field that requires a fruitful interaction between classical cryptographers and quantum information scientists.

XVII. FURTHER TOPICS IN QUANTUM CRYPTOGRAPHY

Modern (classical) cryptography covers a wide range of functionalities and primitives and goes much beyond

"simple" encryption and signatures schemes. The development of quantum technologies is likely to enable new possibilities or enhance the security and efficiency of current cryptographic solutions in all these fields. In the physics community, one mostly reserves the use of the term "quantum cryptography" for QKD and related primitives (QRNG, QDS). However it is important to note that under this umbrella (or the more general "quantum cyber security" [932]) there are numerous different protocols that researchers have developed both theoretically and implemented them experimentally. It is beyond the scope of this review to give an extensive review of all these, but for completeness, we briefly mention some of these (see also the complementary reviews [434, 933]).

We will group the research into three categories: basic cryptographic primitives, cryptographic functionalities, and secure quantum computing.

A. Basic cryptographic primitives

These are tasks that while on its own right do not have an obvious use, can be used as building blocks for involved tasks. Two such prominent tasks is the bit-commitment (a two party task where one party commits a bit-value without announcing or leaking information about this choice but also without being able to alter this choice later) and oblivious transfer (multiple variations of this primitive exist). One of the most well known limitations that quantum cryptography has, is that it was shown [934, 935] that it is impossible to achieve either of these primitives perfectly with information theoretic security, using quantum information without any extra assumptions. On the other hand, it is still possible to perform better than classical protocols (e.g. [936]) or to achieve information theoretic security by using extra assumptions (such as the relativistic bound of the speed of transfer of information, or the bounded storage assumption) [937, 938].

Other primitives involve the closely related protocols of: coin-tossing [939], quantum secret sharing [562] (where a quantum secret is shared among parties in a way that it requires at least a subset of these parties to recover *any* information), quantum fingerprinting [940] (that can play the role of a cryptographic hash function, and it is shown that there is an exponential separation between classical and quantum solutions) and zero-knowledge proofs [941, 942] (where parties can prove that they know the answer to certain statement without giving any details of the proof).

B. Cyptographic functionalities

We group here tasks that have direct interest on their own right and that they admit quantum solutions. Historically the first seminal paper on quantum cryptography was the quantum money paper by Wisner [943] that actually preceded and inspired QKD. The basic idea is to exploit the no-cloning of quantum information to generate money that cannot be forged. This topic has recently being revived, while multiple variations (tokens vs coins, private vs public) exist [944], some of which have even been implemented [945]. Byzantine agreement [946] and blockchain [947] are both ways to generate consensus among mistrustful parties, without using a trusted third party. There are also proposals to enhance the task of e-voting using quantum means [948] where recently a more rigorous treatment has been taken [949].

Verifying the position of a non-trusted party is also a hard task (impossible classically) that has many applications and cryptographic consequences. Using relativistic and quantum methods, and posing an upper bound on the available adversarial resources this task becomes possible [950]. Private information retrieval enables a party to recover an item from a database without leaking to the database owner the item that was retrieved. A quantum protocol outperforming its classical counterparts also exists [951]. Finally, protocols for encryption (symmetric and public key [952]) and authentication of *quantum* information have been developed [891, 953–955].

C. Secure quantum computing

Here we assume that one (or multiple) parties have a quantum computer that can offer computational speed-up for certain tasks. However, we are in a setting where some parties (either the ones with the quantum computing devices or other parties with fewer resources) have sensitive information that do not want to share. Classically such situations are very common and important (e.g. computations on medical records, auctions, etc). In the quantum technologies landscape, such possibility is even more timely, since the companies or research centers that will have large quantum computers will be few and most of the revenue will be generated by providing cloud quantum computing services to companies with specific applications. The privacy of data and algorithms that clients may want to run could be crucial.

Quantum protocols for many of these tasks have been developed (theoretically and in proof-of-principle experiments). These include: blind quantum computing [956, 957] (client delegating quantum computation to an untrusted server without leaking input/output or computation), verifiable blind quantum computing [958–960] (here the client can also check the correctness of the computation), quantum fully homomorphic encryption [961] (the delegation happens in a non-interactive way) and secure multiparty quantum computation [962, 963] (where many untrusted parties want to compute a joint circuit on a joint input, without leaking to each other anything beyond the actual outcome of the computation).

Most of these protocols require quantum communication and capabilities from all parties (including the parties/clients with limited resources that want to delegate

the task). According to recent developments, exploiting techniques from post-quantum cryptography, one can show that many of these tasks can be achieved with fully-classical clients at the cost of reducing the security to hold only against computationally-bounded quantum adversaries [964–967]. In theory, this opens up the possibility for classical parties/clients to use cloud quantum computing services with a certain level of security.

XVIII. CONCLUSIONS

In this review we have presented basic notions and recent advances in the field of quantum cryptography. We have focused most of the discussion on QKD, but also presented some developments which goes beyond the standard setting of key distribution. While quantum cryptography is certainly the most mature quantum technology so far, a number of challenges and open questions are facing both theoretical and experimental work.

There is still the need to develop and implement more robust QKD protocols, which are able to achieve long distances at reasonably high rates. These protocols could then be integrated in trusted-node QKD networks, whose performance would consequently be improved. An even more ideal goal would be the realization of a QKD network which is both scalable and end-to-end, so that the middle nodes can be of arbitrary number while being simultaneously untrusted. In principle, this network may be realized by building efficient quantum repeaters for entanglement distillation and distribution. In practice, we would like to employ cheaper designs, e.g., untrusted QKD repeaters that are only based on measurement operations. However, this solution is not currently scalable.

From a purely theoretical point of view, there are efforts directed at establishing the fully-composable finite-size security of a number of QKD protocols, both in DV and CV settings. It is then an open question to determine the secret key capacity of several fundamental quantum channels for quantum communications, such as the thermal-loss channel and the amplitude damping channel. While the recently-developed simulation techniques have been successful in many cases, the two-way assisted capacities of these channels may need the development of a completely new and different approach.

Current experimental efforts are going towards many directions, from photonic integrated circuits to satellite quantum communications, from more robust point-to-point protocols to implementations in trusted-node quantum networks, from qubit-based approaches to higher dimensions and CV systems. While optical and telecom frequencies are by far the more natural for quantum communications, longer wavelengths such as THz and microwaves may have non-trivial short-range applications which are currently under-developed.

A number of loopholes need to be carefully considered before QKD can be considered to have become an fully-secure quantum technology. Practical threats are coming from side-channel attacks, for which countermeasures are currently being studied and developed for some of the most dangerous quantum hacks. Weakness may come from things like imperfections in detectors or the random number generators. Quantum hacking and countermeasures is therefore an important and growing area.

In general, for a technological deployment of quantum cryptography and QKD, we will need to consider its integration with the current classical infrastructure and develop layers of security, depending on the degree of confidentiality to be reached which, in turn, depends on the stakeholder and the type of business involved. Protocols based on bounded-memories and QDL provide a temporary low-level of quantum security that may be suitable for private personal communications. Standard QKD protocols provide higher levels of security that may be suitable for financial transactions. Within QKD, different secret key rates might be considered, for instance, with respect to individual, collective or fully-coherent attacks. The choice of these rates may also be associated with a specific sub-level of security to be reached. Higher level of security, for applications such as political or strategic decisions, may involve the use of DI-QKD, which is more robust to both conventional and side-channel attacks. These aspects will become clearer and clearer as quantum cryptography will progressively become a wider technological product.

ACKNOWLEDGMENTS

This work has been supported by the EPSRC via the 'UK Quantum Communications Hub' (EP/M013472/1, EP/T001011/1) and the First Grant EP/P016588/1; the European Union via the project 'Continuous Variable Quantum Communications' (CiViQ, no 820466), the project UNIQORN (no 820474), and the H2020 Marie Sklodowska Curie Project 675662 (QCALL); the Danish National Research Foundation bigQ (DNRF142); the Czech Science Foundation (project No 19-23739S); the Czech Ministry of Education via the INTER-COST grant No LTC17086; the Air Force Office of Scientific Research program FA9550-16-1-0391 (supervised by Gernot Pomrenke) and the Office of Naval Research CONQUEST program. Authors are indebted to Marco Lucamarini for his help, comments and suggestions, and for providing the file for the rate of the TF-QKD protocol, plotted in Figs. 3 and 11. A special thank also goes to Xiongfeng Ma, Pei Zeng, Xiang-Bin Wang, Zhen-Qiang Yin, and Federico Grasselli for having provided files and data points for the rates plotted in Fig. 11. Authors also thank Davide Bacco, József Zsolt Bernád, Samuel L. Braunstein, David E. Bruschi, Dagmar Bruß, Zeng-Bing Chen, Wolfgang Dür, Saikat Guha, Tobias Heindel, Timo Holz, Neda Hosseinidehaj, Nitin Jain, David I. Kaiser, Hermann Kampermann, Aeysha Khalique, Alex Koehler-Sidki, Rupesh Kumar, Fabian Laudenbach, Riccardo

Laurenza, Anthony Leverrier, Yongmin Li, Qin Liao, Seth Lloyd, Peter van Loock, Robert Malaney, Daniel Miller, William J. (Bill) Munro, George Nikolopoulos, Kaushik P. Seshadreesan, Jeffrey H. Shapiro, Gaetana Spedalieri, Spyros Tserkis, Lev Vaidman, David Vitali, Qin Wang, Christian Weedbrook, Hua-Lei Yin, Yichen Zhang, Zheshen Zhang, and Quntao Zhuang for useful comments, suggestions, and feedback.

Appendix A: Formulas for Gaussian states

Consider n bosonic modes described by the creation and annihilation operators $\hat{a}_j^\dagger$, $\hat{a}_j$ with $j = 1, \ldots, n$ and define the quadrature operators as

$$\hat{q}_j = (\hat{a}_j + \hat{a}_j^\dagger)/\sqrt{2\kappa}, \quad \hat{p}_j = -i(\hat{a}_j - \hat{a}_j^\dagger)/\sqrt{2\kappa}, \tag{A1}$$

where the factor κ is introduced to consistently describe different notations used in the literature (see also Ref. [968]). The canonical choice in quantum optics is $\kappa = 1$ (vacuum noise/SNU equal to 1/2) where we recover the canonical commutation relations $[\hat{q}_k, \hat{p}_j] = i\delta_{kj}$, while a popular choice in quantum information is $\kappa = 1/2$ (vacuum noise/SNU equal to 1). For any general κ, the quadrature operator can be grouped into a vector $\hat{\mathbf{x}}$ with $2n$ components that satisfies the following commutation relation

$$[\hat{\mathbf{x}}, \hat{\mathbf{x}}^T] = \frac{i\Omega}{\kappa}. \tag{A2}$$

The coordinate transformations $\hat{\mathbf{x}}' = \mathbf{S}\hat{\mathbf{x}}$ that preserve the above commutation relations form the symplectic group, i.e. the group of real matrices such that $\mathbf{S}\Omega\mathbf{S}^T = \Omega$. There are essentially two standard ways of grouping the quadrature operators, and the definition of Ω changes accordingly. These are

$$\hat{\mathbf{x}} := (\hat{q}_1, \ldots, \hat{q}_n, \hat{p}_1, \ldots, \hat{p}_n)^T, \quad \Omega := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \otimes \mathbb{1}\,, \tag{A3}$$

where $\mathbb{1}$ is the $n \times n$ identity matrix, or

$$\hat{\mathbf{x}} := (\hat{q}_1, \hat{p}_1, \ldots, \hat{q}_n, \hat{p}_n)^T, \quad \Omega := \bigoplus_{j=1}^{n} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\,. \tag{A4}$$

All the formulae that we review here are independent of this choice, provided that the grouping $\hat{\mathbf{x}}$ and matrix Ω are chosen consistently.

Any multimode bosonic state ρ can be described using phase-space methods by means of the Wigner characteristic function $\chi(\boldsymbol{\xi}) = \mathrm{Tr}[\rho e^{i\hat{\mathbf{x}}^T\Omega\boldsymbol{\xi}}]$. The state ρ is called Gaussian when $\chi(\boldsymbol{\xi})$ is Gaussian [7]. For a Gaussian state, the density operator ρ has a one-to-one correspondence with the first- and second-order statistical moments of the state. These are the mean value $\bar{\mathbf{x}} := \langle\hat{\mathbf{x}}\rangle_\rho = \mathrm{Tr}(\hat{\mathbf{x}}\rho) \in \mathbb{R}^{2n}$ and the covariance matrix (CM) V, with generic element

$$V_{kl} = \frac{1}{2}\langle\{\hat{x}_k - \bar{x}_k, \hat{x}_l - \bar{x}_l\}\rangle_\rho\,, \tag{A5}$$

where $\{,\}$ is the anticommutator.

According to Williamson's theorem, there exists a symplectic matrix $\mathbf{S}$ such that [7]

$$\mathbf{V} = \mathbf{S}(\mathbf{D} \odot \mathbf{D})\mathbf{S}^T, \quad \mathbf{D} = \mathrm{diag}(v_1, \ldots, v_n), \tag{A6}$$

where the v_j's are called symplectic eigenvalues and satisfy $v_j \geq (2\kappa)^{-1}$. When $v_j = (2\kappa)^{-1}$ for all j the state is pure. With the canonical choice $\kappa = 1$ this means that a pure state is defined by $v_j = 1/2$ for all j, while with the choice $\kappa = 1/2$ a pure state has $v_j = 1$ for all j. The dot operator $\odot$ in Eq. (A6) has been introduced to make the notation uniform depending on the different grouping rules of Eqs. (A3) and (A4). When Eq. (A3) is employed the dot operator is defined as $\mathbf{D} \odot \mathbf{D} := \mathbf{D} \oplus \mathbf{D} = (v_1, \ldots, v_n, v_1, \ldots, v_n)$, while when Eq. (A4) is employed the dot operator is defined as $\mathbf{D} \odot \mathbf{D} := (v_1, v_1, \ldots, v_n, v_n)$.

Although the Wigner function formalism is a popular approach for describing Gaussian quantum states [7], quantities normally appearing in quantum information theory can often be computed more straightforwardly using an algebraic approach [969]. Any multi-mode Gaussian state $\rho(\mathbf{V}, \bar{\mathbf{x}})$ parameterized by the first- and second-moments $\bar{\mathbf{x}}$ and $\mathbf{V}$ can be written in the operator exponential form [969] (see also [970, 971])

$$\rho(\mathbf{V}, \bar{\mathbf{x}}) = \exp\left[-\frac{\kappa}{2}(\hat{\mathbf{x}} - \bar{\mathbf{x}})^T\mathbf{G}(\hat{\mathbf{x}} - \bar{\mathbf{x}})\right]/Z_\rho\,, \tag{A7}$$

where

$$Z_\rho = \det\left(\kappa\mathbf{V} + \frac{i\Omega}{2}\right)^{1/2}, \tag{A8}$$

and the *Gibbs matrix* $\mathbf{G}$ is related to the CM $\mathbf{V}$ by

$$\mathbf{G} = 2i\Omega\,\coth^{-1}(2\kappa\mathbf{V}i\Omega), \quad \mathbf{V} = \frac{1}{2\kappa}\coth\left(\frac{i\Omega\mathbf{G}}{2}\right)i\Omega. \tag{A9}$$

The above relations are basis independent and allow the direct calculation of $\mathbf{G}$ from $\mathbf{V}$ without the need of the symplectic diagonalization (A6). This is a consequence of the "symplectic action" formalism that is discussed in the next section. From the operator exponential form, we then show how to compute quantities like the fidelity between Gaussian states, the von Neumann entropy, the quantum relative entropy and its variance.

1. Symplectic action and its computation

Given a function $f : \mathbb{R} \to \mathbb{R}$ we can extend f to map Hermitian operators to Hermitian operators in the following way: let $M = UxU^\dagger$ be the spectral decomposition of a Hermitian operator M, then $f(M) := Uf(x)U^\dagger$

where $f(x)$ is a vector whose j-th element is $f(x_j)$. For more general operators M that admit a decomposition $M = UxU^{-1}$, with a possibly non-unitary U, we define an operator function as $f(M) := Uf(x)U^{-1}$.

The symplectic action was introduced in Ref. [972] to extend a function f to any operator with symplectic structure. More precisely, for a given matrix $\mathbf{V}$ with symplectic diagonalization as in Eq. (A6), the symplectic action f_* on $\mathbf{V}$ is defined by

$$f_*(\mathbf{V}) = \mathbf{S}[f(\mathbf{D}) \odot f(\mathbf{D})]\mathbf{S}^T, \tag{A10}$$

where $f(\mathbf{D}) = \mathrm{diag}[f(v_1), f(v_2), \ldots, f(v_n)]$ acts as a standard matrix function. In Ref. [969] it was proven that, for any odd function $f(-x) = -f(x)$, the symplectic action can be explicitly written as

$$f_*(\mathbf{V}) = f(\mathbf{V}i\Omega)i\Omega. \tag{A11}$$

where $f(\mathbf{V}i\Omega)$ is a matrix function.

Matrix functions are part of most numerical libraries and symbolic computer algebra systems, so their computation, either numerical or analytical, can be easily done on a computer. This is an advantage especially for symbolic calculations [43, 969]. On the other hand, for a full symplectic diagonalization, the practical problem is not the computation of the symplectic spectrum but the derivation of the symplectic matrix $\mathbf{S}$ performing the diagonalization $\mathbf{SVS}^T$ into the Williamson's form [7]. (For a simple proof of this theorem see Ref. [973] and also Appendix A of Ref. [518].) For the symplectic matrix $\mathbf{S}$, we know closed analytical formulas only for specific types of two-mode Gaussian states [974] which appear in problems of quantum sensing [725], such as quantum illumination [727] and quantum reading [728]. For a numerical way to compute the symplectic matrix $\mathbf{S}$, see the recipe in Appendix B of Ref. [518].

The Gibbs exponential form (A7) can be proven by first noting that a single mode thermal state with diagonal CM $\mathbf{V} = v \odot v$ can be written as an operator exponential

$$\rho = e^{-\frac{g}{2}\kappa(\hat{q}^2+\hat{p}^2)}/Z_\rho \ , \tag{A12}$$

with $g = 2\coth^{-1}(2\kappa v)$ and extending the result to multi-mode, possibly non-thermal states, via the symplectic action. Indeed, since $\rho \propto e^{-g\hat{a}^\dagger\hat{a}}$, we may write

$$v := \langle \hat{q}^2 \rangle = \langle \hat{p}^2 \rangle = \frac{\langle \hat{a}^\dagger \hat{a} \rangle + 1/2}{\kappa} = \frac{1}{2\kappa}\coth\frac{g}{2}. \tag{A13}$$

Following the same construction of Ref. [969], which was done for $\kappa = 1$, we get the final result of Eq. (A7).

2. Fidelity between arbitrary Gaussian states

The fidelity $F(\rho_1, \rho_2)$ quantifies the degree of similarity between two quantum states ρ_1 and ρ_2. It is a central tool is many areas of quantum information, especially for quantum state discrimination which is a fundamental process in any decoding process. For pure states, it is defined as $F = |\langle\psi_1|\psi_2\rangle|^2$, while for mixed states it may be defined in terms of the trace norm $||O|| := \mathrm{Tr}|O| = \mathrm{Tr}\sqrt{O^\dagger O}$ as [975]

$$F := ||\sqrt{\rho_1}\sqrt{\rho_2}|| = \mathrm{Tr}\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}} \ . \tag{A14}$$

A general closed-form for the fidelity between two arbitrary multi-mode Gaussian states was derived in Ref. [969], thus generalizing partial results known for single-mode states [976–978], two-mode states [979], pure [972] or thermal states [980].

Given two arbitrary multi-mode states with CMs $\mathbf{V}_i$ and first moments $\bar{\mathbf{x}}_i$, the fidelity F can be written as [969]

$$F(\rho_1, \rho_2) = \frac{F_{\mathrm{tot}}}{\sqrt[4]{\det\left[\kappa(\mathbf{V}_1 + \mathbf{V}_2)\right]}} e^{-\frac{1}{4}\delta^T(\mathbf{V}_1+\mathbf{V}_2)^{-1}\delta}, \tag{A15}$$

where $\delta := \bar{\mathbf{x}}_2 - \bar{\mathbf{x}}_1$, while the term F_{tot} only depends on $\mathbf{V}_1$ and $\mathbf{V}_2$ and is easily computable from the auxiliary matrix

$$\mathbf{V}_{\mathrm{aux}} = \Omega^T(\mathbf{V}_1 + \mathbf{V}_2)^{-1}\left(\frac{\Omega}{4\kappa^2} + \mathbf{V}_2\Omega\mathbf{V}_1\right), \tag{A16}$$

as

$$F_{\mathrm{tot}}^4 = \det\left[2\kappa\left(\sqrt{\mathbb{1} + \frac{(\mathbf{V}_{\mathrm{aux}}\Omega)^{-2}}{4\kappa^2}} + \mathbb{1}\right)\mathbf{V}_{\mathrm{aux}}\right] \ . \tag{A17}$$

The general solution (A15) has been derived thanks to the operator exponential form (A7) that makes straightforward the calculation of the operator square roots in the fidelity (A14). Indeed, using the Gibbs matrices $\mathbf{G}_i$ of the two Gaussian states, it was found in [969] that

$$F_{\mathrm{tot}} = \det\left(\frac{e^{i\Omega\mathbf{G}_{\mathrm{tot}}/2} + \mathbb{1}}{e^{i\Omega\mathbf{G}_{\mathrm{tot}}/2} - \mathbb{1}} i\Omega\right)^{\frac{1}{4}} \ , \tag{A18}$$

where

$$e^{i\Omega\mathbf{G}_{\mathrm{tot}}} = e^{i\Omega\mathbf{G}_1/2}e^{i\Omega\mathbf{G}_2}e^{i\Omega\mathbf{G}_1/2} \ . \tag{A19}$$

The final form (A15) is then obtained by expressing the above matrix functions in terms of CMs. Note that the asymmetry of $\mathbf{V}_{\mathrm{aux}}$ upon exchanging the two states is only apparent and comes from the apparent asymmetry in the definition of Eq. (A14). One can check that the eigenvalues of $\mathbf{V}_{\mathrm{aux}}\Omega$, and thus the determinant in Eqs. (A17), are invariant under such exchange.

As already mentioned, an efficient computation of the quantum fidelity is crucial for solving problems of quantum state discrimination [138, 139, 725], where two multi-mode Gaussian states must be optimally distinguished. Consider N copies of two multimode Gaussian states, $\rho_1^{\otimes N}$ and $\rho_2^{\otimes N}$, with the same a priori probability. The minimum error probability $p_{\mathrm{err}}(N)$ in their

statistical discrimination is provided by the Helstrom bound [981], for which there is no closed form for Gaussian states. Nonetheless, we may write a fidelity-based bound [969, 982] as

$$\frac{1-\sqrt{1-[F(\rho_1,\rho_2)]^{2N}}}{2} \leq p_{\rm err}(N) \leq \frac{[F(\rho_1,\rho_2)]^N}{2} \ . \tag{A20}$$

The fidelity can be expressed [983] as a minimization over POVMs E_x of the overlap between two classical probability distributions $p_i = \mathrm{Tr}[\rho_i E_x]$

$$F(\rho_1,\rho_2) = \min_{\{E_x\}} \sqrt{\mathrm{Tr}[\rho_1 E_x]\mathrm{Tr}[\rho_2 E_x]} \ . \tag{A21}$$

Calling $\tilde{E}_x$ the optimal POVM that achieves the minimum of the above quantity, we see that the fidelity can be measured with a single POVM without state tomography. As such we may write

$$p_{\rm err}(N) \leq \frac{1}{2}\left(\sqrt{\mathrm{Tr}[\rho_1\tilde{E}_x]\mathrm{Tr}[\rho_2\tilde{E}_x]}\right)^N \ . \tag{A22}$$

where $\tilde{E}_x$ is optimal for the bound, in the sense that any other POVM provides a larger upper bound. Recently [984], it has been shown that such optimal POVM can be explicitly computed between any two multi-mode Gaussian states. Indeed, it was found that the optimal POVM is formed by the eigenbasis of the operator [984]

$$\hat{M} \propto \hat{D}(\bar{\mathbf{x}}_1)\exp\left[-\frac{\kappa}{2}\hat{\mathbf{x}}^{\rm T}\mathbf{G}_M\hat{\mathbf{x}} - v_M^{\rm T}\hat{\mathbf{x}}\right]\hat{D}^\dagger(\bar{\mathbf{x}}_1), \tag{A23}$$

where $\hat{D}$ is a displacement and $v_M = 0$ when $\bar{\mathbf{x}}_1 = \bar{\mathbf{x}}_2$, while the general case is provided in [984]. On the other hand, the matrix $\mathbf{G}_M$ is given by

$$e^{i\Omega\mathbf{G}_M} = e^{-i\Omega\mathbf{G}_1/2}\sqrt{e^{i\Omega\mathbf{G}_1/2}e^{i\Omega\mathbf{G}_2}e^{i\Omega\mathbf{G}_1/2}}e^{-i\Omega\mathbf{G}_1/2}. \tag{A24}$$

Based of this general multi-mode solution, it was found in [984] that, for single-mode Gaussian states, there are only three possible kinds of optimal measurements, depending on ρ_1 and ρ_2: number-resolving detection, quadrature detection, or a projection onto the eigenbasis of operator $\hat{q}\hat{p}+\hat{p}\hat{q}$.

3. Entropic quantities

Entropic quantities are widespread in quantum information theory, and are employed to bound the performances of QKD protocols, entanglement sharing and data compression, to name a few examples. Here we provide some simple formula for the von Neumann entropy of a Gaussian state and for the relative entropy between two arbitrary Gaussian states $\rho_1(\bar{\mathbf{x}}_1,\mathbf{V}_1)$ and $\rho_2(\bar{\mathbf{x}}_2,\mathbf{V}_2)$ directly in terms of their first moments $\bar{\mathbf{x}}_j$ and covariance matrices $\mathbf{V}_j$. The following results first appeared in [43], where the operator exponential form (A7) was employed to explicitly evaluate operator logarithms.

Consider two arbitrary multimode Gaussian states, $\rho_1(\bar{\mathbf{x}}_1,\mathbf{V}_1)$ and $\rho_2(\bar{\mathbf{x}}_2,\mathbf{V}_2)$. Then, the entropic functional

$$\Sigma := -\mathrm{Tr}\left(\rho_1\log_2\rho_2\right) \tag{A25}$$

is given by [43, Theorem 7]

$$\Sigma(\mathbf{V}_1,\mathbf{V}_2,\delta) = \frac{1}{2\ln 2}\times \left[\ln\det\left(\kappa\mathbf{V}_2+\frac{i\Omega}{2}\right)+\kappa\mathrm{Tr}(\mathbf{V}_1\mathbf{G}_2)+\kappa\delta^T\mathbf{G}_2\delta\right], \tag{A26}$$

where $\delta := \bar{\mathbf{x}}_2 - \bar{\mathbf{x}}_1$ and $\mathbf{G}_j$ are the Gibbs matrices, obtained from the covariance matrices $\mathbf{V}_j$ from Eq. (A9).

From the above entropic functional, we may compute both the von Neumann entropy and the quantum relative entropy. Indeed, from (A26), the von Neumann entropy of a Gaussian state $\rho(\bar{\mathbf{x}},\mathbf{V})$ is equal to

$$S(\rho) := -\mathrm{Tr}\left(\rho\log_2\rho\right) = \Sigma(\mathbf{V},\mathbf{V},0) \ , \tag{A27}$$

The functional $\Sigma(\mathbf{V},\mathbf{V},0)$ is a symplectic invariant, namely $\Sigma(\mathbf{SVS}^T,\mathbf{SVS}^T,0) = \Sigma(\mathbf{V},\mathbf{V},0)$. As such, from the Williamson decomposition (A6) we find that $S(\rho)$ only depends on the symplectic eigenvalues v_j of $\mathbf{V}$, that can be written as

$$v_j = \frac{2\bar{n}_j+1}{2\kappa}, \tag{A28}$$

where $\bar{n}_j$ are the mean number of photons in each mode. The von Neumann entropy of an m-mode Gaussian state can then be expressed as [970]

$$S(\rho) = \sum_{j=1}^{m} h(\bar{n}_j), \tag{A29}$$

where $h(x) := (x+1)\log_2(x+1) - x\log_2 x$ as in Eq. (207).

The entropic functional of Eq. (A25) also provides a tool for writing the relative entropy between two arbitrary Gaussian states $\rho_1(\bar{\mathbf{x}}_1,\mathbf{V}_1)$ and $\rho_2(\bar{\mathbf{x}}_2,\mathbf{V}_2)$, in terms of their statistical moments. Indeed, we may write [43]

$$\begin{aligned} S(\rho_1||\rho_2) &:= \mathrm{Tr}\left[\rho_1(\log_2\rho_1 - \log_2\rho_2)\right] \\ &= -S(\rho_1) - \mathrm{Tr}\left(\rho_1\log_2\rho_2\right) \\ &= -\Sigma(\mathbf{V}_1,\mathbf{V}_1,0) + \Sigma(\mathbf{V}_1,\mathbf{V}_2,\delta) \ . \end{aligned} \tag{A30}$$

It is worth mentioning that the final result Eq. (A30) is expressed directly in terms of the statistical moments of the two Gaussian states. There is no need of resorting to full symplectic diagonalizations (A6) as in previous formulations [985, 986]. This is an advantage because, while the computation of the symplectic spectrum needed for the von Neumann entropy is easy to get, the symplectic matrix $\mathbf{S}$ performing such a symplectic diagonalization is known only in a few cases as for specific types of two-mode Gaussian states [974]. On the other hand, the invariant matrix formulation shown Eq. (A30) allows one

to bypass such complicate diagonalization and directly compute the quantum relative entropy.

Finally, we consider the quantum relative entropy variance

$$V_S(\rho_1\|\rho_2) = \mathrm{Tr}\left[\rho_1\left(\log_2\rho_1 - \log_2\rho_2 - S(\rho_1\|\rho_2)\right)^2\right]. \tag{A31}$$

The relative entropy variance was introduced in Ref. [987, 988] to bound the capacity of quantum channels and quantum hypothesis testing. Using the operator exponential form (A7) and the definitions (A9), one can show that, for any two Gaussian states ρ_1 and ρ_2, the variance $V_S(\rho_1\|\rho_2)$ can be written in terms of the states' first and second moments as

$$V_S(\rho_1\|\rho_2) = \frac{4\kappa^2\mathrm{Tr}[(\mathbf{V}_1\tilde{\mathbf{G}})^2] + \mathrm{Tr}[(\tilde{\mathbf{G}}\Omega)^2] + \delta^T\mathbf{B}\delta}{2(2\ln 2)^2}, \tag{A32}$$

where $\tilde{\mathbf{G}} = \mathbf{G}_1 - \mathbf{G}_2$, $\delta = \bar{\mathbf{x}}_1 - \bar{\mathbf{x}}_2$ and $\mathbf{B} = 8\kappa^2\mathbf{G}_2\mathbf{V}_1\mathbf{G}_2$. The above formula was first derived in Ref. [989] for $\kappa = 1$. It was then easily generalized to arbitrary κ in Ref. [736], where an alternative simplified proof was presented by exploiting a trace formula from Ref. [990].

Appendix B: Composable secret key rate of a CV-QKD protocol

Part of the following approach has been also presented in Ref. [539]. It combines various ingredients developed in Refs. [94, 109, 546, 614, 633, 991]. More precisely, it starts from the direct hash bound of Ref. [546, 991] and then uses ideas from Ref. [633] but where the error correction (EC) analysis is simplified according to the results in Ref. [94] (there developed for the specific case of CV-MDI-QKD, but implicitly applicable to more general cases). This combined approach leads to a simple formula for the composable secret key rate of a generic CV-QKD protocol under collective attacks. This formula is complete and computable when parameter estimation and finite-size effects are explicitly accounted for. This can be easily done when the collective attack is Gaussian [469], which is the optimal collective attack for many continuous-alphabet (Gaussian-modulated) CV-QKD protocols [488, 489], while it is a realistic assumption for discrete-alphabet CV-QKD protocols [539]. Finally, for Gaussian-modulated coherent-state protocols with suitable symmetries, one can extend the composable security to general collective attacks [93].

1. ϵ-security under collective attacks

Consider a generic CV-QKD protocol. After n uses, Alice and Bob aims at sharing the following ideal classical-quantum state

$$\rho_{\mathrm{id}} := 2^{-s}\sum_{z=0}^{2^{-s}-1} |z\rangle_{A^n}\langle z| \otimes |z\rangle_{B^n}\langle z| \otimes \rho_{\mathbf{E}^n}, \tag{B1}$$

where A^n is Alice's classical system, B^n is Bob's, and $\mathbf{E}^n$ is the total set of Eve's quantum systems. In particular, note that Eve's output state $\rho_{\mathbf{E}^n}$ must not depend on z, and s is the number of secret bits.

In reality, after a collective attack, all the parties (Alice, Bob and Eve) will get a classical-quantum output state of the form $\rho^{\otimes n}$ where

$$\rho = \sum_{k,l} p(k,l)\,|k\rangle_A\langle k| \otimes |l\rangle_B\langle l| \otimes \rho_{\mathbf{E}}(k,l), \tag{B2}$$

where the systems A, B and $\mathbf{E}$ refer to a single use of the protocol, and $p(k,l)$ is a joint probability distribution. There will be corresponding sequences k^n and l^n, for Alice and Bob, with probability $p(k^n,l^n)$. In a discrete-alphabet CV-QKD protocol, k^n and l^n are directly given by Alice's encoding and Bob's decoding, while for a continuous-alphabet (e.g., Gaussian modulated) CV-QKD protocol, these are discretized variables that are given by an analog-to-digital (ADC) conversion of the continuous variables, x^n and y^n, that are measured by the two parties. Assuming that each CV symbol x and y is encoded with d bits of precision, then their discretizations k and l are d-ary symbols (so that the sequences k^n and l^n have binary length nd).

Assume that Alice and Bob perform a classical protocol of EC, reconciliating over Bob's variable l (reverse reconciliation). During the process, a number of bits $\mathrm{leak}_{\mathrm{EC}}$ are publicly revealed to Eve who stored them in a register R with dimension $d_R = 2^{\mathrm{leak}_{\mathrm{EC}}}$. In a practical scheme, Bob reveals $\mathrm{leak}_{\mathrm{EC}}$ bits of information corresponding to the syndrome computed over its sequence l^n, which is interpreted as the noisy codeword of a linear EC code (agreed with Alice). Using this syndrome and her local data k^n, Alice infers a guess $\tilde{l}^n$ of Bob's sequence l^n. Then, Bob computes a hash of l^n of length $\leq 1-\log_2\epsilon_{\mathrm{cor}}$ which is sent to Alice (for a suitable ϵ_{cor}). She compares Bob's hash with the one computed from her guess: in case they are different the protocol is aborted (see also Ref. [633]). Here ϵ_{cor} is the ϵ-correctness, i.e., the conditional probability that Alice's and Bob's sequences are different even though their hashes are the same. Then, let us denote by $p_\perp$ the probability of abortion (occuring for two different hashes). The overall probability that $\tilde{l}^n$ is different from l^n is given by $(1-p_\perp)\epsilon_{\mathrm{cor}}$ and the protocol is correspondingly called ϵ_{cor}-correct [109, Sec. 4.3].

The successful implementation of the EC protocol can be represented as a projection $\Pi_{\mathcal{S}}$ of Alice's and Bob's classical (orthogonal) states onto a "good" set $\mathcal{S}$ of sequences $\{k^n,l^n\}$ [94, 633]. In other words, we may write

$$\Pi_{\mathcal{S}} := \sum_{\{k^n,l^n\}\in\mathcal{S}} |k^n\rangle_{A^n}\langle k^n| \otimes |l^n\rangle_{B^n}\langle l^n| \otimes I_{\mathbf{E}^n}. \tag{B3}$$

With success probability $p := \mathrm{Tr}(\Pi_{\mathcal{S}}\rho^{\otimes n}) = 1 - p_{\perp}$, this generates the classical-quantum state

$$\tilde{\rho}^n := p^{-1}\ \Pi_{\mathcal{S}}\rho^{\otimes n}\Pi_{\mathcal{S}}, \tag{B4}$$

which is no longer in a tensor-product structure.

After EC, there is the step of privacy amplification (PA), where a randomly-chosen two-way hash function f transforms the error-corrected state $\tilde{\rho}^n$ into a privacy-amplified state $\bar{\rho}^n$ close to the ideal private state ρ_{id}, so that the overall process is

$$\rho^{\otimes n} \xrightarrow{\mathrm{EC}} \tilde{\rho}^n \xrightarrow{\mathrm{PA}} \bar{\rho}^n \simeq \rho_{\mathrm{id}}. \tag{B5}$$

The closeness between $\bar{\rho}^n$ and ρ_{id} is the condition of ϵ-secrecy, expressed by $(1-p_{\perp})D(\bar{\rho}^n, \rho_{\mathrm{id}}) \leq \epsilon_{\mathrm{sec}}$, where D is the trace distance [109, Sec. 4.3]. By using the triangle inequality, it is easy to show that [109, Th. 4.1]

$$D(\tilde{\rho}^n, \rho_{\mathrm{id}}) \leq \epsilon := \epsilon_{\mathrm{cor}} + \epsilon_{\mathrm{sec}}, \tag{B6}$$

and the protocol is said to be ϵ-secure.

Call s_n the bits of shared uniform randomness that are extracted from $\tilde{\rho}^n$ by the two-universal hashing protocol (number of shared classical bits in $\bar{\rho}^n$). This quantity satisfies the following direct leftover hash bound [991, Th. 6]

$$s_n \geq H_{\min}^{\epsilon_{\mathrm{s}}}(l^n|\mathbf{E}^n)_{\tilde{\rho}^n} + 2\log_2 2\epsilon_{\mathrm{h}}, \tag{B7}$$

where $H_{\min}^{\epsilon_{\mathrm{s}}}(l^n|\mathbf{E}^n)_{\tilde{\rho}^n}$ is the smooth min-entropy of Bob's sequence l^n conditioned on Eve's quantum systems $\mathbf{E}^n$, globally described by the error-corrected state $\tilde{\rho}^n$. In particular, the smothing parameter ϵ_{s} and the hashing parameter ϵ_{h} are such that $\epsilon_{\mathrm{sec}} = \epsilon_{\mathrm{s}} + \epsilon_{\mathrm{h}}$.

Various observations are now in order. First of all, after the EC procedure, Eve's systems can be decomposed as $\mathbf{E}^n = E^n R$ where E^n are the systems using during the attack, and R is the register used to store Alice and Bob's public communication with dimension $d_R = 2^{\mathrm{leak}_{\mathrm{EC}}}$. We can subtract the contribution of the register by using the chain rule for the smooth-min entropy, so that

$$H_{\min}^{\epsilon_{\mathrm{s}}}(l^n|\mathbf{E}^n)_{\tilde{\rho}^n} \geq H_{\min}^{\epsilon_{\mathrm{s}}}(l^n|E^n)_{\tilde{\rho}^n} - \log_2 d_R, \tag{B8}$$

and, therefore, we may write

$$s_n \geq H_{\min}^{\epsilon_{\mathrm{s}}}(l^n|E^n)_{\tilde{\rho}^n} + 2\log_2 2\epsilon_{\mathrm{h}} - \mathrm{leak}_{\mathrm{EC}}. \tag{B9}$$

Second, we can use Ref. [94, Prop. 6] which relates the smooth-min entropy of $\tilde{\rho}^n$ (after EC) to that of $\rho^{\otimes n}$ (before EC), i.e., we may write

$$\begin{aligned} H_{\min}^{\epsilon_{\mathrm{s}}}(l^n|E^n)_{\tilde{\rho}^n} \geq\ & H_{\min}^{\frac{2}{3}p\epsilon_{\mathrm{s}}}(l^n|E^n)_{\rho^{\otimes n}} \\ & + \log_2[p\,(1-2\epsilon_{\mathrm{s}}/3)]. \end{aligned} \tag{B10}$$

Third, we can relate the smooth-min entropy computed over $\rho^{\otimes n}$ to the conditional von-Neumann entropy $H(l|E)$ computed over the single-copy state ρ where E is the system used by Eve in her attack. In fact, according to Ref. [546, Cor. 6.5], we may write the asymptotic equipartition property (AEP)

$$\begin{aligned} H_{\min}^{\frac{2}{3}p\epsilon_{\mathrm{s}}}(l^n|E^n)_{\rho^{\otimes n}} \geq\ & nH(l|E)_{\rho} \\ & - \sqrt{n}\Delta_{\mathrm{AEP}}\left(\frac{2}{3}p\epsilon_{\mathrm{s}}, d\right), \end{aligned} \tag{B11}$$

where

$$\Delta_{\mathrm{AEP}}(\epsilon_{\mathrm{s}}, d) := 4\log_2\left(2\sqrt{d}+1\right)\sqrt{\log(2/\epsilon_{\mathrm{s}}^2)}, \tag{B12}$$

with d being the dimension/cardinality of Bob's alphabet (number of possible values of l). Note that the expression in Eq. (B12) for the AEP [614] can be derived from Ref. [546, Result 5] by bounding the max-entropies therein with the log of the dimension of Bob's key system (alphabet).

Combining Eqs. (B9), (B10) and (B11), we write the bound

$$\begin{aligned} s_n \geq\ & nH(l|E)_{\rho} - \sqrt{n}\Delta_{\mathrm{AEP}}\left(\frac{2}{3}p\epsilon_{\mathrm{s}}, d\right) \\ & + \log_2[p\,(1-2\epsilon_{\mathrm{s}}/3)] + 2\log_2 2\epsilon_{\mathrm{h}} - \mathrm{leak}_{\mathrm{EC}}. \end{aligned} \tag{B13}$$

This can be further simplified by recalling one of the definitions of the quantum mutual information $I(Q:E) = S(Q) - S(Q|E)$ and the fact that, when first system is classical $Q = l$, then the von Neumann entropy $S(Q)$ is its Shannon entropy $H(l)$, and $I(Q:E)$ becomes the Holevo information $I(l:E)$ [704]. Therefore, we may write

$$H(l|E)_{\rho} = H(l) - \chi(l:E)_{\rho}. \tag{B14}$$

Another simplification is to perform the replacement

$$H(l) - n^{-1}\mathrm{leak}_{\mathrm{EC}} = \xi I(k:l), \tag{B15}$$

where $\xi \in [0,1]$ is a reconciliation parameter and $I(k:l)$ is the classical mutual information between Alice's and Bob's variables. In this way, the asymptotic rate

$$R_{\infty} = \xi I(k:l) - \chi(l:E)_{\rho} \tag{B16}$$

appears in the formula when we replace Eqs. (B14) and (B15) into Eq. (B13). In fact, we may write

$$\begin{aligned} s_n \geq\ & nR_{\infty} - \sqrt{n}\Delta_{\mathrm{AEP}}\left(\frac{2}{3}p\epsilon_{\mathrm{s}}, d\right) \\ & + \log_2[p\,(1-2\epsilon_{\mathrm{s}}/3)] + 2\log_2 2\epsilon_{\mathrm{h}}, \end{aligned} \tag{B17}$$

which refers to a protocol with epsilon security $\epsilon = \epsilon_{\mathrm{cor}} + \epsilon_{\mathrm{s}} + \epsilon_{\mathrm{h}}$ and success probability p. Typically, the epsilons can be chosen to be very small (of the order of 10^{-20} or less), while the abort probability $p_{\perp} = 1-p$ is connected to the experimental frame error rate (see Ref. [595] for typical values).

2. Parameter estimation

The remaining step is to account for parameter estimation (PE) which can be done after EC. Alice compares her data k^n with the inferred sequence $\tilde{l}^n$ of Bob. In this way, she can estimate the parameters $\mathbf{t} = \{t_1, t_2, \ldots\}$ of the noisy communication channel (or the statistical moments of their distributed data). In a typical procedure of PE, Alice and Bob compute worst-case values $\mathbf{t}_{\rm wc}$ for the parameters $\mathbf{t}$ in such a way that they minimize the asymptotic rate $R_\infty(\mathbf{t})$ within some confidence intervals. Such a procedure is certainly possible if the collective attack is Gaussian [469]. In particular, if the communication channel is a thermal-loss channel with transmissivity η and thermal noise ω, one can derive maximum likelihood estimators for η and ω, and replace worst-case values of them according to 6.5 confidence intervals [488, 489, 539].

By choosing the worst-case values $\mathbf{t}_{\rm wc}$, Alice and Bob implicitly assume a worst-case state $\tilde{\rho}^n_{\rm wc}$ for the global output $\tilde{\rho}^n$ of Alice-Bob-Eve after EC. Assuming this worst-case state, we can repeat the previous steps starting from $\tilde{\rho}^n_{\rm wc}$ which will be ϵ-close to an ideal private state $\rho_{\rm id}$ whose number of secret bits s_n is now bounded by Eq. (B17) up to the replacement $R_\infty \to R_{\rm PE} := R_\infty(\mathbf{t}_{\rm wc})$.

However, it is important to note that also PE may be affected by errors. Call $\epsilon_{\rm PE}$ the overall error probability that the actual values of the channel parameters $\mathbf{t}$ are worse than $\mathbf{t}_{\rm wc}$ (e.g., that $\eta < \eta_{\rm wc}$ and $\omega > \omega_{\rm wc}$ for a thermal-loss channel). This means that there may be a different state $\tilde{\rho}^n_{\rm bad}$ which gives a lower rate than $\tilde{\rho}^n_{\rm wc}$. In order to account for this error, consider the average state $\rho_{\rm PE} := (1-\epsilon_{\rm PE})\tilde{\rho}^n_{\rm wc} + \epsilon_{\rm PE}\tilde{\rho}^n_{\rm bad}$ whose trace distance from $\tilde{\rho}^n_{\rm wc}$ is $D(\rho_{\rm PE}, \tilde{\rho}^n_{\rm wc}) = \epsilon_{\rm PE}$. Now, using $D(\tilde{\rho}^n_{\rm wc}, \rho_{\rm id}) \leq \epsilon$ and the triangle inequality, we may compute the trace distance from the ideal state

$$D(\rho_{\rm PE}, \rho_{\rm id}) \leq \epsilon + \epsilon_{\rm PE}. \tag{B18}$$

Therefore, the average state $\rho_{\rm PE}$ is $(\epsilon + \epsilon_{\rm PE})$-close to an ideal state $\rho_{\rm id}$ whose number of secret bits s_n is lower-bounded as in Eq. (B17) with the $R_\infty \to R_{\rm PE}$.

By making this replacement in Eq. (B17) and dividing by n, we derive the following bound for the composable secret key rate (bits per use) of a generic CV-QKD protocol under collective attacks

$$\begin{aligned} R_n := \frac{s_n}{n} \geq R_{\rm PE} &- \frac{1}{\sqrt{n}}\Delta_{\rm AEP}\left(\frac{2}{3}p\epsilon_{\rm s}, d\right) \\ &+ n^{-1}\left\{\log_2[p\,(1-2\epsilon_{\rm s}/3)] + 2\log_2 2\epsilon_{\rm h}\right\}. \end{aligned} \tag{B19}$$

This is valid for a protocol with overall epsilon security

$$\epsilon \to \epsilon + \epsilon_{\rm PE} = \epsilon_{\rm cor} + \epsilon_{\rm s} + \epsilon_{\rm h} + \epsilon_{\rm PE}. \tag{B20}$$

Using Eq. (B19), we can certainly compute the composable key rate for a generic CV-QKD protocol under collective Gaussian attacks. For instance, this is the approach followed by Ref. [539], which considered a discrete-alphabet CV-QKD protocol and, more precisely, a phase-shift keying protocol with d possible phases. In the case of a Gaussian-modulated QKD protocol, the variables k and l comes from ADC with d bits of precision, applied to continuous variables x and y (for instance, this is the case for the switching protocol [462], where only one quadrature is agreed per use of the channel). Assuming collective Gaussian attacks, one can compute $R_{\rm PE}$ (e.g., see Refs. [488, 489]) and again use Eq. (B19). Furthermore, using the fact that ADC cannot increase Eve's Holevo bound and the fact that Gaussian states are extremal, we can consider the replacement

$$\chi(l:E)_\rho \leq \chi(y:E)_\rho \leq \chi(y:E)_{\rho_{\rm G}} \tag{B21}$$

so that Eve's Holevo information is directly computed from Bob's CV outcome y of the homodyne detector, and we may assume that Bob and Eve's joint state is Gaussian $\rho_{\rm G}$. Also note that we can assume $I(k:l) \simeq I(x:y)$ for high values of d in the ADC process.

Finally, the formula of the key rate in Eq. (B19) can be extended to CV-MDI-QKD. The main difference with respect to a standard one-way protocol is that the output state (under collective attacks) is now conditioned to the outcome γ of the Bell measurement at the untrusted relay station, i.e., we have $\rho^{\otimes n} := \rho^{\otimes n}_{AB\mathbf{E}} \to \rho^{\otimes n}_{|\gamma} := \rho^{\otimes n}_{AB\mathbf{E}|\gamma}$. One can repeat the previous steps and derive the formula of Eq. (B19) up to the replacement $R_{\rm PE} \to R_{{\rm PE}|\gamma}$ which is the finite-size rate associated to the conditional asymptotic rate

$$R_{\infty|\gamma} = \xi I(k:l|\gamma) - \chi(l:E)_{\rho_{|\gamma}}. \tag{B22}$$

Assuming collective Gaussian attacks, the calculation of $R_{{\rm PE}|\gamma}$ is performed using the same technique for standard one-way protocols (estimators and confidence intervals).

Let us discuss more the crucial procedure of PE. Above we have considered the case where this is done after EC. To be precise, even in this case, a very small session of PE is anyway needed before EC, because Alice and Bob needs to have a rough estimate of the loss and noise in order to apply the best possible error correcting codes. The amount of data to be disclosed (and discarded) for this operation can however be considered to be negligible.

Another option is to perform PE before EC, which means that Alice and Bob need to sacrifice a non-trivial part of their data. In fact, in this case they publicly disclose the variables in $m_{\rm PE}$ randomly-chosen uses of the protocol, so that they can reconstruct the channel parameters or the statistical moments of the shared probability distribution. The number of uses which are employed for key generation will be now reduced from n to $n-m$. In this case, the previous theory can be modified to give the following rate

$$\begin{aligned} R_n := \frac{s_{n-m_{\rm PE}}}{n} \geq \frac{n-m_{\rm PE}}{n}R_{\rm PE} &- \frac{\sqrt{n-m_{\rm PE}}}{n}\Delta_{\rm AEP}\left(\frac{2}{3}p\epsilon_{\rm s}, d\right) \\ &+ n^{-1}\left\{\log_2[p\,(1-2\epsilon_{\rm s}/3)] + 2\log_2 2\epsilon_{\rm h}\right\}. \end{aligned} \tag{B23}$$

3. Extension to coherent attacks

Finally, let us discuss the extension of the security to general coherent attacks, following the approach in Ref. [93]. Suppose that a CV-QKD coherent-state based protocol is ϵ-secure with rate R_n under collective Gaussian attacks and it is also symmetric (or suitably symmetrized) with respect to a Fock-space representation G of the group $U(n)$ of $n \times n$ unitary matrices [93]. Then, the protocol is also ϵ'-secure under coherent attacks, with $\epsilon' = K^4\epsilon/50$ where

$$K = \max\left\{1, n(d_A + d_B)\frac{1 + 2\sqrt{\frac{\ln(8/\epsilon)}{2n}} + \frac{\ln(8/\epsilon)}{n}}{1 - 2\sqrt{\frac{\ln(8/\epsilon)}{2m_{\mathrm{ET}}}}}\right\}, \tag{B24}$$

with m_{ET} being the number of signals sacrificed in a suitable energy test [93], and d_A (d_B) being Alice's (Bob's) effective local dimension.

Correspondingly, the secret key rate will be lowered by a quantity equal to $\frac{2}{n}\log_2\binom{K+4}{4}$. This means the secret key rate in Eq. (B23) will be modified into the following form

$$\begin{aligned} R_n \geq\ & \frac{n-m}{n}R_{\mathrm{PE}} - \frac{\sqrt{n-m}}{n}\Delta_{\mathrm{AEP}}\left(\frac{2}{3}p\epsilon_{\mathrm{s}}, d\right) \\ & + n^{-1}\left\{\log_2[p\,(1-2\epsilon_{\mathrm{s}}/3)] + 2\log_2 2\epsilon_{\mathrm{h}}\right\} \\ & - \frac{2}{n}\log_2\binom{K+4}{4}, \end{aligned} \tag{B25}$$

where $m := m_{\mathrm{PE}} + m_{\mathrm{ET}}$. Note that the parameter K scales linearly as $K \simeq n(d_A + d_B)$, so that the overhead in the security parameter is only polynomial in the total number n of uses. Also note that the formula in Eq. (B25) can be applied to CV-MDI-QKD (up to symmetrization of the protocol) by replacing R_{PE} with $R_{\mathrm{PE}|\gamma}$, which is the finite-size version of the asymptotic rate in Eq. (B22) under collective Gaussian attacks.

Appendix C: List of commonly-used symbols and some acronyms

Quantity	Symbol(s)
Classical variables/systems	α, β, x, y, X, Y
Quantum variables/systems	A, B, E, a_1, b_1, $\mathbf{a}$, $\mathbf{b}$
Probability	p, $P(\alpha)$
Identity operator	σ_0, $\mathbb{1}$, $\mathbb{1}_n$
Identity matrix, identity channel (map)	$\mathbf{I}$, $\mathcal{I}$
Pauli operators	σ_i with $i = 1, 2, 3$ (or x, y, z), X, Y, Z
Bases	X, Y, Z, rect, diag
Quadratures	$\hat{q}$, $\hat{p}$, $\hat{\mathbf{x}}$
Quantum states	ρ, σ, $\|\varphi\rangle$...
Sequences of states	Φ^μ, $\tilde{\gamma}^\mu$
Choi states, asymptotic Choi states	$\sigma_\mathcal{E}$, $\sigma_\mathcal{E}^\mu$
Covariance matrix, mean value	$\mathbf{V}$, $\bar{\mathbf{x}}$
Quantum channels	$\mathcal{E}$, $\mathcal{E}_p$, $\mathcal{E}_\eta$, $\mathcal{E}_{\eta,\bar{n}}$, $\mathcal{E}_{g,\bar{n}}$, ...
Shannon entropy, binary Shannon entropy	$H(X)$, $H_2(X)$
von Neumann entropy	$S(AB)$, $S(\rho_{AB})$, $H(B)$
Conditional von Neumann entropy	$S(B\|\alpha)$, $H(B\|X)$
Relative entropy	$S(\rho\|\|\sigma)$
Smooth min entropy	$H_{\min}^\epsilon$, $S_{\min}$
Mutual information	I_{AB}, $I(\alpha:\beta)$, $I(X:Y)$
Accessible information	I_{acc}
Coherent information, reverse coherent information	I_C, I_{RC}
Holevo bound	χ_E, χ_{AE}, $\chi(\alpha:E)$, $I(\alpha:E)$
Direct, reverse reconciliation	$\blacktriangleright$, $\blacktriangleleft$
Rate	R, $R^\blacktriangleright$, $R^\blacktriangleleft$
QBER	D, E, E_μ, e, e_1, e_b, e_p
Relative entropy of entanglement	E_{R}
Generic 2-way capacity of $\mathcal{E}$	$\mathcal{C}(\mathcal{E})$
Secret key capacity of $\mathcal{E}$	$K(\mathcal{E})$
2-way quantum, entanglement distribution capacity	$Q_2(\mathcal{E})$, $D_2(\mathcal{E})$

Acronym	Meaning
AEP	asymptotic equipartition property
AOPP	active odd-parity pair
APD	avalanche photon detection/avalanche photodiodes
BK	Braunstein-Kimble
BQC	blind quantum computing
BQSM	bounded quantum storage model
BS	beam-splitter
BSM	Bell-state measurement
CC(s)	classical communication(s)
CFS	Courtois-Finiasz-Sendrier
CHSH	Clauser-Horne-Shimony-Holt
CI	coherent information
CM	control mode
CM(s)	covariance matrix (matrices)
COW	coherent-one-way
CSS	Calderbank-Shor-Steane
CV(s)	continuous variable(s)
CW	continuous wave
DAD	diagonal amplitude damping
DCNOT	double CNOT
DEM	detector efficiency mismatch
DI	device independent
DLCZ	Duan-Lukin-Cirac-Zoller
DMD	digital micro-mirror device
DPS	differential phase shift
DQPS	differential quadrature phase shift
DR	direct reconciliation
DSA	digital signature algorithm
DSP	digital signature processing
DV(s)	discrete variable(s)
EAT	entropy accumulation theorem
EC	error correction
ECD	energy-constrained diamond
ED	entanglement distribution
EDP	entanglement distillation protocol
EM	encoding mode
EPR	Einstein-Podolsky-Rosen
EUR(s)	entropic uncertainty relation(s)
GC-QDS	Gottesman-Chuang QDS
GEO	geostationary orbit
GHZ	Greenberger-Horne-Zeilinger
GLLP	Gottesman-Lo-Lütkenhaus-Preskill
GKP	Gottesman-Preskill-Kitaev
GNSS	Global Navigation Satellite Systems
HD	high-dimensional
i.i.d	independent and identically distributed
ISS	International Space Station
ITS	information-theoretic security
KG	key generation
LDPC	low density parity check
LEO	low Earth orbit
LIDT	laser induced damage threshold
LLM	line length measurement
LO	local oscillator

Acronym	Meaning
LOCCs	local operation(s) and classical communication
LWE	learning-with-errors
MDI	measurement device independent
MEMS	micro-electro-mechanical system(s)
MEO	medium Earth orbit
MLRO	Matera Laser Ranging Observatory
MUB(s)	mutually unbiased basis (bases)
MZI	Mach-Zehnder interferometer
NIST	National Institute of Standards and Technology
NLA(s)	noiseless linear amplifier(s)
NPPTF	no-phase-postselected TF
OAM	orbital angular momentum
OPLL	optical phase-locked loop
PA	privacy amplification
PBS	polarising beam splitter
PIC(s)	photonic integrated circuit(s)
PLOB	Pirandola-Laurenza-Ottaviani-Banchi
PM	phase matching
PNS	photon-number splitting
POVM	positive-operator valued measurement
PPKTP	periodically-poled potassium titanyl phosphate
PR-box	Popescu-Rohrlich-box
QBER	quantum bit error rate
QC	quantum communication
QCM(s)	quantum cloning machine(s)
QCSE	quantum-confined Stark effect
QEC	quantum error correction/correcting
QDL	quantum data locking
QDS	quantum digital signature
QEM	quantum enigma machine
QKD	quantum key distribution
QPSK	quadrature phase shift keying
QRE	quantum randomness expansion
QRNG(s)	quantum RNG(s)
RCI	reverse coherent information
REE	relative entropy of entanglement
RNG(s)	random number generator(s)
RR	reverse reconciliation
RSA	Rivest-Shamir-Adleman
SFWM	spontaneous four-wave mixing
SHA	secure hash algorithm
SLM	spatial light modulator
SNR	signal-to-noise ratio
SNS	sending or not sending
SNSPD(s)	superconducting nanowire single photon detector(s)
SNU	shot noise unit
SVP	shortest vector problem
TF	twin field
THA	Trojan horse attack
TMSV	two-mode squeezed vacuum
UD	unidimensional
USD	unambiguous state discrimination
USS	unconditionally secure digital signatures
VOA	variable optical attenuator

[1] M. A. Nielsen, and I. L. Chuang, "Quantum computation and quantum information," (Cambridge University Press, Cambridge, 2000).

[2] A. Holevo, "Quantum Systems, Channels, Information: A Mathematical Introduction," (De Gruyter, Berlin-Boston, 2012).

[3] I. Bengtsson and K. Życzkowski, "Geometry of quantum states: An Introduction to Quantum Entanglement," (Cambridge University Press, Cambridge 2006).

[4] M. Hayashi, "Quantum Information Theory: Mathematical Foundation," (Springer-Verlag, Berlin, 2017).

[5] J. Watrous, "The theory of quantum information," (Cambridge University Press, Cambridge, 2018).

[6] M. Tomamichel, "Quantum Information Processing with Finite Resources - Mathematical Foundations," (Springer International Publishing, 2016), Vol. 5.

[7] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," Rev. Mod. Phys. **84**, 621 (2012).

[8] S. L. Braunstein, and P. Van Loock, "Quantum information with continuous variables," Rev. Mod. Phys. **77**, 513 (2005).

[9] R. Van Meter, "Quantum Networking," John Wiley & Sons, Wiley (2014).

[10] G. Adesso, S. Ragy, and A. R. Lee, "Continuous Variable Quantum Information: Gaussian States and Beyond," Open Syst. Inf. Dyn. **21**, 1440001 (2014).

[11] A. Serafini, "Quantum Continuous Variables: A Primer of Theoretical Methods," (Taylor & Francis, Oxford, 2017).

[12] U. L. Andersen, J. S. Neergaard-Nielsen, P. van Loock, and A. Furusawa, "Hybrid quantum information processing," Nat. Phys. **11**, 713–719 (2015)

[13] G. Kurizki, P. Bertet, Y Kubo, K. Mølmer, D. Petrosyan, P. Rabl, J. Schmiedmayer, "Quantum technologies with hybrid systems," Proc. Natl. Acad. Sci. USA **112**, 3866-73 (2015).

[14] S. Barnett, "Quantum Information," (Oxford University Press, 2009)

[15] B. Schumacher, and M. Westmoreland, "Quantum Processes Systems, and Information," (Cambridge University Press, Cambridge, 2010).

[16] D. Bouwmeester, "The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation," (Springer-Verlag, Berlin, 2000).

[17] M. M. Wilde, "Quantum Information Theory," (Cambridge University Press, Cambridge 2013).

[18] C. A. Fuchs, "Coming of Age With Quantum Information: Notes on a Paulian Idea," (Cambridge University Press, Cambridge, 2011).

[19] D. Mermin, "Quantum Computer Science: An Introduction," (Cambridge University Press, Cambridge 2007).

[20] V. Vedral, "Introduction to Quantum Information Science," (Oxford University Press, 2006).

[21] G. Benenti, G. Casati, and D. Rossini "Principles of Quantum Computation and Information: A Comprehensive Textbook," (World Scientific Publishing, Singapore, 2019).

[22] J. Lars, "The Second Quantum Revolution: From Entanglement to Quantum Computing and Other Super-Technologies," (Springer International Publishing, 2018).

[23] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, "Quantum entanglement," Rev. Mod. Phys. **81**, 865 (2009).

[24] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," Phys. Rev. Lett. **70**, 1895 (1993).

[25] S. L. Braunstein and H. J. Kimble, "Teleportation of Continuous Quantum Variables," Phys. Rev. Lett. **80**, 869–872 (1998).

[26] S. L. Braunstein, G. M. D'Ariano, G. J. Milburn, and M. F. Sacchi, "Universal Teleportation with a Twist," Phys. Rev. Lett. **84**, 3486 (2000).

[27] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, "Advances in Quantum Teleportation," Nature Photonics **9**, 641-652 (2015).

[28] W. Wootters, W. Zurek, "A Single quantum cannot be cloned," Nature **299**, 802 (1982).

[29] J. Park, "The concept of transition in quantum mechanics," Found. Phys. **1**, 23 (1970).

[30] R. J. Schoelkopf and S. M Girvin, "Wiring up quantum systems," Nature **451**, 664 (2008).

[31] P.W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, Nov. 20-22 (1994).

[32] P.W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM J. Comput., **26**, 1484 (1997).

[33] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM', **21**, 120 (1978).

[34] M. Agrawal, N. Kayal, N. Saxena, "Primes is in P," Annals of Mathematics **160**, 781-793 (2004).

[35] M. Mosca, "Setting the Scene for the ETSI Quantum-safe Cryptography Workshop," e-proceedings of 1st Quantum-Safe-Crypto Workshop, Sophia Antipolis, 26-27 September (2013).

[36] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography," Rev. Mod. Phys. **74**, 145 (2002).

[37] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The Security of Practical Quantum Key Distribution," Rev. Mod. Phys. **81**, 1301 (2009).

[38] E. Diamanti and A. Leverrier, "Distributing Secret Keys with Quantum Continuous Variables: Principle, Security and Implementations," Entropy **17**, 6072 (2015).

[39] E, Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," npj Quantum Information **2**, 16025 (2016).

[40] A. Shenoy-Hejamadi, A. Pathak, and S. Radhakrishna, "Quantum Cryptography: Key Distribution and Beyond," Quanta **6**, 1-147 (2017).

[41] D. Mayers and A. Yao, "Quantum Cryptography with

Imperfect Apparatus," Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS-98), IEEE Computer Society, 503 (1998). See also arXiv:quant-ph/9809039.

[42] J. Barrett, L. Hardy, and A. Kent, "No Signaling and Quantum Key Distribution," Phys. Rev. Lett. **95**, 010503 (2005).

[43] S. Pirandola, R. Laurenza, C. Ottaviani and L. Banchi, "Fundamental Limits of Repeaterless Quantum Communications," Nature Comm. **8**, 15043 (2017). See also arXiv:1510.08863 (2015).

[44] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, "Direct and Reverse Secret-Key Capacities of a Quantum Channel," Phys. Rev. Lett. **102**, 050503 (2009).

[45] E. Chip, "Building the quantum network," New J. Phys. **4**, 46 (2002).

[46] E. Chip, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA Quantum Network," Defense and Security, International Society for Optics and Photonics, pp. 138-149 (2005).

[47] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, et al. "The SECOQC quantum key distribution network in Vienna," New J. Phys. **11**, 075001 (2009).

[48] F. Xu, W. Chen, S. Wang, Z. Yin, Y. Zhang, Y. Liu, Z. Zhou, Y. Zaho, H. Li, D. Liu, Z. Han, G. Cuo, "Field experiment on a robust hierarchical metropolitan quantum cryptography network," Chin. Sci. Bull. **54**, 2991-2997 (2009).

[49] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, et al., "Field test of quantum key distribution in the Tokyo QKD Network," Opt. Express **19**, 10387-10409 (2011).

[50] https://spectrum.ieee.org/telecom/security/chinas-2000km-quantum-link-is-almost-complete (accessed 26/9/2019).

[51] https://eandt.theiet.org/content/articles/2019/03/ultra-secure-quantum-connection-tests-begin-over-uk-network/ (accessed 26/9/2019).

[52] S. L. Braunstein and S. Pirandola, "Side-Channel-Free Quantum Key Distribution," Phys. Rev. Lett. **108**, 130502 (2012).

[53] H.-K. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent Quantum Key Distribution," Phys. Rev. Lett. **108**, 130503 (2012).

[54] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," Nature **557**, 400 (2018).

[55] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication," Phys. Rev. Lett. **81**, 5932 (1998).

[56] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, "Quantum repeaters based on entanglement purification," Phys. Rev. A **59**, 169 (1999).

[57] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," Nature 414, 413 (2001).

[58] S. Pirandola, "Capacities of repeater-assisted quantum communications," Preprint arXiv:1601.00966 (2016).

[59] S. Pirandola, "End-to-end capacities of a quantum communication network," Commun. Phys. **2**, 51 (2019).

[60] S. Pirandola, "Bounds for multi-end communication over quantum networks," Quantum Sci. Technol. **4**, 045006 (2019).

[61] M. Epping, H. Kampermann, and D. Bruß, "Large-scale quantum networks based on graphs," New J. Phys. **18**, 053036 (2016).

[62] M. Epping, H. Kampermann, and D. Bruß, "Robust entanglement distribution via quantum network coding," New J. Phys. **18**, 103052 (2016).

[63] K. Azuma, A. Mizutani, and H.-K. Lo, "Fundamental rate-loss trade-off for the quantum internet," Nat. Commun. **7**, 13523 (2016).

[64] K. Azuma and G Kato, "Aggregating quantum repeaters for the quantum internet," Phys. Rev. A **96**, 032332 (2017).

[65] T. P. W. Cope, K. Goodenough, and S. Pirandola, "Converse bounds for quantum and private communication over Holevo-Werner channels," J. Phys. A: Math. Theor. **51**, 494001 (2018).

[66] L. Rigovacca, G. Kato, S. Bäuml, M. S. Kim, W. J. Munro, and K. Azuma, "Versatile relative entropy bounds for quantum networks," New J. Phys. **20**, 013033 (2018).

[67] M. Pant, H. Krovi, D. Towsley, L. Tassiulas, L. Jiang, P. Basu, D. Englund, and S. Guha, "Routing entanglement in the quantum internet," npj Quantum Information **5**, 25 (2019).

[68] S. Bäuml, K. Azuma, G. Kato, and D. Elkouss, "Linear programs for entanglement and key distribution in the quantum internet," Preprint arXiv:1809.03120 (2018).

[69] S. Guha, H. Krovi, C. A. Fuchs, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel, "Rate-loss analysis of an efficient quantum repeater architecture," Phys. Rev. A **92**, 022357 (2015).

[70] M. Pant, H. Krovi, D. Englund, and S. Guha, "Rate-distance tradeoff and resource costs for all-optical quantum repeaters," Phys. Rev. A **95**, 012304 (2017).

[71] A. Khalique and B. C. Sanders, "Long-distance quantum key distribution using concatenated entanglement swapping with practical resources," Opt. Eng. **56**, 016114 (2017).

[72] J. Z. Bernád, "Hybrid quantum repeater based on resonant qubit-field interactions," Phys. Rev. A **96**, 052329 (2017).

[73] T. Holz, H. Kampermann, and D. Bruß, "Device-independent secret-key-rate analysis for quantum repeaters,"Phys. Rev. A **97**, 012337 (2018).

[74] M. Zwerger, A. Pirker, V. Dunjko, H.J. Briegel and W. Dür, Long-Range Big Quantum-Data Transmission, Phys. Rev. Lett. **120**, 030503 (2018).

[75] J. Wallnöfer, A. Pirker, M. Zwerger and W. Dür, "Multipartite state generation in quantum networks with optimal scaling," Sci. Rep. **9**, 314 (2019).

[76] D. Miller, T. Holz, H. Kampermann, D. Bruß, "Parameter regimes for surpassing the PLOB bound with error-corrected qudit repeaters," preprint arXiv:1906.05172 (2019).

[77] G. Vardoyan, S. Guha, P. Nain, and D. Towsley, "On the Stochastic Analysis of a Quantum Entanglement Switch," preprint arxiv:1903.04420 (2019).

[78] S. Pirandola, "General upper bounds for distributing conferencing keys in arbitrary quantum networks,"

Preprint arXiv:1912.11355 (2019).
[79] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, and W.-Y. Liu et al., "Satellite-Relayed Intercontinental Quantum Network," Phys. Rev. Lett. **120**, 030501 (2018).
[80] P. Ball, "Focus: Intercontinental, Quantum-Encrypted Messaging and Video," Physics **11**, 7 (2018). Available at https://physics.aps.org/articles/v11/7
[81] T. M. Cover and J. A. Thomas, "Elements of Information Theory," 2nd Ed., Wiley Series in Telecommunications and Signal Processing, Wiley, New York (1996).
[82] I. Csiszar and J. Korner, "Information Theory: Coding Theorems for Discrete Memoryless Systems," Akademiai Kiado: 2nd edition, (1997).
[83] A. Holevo, "Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel," Probl. Peredachi Inf. **9**, 3-11 (1973).
[84] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," Proc. R. Soc. A **461**, 207 (2005).
[85] R. Renner, "Symmetry of large physical systems implies independence of subsystems," Nat. Phys. **3**, 645 (2007).
[86] R. Renner, "Security of quantum key distribution," Int. J. Quant. Inf. **6**, 1 (2008).
[87] R. Renner and J. I. Cirac, "de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography," Phys.Rev. Lett. **102**, 110504 (2009).
[88] V. Scarani and R. Renner, "Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing," Phys. Rev. Lett. **100**, 200501 (2008).
[89] L. Sheridan, T. P. Le, and V. Scarani , "Finite-key security against coherent attacks in quantum key distribution," New. J. of Phys. **12**, 123019 (2010).
[90] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," Nat. Commun. **3**, 634 (2012).
[91] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, "Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks," Phys. Rev. Lett. **109**, 100502 (2012).
[92] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. Scholz, M. Tomamichel, and R. Werner, "Erratum: Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks," Phys. Rev. Lett. **112**, 019902 (2014).
[93] A. Leverrier, "Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction," Phys. Rev. Lett. **118**, 200501 (2017).
[94] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, "Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks," Phys. Rev. A **97**, 052327 (2018).
[95] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, "Parameter Estimation with Almost No Public Communication for Continuous-Variable Quantum Key Distribution," Phys. Rev. Lett. **120**, 220505 (2018).
[96] D. Mayers, "Unconditional security in Quantum Cryptography," Journal of the ACM **48**, 351 (2001).
[97] P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," Phys. Rev. Lett. **85**, 441 (2000).
[98] R. König, R. Renner, A. Bariska, and U. Maurer, "Small Accessible Quantum Information Does Not Imply Security, "Phys. Rev. Lett. **98**, 140502 (2007).
[99] R. Canetti, "Security and Composition of Multiparty Cryptographic Protocols," Journal of Cryptology **13**, 143 (2000).
[100] R. Canetti, "Universally composable security: A new paradigm for cryptographic protocols," Proceedings of the 42nd Annual Symposium on Foundations of Computer Science (FOCS-01), 136 (2001).
[101] B. Pfitzmann and M. Waidner, "Composition and Integrity Preservation of Secure Reactive Systems," Proceedings of the 7th ACM Conference on Computer and Communications Security, 245 (2000).
[102] B. Pfitzmann and M. Waidner, "A Model for Asynchronous Reactive Systems and its Application to Secure Message Transmission," Proceedings of the 2001 IEEE Symposium on Security and Privacy (SP01), 184 (2001).
[103] M. Ben-Or and D. Mayers, "General Security Definition and Composability for Quantum and Classical Protocols," preprint quant-ph/0409062.
[104] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, "The Universal Composable Security of Quantum Key Distribution," Second Theory of Cryptography Conference, TCC 2005, Lecture Notes in Computer Science, Ed. Springer Verlag, **3378**, 386 (2005).
[105] D. Unruh, "Simulatable security for quantum protocols," preprint quant-ph/0409125 (2004).
[106] R. Renner and R. König, "Universally Composable Privacy Amplification Against Quantum Adversaries," Second Theory of Cryptography Conference, TCC 2005, Lecture Notes in Computer Science **3378**, 407–425 (2005).
[107] R. Renner, "Security of Quantum Key Distribution," PhD Thesis, Swiss Federal Institute of Technology, Zurich (2005).
[108] J. Barrett, R. Colbeck, and A. Kent, "Unconditionally secure device-independent quantum key distribution with only two devices," Phys. Rev. A **86**, 062326 (2012).
[109] C. Portmann and R. Renner, "Cryptographic security of quantum key distribution," preprint arXiv:1409.3525v1 (2014).
[110] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Int. Conf. on Computers, Systems & Signal Processing, Bangalore, India, Dec 9-12, 1984. Also at Theor. Comput. Sci. **560**, 7 (2014).
[111] G. Brassard, "Brief History of Quantum Cryptography: A Personal Perspective," Proceedings of IEEE Information Theory Workshop on Theory and Practice in Information Theoretic Security, Awaji Island, Japan, 19 (2005).
[112] C. H. Bennett, G. Brassard, S. Breidbart and S. Wiesner,"Quantum cryptography, or Unforgeable subway tokens", Advances in Cryptology: Proceedings of Crypto '82, Santa Barbara, Plenum Press, 267 (1982).
[113] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett. **68**, 3121 (1992).
[114] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**, 661 (1991).

[115] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," Phys. Rev. Lett. **68**, 557 (1992).

[116] A. Acín, N. Gisin and L. Masanes, "From Bell's Theorem to Secure Quantum Key Distribution," Phys. Rev. Lett. **97**, 120405 (2006).

[117] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," Science **283**, 2050 (1999).

[118] L. Goldenberg and L. Vaidman, "Quantum Cryptography Based on Orthogonal States," Phys. Rev. Lett. **75**, 1239-1243 (1995).

[119] M. Koashi and N. Imoto, "Quantum Cryptography Based on Split Transmission of One-Bit Information in Two Steps," Phys. Rev. Lett. **79**, 2383 (1997).

[120] T.-G. Noh, "Counterfactual Quantum Cryptography," Phys. Rev. Lett. **103**, 230501 (2009).

[121] T. Mor, "No Cloning of Orthogonal States in Composite Systems," Phys. Rev. Lett. **80**, 3137 (1998).

[122] H. Ollivier, and W. H. Zurek, "Quantum Discord: A Measure of the Quantumness of Correlations," Phys. Rev. Lett. **88**, 017901 (2001).

[123] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral, "The classical-quantum boundary for correlations: Discord and related measures," Rev. Mod. Phys. **84**, 1655 (2012).

[124] S. Pirandola, "Quantum discord as a resource for quantum cryptography," Sci. Rep. **4**, 6956 (2014).

[125] S. Pirandola, "Symmetric collective attacks for the eavesdropping of symmetric quantum key distribution," Int. J. Quant. Inf. **6**, 765 (2008).

[126] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres "Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy," Phys. Rev. A **56**, 1163-1172 (1997).

[127] C. S. Niu, and R. B. Griffiths, "Two-qubit copying machine for economical quantum eavesdropping" Phys. Rev. A **60**, 2764-2776 (1999).

[128] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1997).

[129] A. M. Steane, "Error Correcting Codes in Quantum Theory," Phys. Rev. Lett. **77**, 793-767 (1996).

[130] A. R. Calderbank, and P. W. Shor, "Good quantum error-correcting codes exist," Phys. Rev. A **54**, 1098-1105 (1996).

[131] A. M. Steane, "Multiple-particle interference and quantum error correction," Proc. Roy. Soc. Lond. A **452**, 2551-2577 (1996).

[132] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," J. Cryptol. **18**, 133 (2005).

[133] D. Bruss, "Optimal Eavesdropping in Quantum Cryptography with Six States," Phys. Rev. Lett. **81**, 3018 (1998)

[134] H. Inamori, "Security of EPR-based Quantum Key Distribution using three bases," preprint quant-ph/0008076 (2000)

[135] H-.K. Lo, "Proof of unconditional security of six-state quantum key distribution scheme," Quant. Inf. Comp. **1**, 81-94 (2001).

[136] V. Scarani, S. Iblisdir, N. Gisin and A. Acín, "Quantum Cloning," Rev. Mod. Phys. **77**, 1225 (2005).

[137] D. Bruss, M. Cinchetti, G. M. D'Ariano and C. Macchiavello, "Phase-covariant quantum cloning," Phys. Rev. A. **62**, 012302 (2000).

[138] A. Chefles, "Quantum State Discrimination," Contemp. Phys. **41**, 401–424 (2000).

[139] S. M. Barnett and S. Croke, "Quantum state discrimination," Advances in Optics and Photonics **1**, 238-278 (2009).

[140] K. Tamaki, M. Koashi, and N. Imoto, "Unconditionally Secure Key Distribution Based on Two Nonorthogonal States," Phys. Rev. Lett. **90**, 167904 (2003).

[141] K. Tamaki and N. Lütkenhaus, "Unconditional security of the Bennett 1992 quantum key-distribution protocol over a lossy and noisy channel," Phys. Rev. A **69**, 032316 (2004).

[142] M. Koashi, "Unconditional Security of Coherent-State Quantum Key Distribution with a Strong Phase-Reference Pulse," Phys. Rev. Lett. **93**, 120501 (2004).

[143] K. Tamaki, "Unconditionally secure quantum key distribution with relatively strong signal pulse," Phys. Rev. A **77**, 032341 (2008).

[144] K. Tamaki, N. Lütkenhaus, M. Koashi, and J. Batuwantudawe, "Unconditional security of the Bennett 1992 quantum-key-distribution scheme with a strong reference pulse," Phys. Rev. A **80**, 032302 (2009).

[145] M. Lucamarini, G. Di Giuseppe, and K. Tamaki, "Robust unconditionally secure quantum key distribution with two nonorthogonal and uninformative states," Phys. Rev. A **80**, 032327 (2009).

[146] M. Lucamarini, G. Vallone, I. Gianani, P. Mataloni, and G. Di Giuseppe, "Device-independent entanglement-based Bennett 1992 protocol," Phys. Rev. A **86**, 032325 (2012).

[147] J. F. Clauser and M. A. Horne, "Experimental consequences of objective local theories," Phys. Rev. D **10**, 526 (1973).

[148] Ll. Masanes, S. Pironio, and A. Acin, "Secure device-independent quantum key distribution with causally independent measurement devices," Nat. Commun. **2**, 238 (2011).

[149] M. Lucamarini, R. Kumar, G. di Giuseppe, D. Vitali, and P. Tombesi, "Compensating the Noise of a Communication Channel via Asymmetric Encoding of Quantum Information," Phys. Rev. Lett. **105**, 140504 (2010).

[150] T. Heindel, C. A Kessler, M. Rau, C. Schneider, M. Fürst, F. Hargart, W.-M. Schulz, M. Eichfelder, R. Roßbach, S. Nauerth, et al., "Quantum key distribution using quantum dot single-photon emitting diodes in the red and near infrared spectral range," New J. Phys. **14**, 083001 (2012).

[151] T. Heindel, C. Schneider, M. Lermer, S. H. Kwona, T. Braun, S. Reitzensteinb, S. Höfling, M. Kamp, and A. Forchel, "Electrically driven quantum dot-micropillar single photon source with 34% overall efficiency," Appl. Phys. Lett. **96**, 011107 (2010).

[152] M. Reischle, C. Kessler, W.-M. Schulz, M. Eichfelder, R. Roßbach, M. Jetter, and P. Michler, "Triggered single-photon emission from electrically excited quantum dots in the red spectral range," Appl. Phys. Lett. **97**, 143513 (2010).

[153] M. Rau, T. Heindel, S. Unsleber, T. Braun, J. Fischer, S. Frick, S. Nauerth, C. Schneider, G. Vest, S. Reitzenstein, et al. "Free space quantum key distribution over 500 meters using electrically driven quantum dot single-photon sources -a proof of principle experiment," New J. Phys. **16**, 043003 (2014).

[154] B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," Phys. Rev. A **51**, 1863 (1995).

[155] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on Practical Quantum Cryptography," Phys. Rev. Lett. **85**, 1330-1333 (2000). arXiv:quant-ph/9911054v1 (1999).

[156] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," Phys. Rev. A **61**, 052304 (2000).

[157] D. Gottesman, H. K. Lo, Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," Quantum Information and Computation **5**, 325 (2004).

[158] X. Ma, "Quantum cryptography: theory and practice," (PhD thesis, University of Toronto, 2008).

[159] H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," Phys. Rev. Lett. **94**, 230504 (2005).

[160] W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," Phys. Rev. Lett. **91**, 057901 (2003).

[161] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography", Phys. Rev. Lett. **94**, 230503 (2005).

[162] X.-B. Wang, "Decoy-state protocol for quantum cryptography with four different intensities of coherent light," Phys. Rev. A **72**, 012322 (2005).

[163] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," Phys. Rev. A **72**. 012326 (2005).

[164] X.-B. Wang, C.-Z. Peng, J. Zhang, L. Yang, and J.-W. Pan, "General theory of decoy-state quantum cryptography with source errors," Phys. Rev. A **77**, 042311 (2008).

[165] X.-B. Wang, L. Yang, C.-Z. Peng, and J.-W. Pan, "Decoy-state quantum key distribution with both source errors and statistical fluctuations," New J. Phys. **11**, 075006 (2009).

[166] X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, "Quantum information with Gaussian states," Phys. Rep **448**, 1-111(2007).

[167] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations," Phys. Rev. Lett. **92**, 057901 (2004).

[168] K. Tamaki and H.-K. Lo, "Unconditionally secure key distillation from multiphotons," Phys. Rev. A **73**, 010302 (2006).

[169] H.-L. Yin , Y. Fu , Y. Mao, and Z.-B. Chen, "Security of quantum key distribution with multiphoton components", Sci. Rep. **6**, 29482 (2016).

[170] J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt, "Proposed experiment to test local hidden-variable theories", Phys. Rev. Lett., **23**, 880 (1970).

[171] A. Pirker, V. Dunjko, W. Dür and H.J. Briegel, "Entanglement generation secure against general attacks," New J. Phys. **19**, 113012 (2017).

[172] A. Pirker, M. Zwerger, V. Dunjko, H.J. Briegel and W. Dür, "Simple proof of confidentiality for private quantum channels in noisy environments," Quantum Sci. Technol. **4**, 025009 (2019).

[173] K. Boström and T. Felbinger, "Deterministic Secure Direct Communication Using Entanglement," Phys. Rev. Lett. **89**, 187902 (2002).

[174] Q.-Y. Cai and B.-W. Li, "Deterministic Secure Communication Without Using Entanglement," Chin. Phys. Lett. **21**, 601 (2004).

[175] F.-G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," Phys. Rev. A **69**, 052319 (2004).

[176] F.-G. Deng and G. L. Long, "Bidirectional quantum key distribution protocol with practical faint laser pulses," Phys. Rev. A **70**, 012311 (2004).

[177] M. Lucamarini and S. Mancini, "Secure Deterministic Communication without Entanglement," Phys. Rev. Lett. **94**, 140501 (2005).

[178] H. Lu, C.-H. Fred Fung, X. Ma, and Q.-Y. Cai, "Unconditional security proof of a deterministic quantum key distribution with a two-way quantum channel," Phys. Rev. A **84**, 042344 (2011).

[179] K. Boström, "Secure direct communication using entanglement," arXiv:0203064 v1 [quant-ph]) (2002).

[180] Q.-Y. Cai, "The "Ping-Pong" Protocol Can Be Attacked without Eavesdropping," Phys. Rev. Lett. **91**, 109801 (2003).

[181] S. Pirandola, S.L. Braunstein, S. Mancini, S. Lloyd, "Quantum direct communication with continuous variables," Europhys. Lett. **84**, 20013 (2008).

[182] S. Pirandola, S.L. Braunstein, S. Lloyd, S. Mancini, "Confidential direct communications: a quantum approach using continuous variables," IEEE J. Sel. Top. Quantum Electron. **15**, 1570 (2009).

[183] Jeffrey H. Shapiro, Don M. Boroson, P. Ben Dixon, Matthew E. Grein, and Scott A. Hamilton, "Quantum low probability of intercept," Journal of the Optical Society of America B **36**, B41-B50 (2019).

[184] J. S. Shaari, M. Lucamarini, and S. Mancini, "Checking noise correlations for safer two-way quantum key distribution," Quantum Information Processing **13**, 1139, (2014).

[185] A. Cerè, M. Lucamarini, G. Di Giuseppe, and P. Tombesi, "Experimental Test of Two-way Quantum Key Distribution in Presence of Controlled Noise," Phys. Rev. Lett. **96**, 200501 (2006).

[186] M. F. Abdul Khir, M. N. Mohd Zain, S. Soekardjo, S. Saharudin, and S. Shaari, "Implementation of two-way free space quantum key distribution," Opt. Eng. **51**, 045006 (2012).

[187] M. F. Abdul Khir, M. Zain, I. Bahari, and S. Shaari, "Experimental two way quantum key distribution with decoy state," Opt. Commun. **285**, 842–845 (2012).

[188] R. Kumar, M. Lucamarini, G. Di Giuseppe, R. Natali, G. Mancini, and P. Tombesi, "Two-way quantum key distribution at telecommunication wavelength," Phys. Rev. A **77**, 022304 (2008).

[189] N. J. Beaudry, M. Lucamarini, S. Mancini and R. Renner, "Security of two-way quantum key distribution," Phys. Rev. A **88**, 062302 (2013).

[190] Q.-Y. Cai, "Eavesdropping on the two-way quantum communication protocols with invisible photons," Phys. Lett. A **351**, 23 (2006).

[191] A. Wócjik, "Eavesdropping on the Ping-Pong Quantum Communication Protocol," Phys. Rev. Lett. **90**, 157901 (2003).

[192] M. Lucamarini and S. Mancini, "Quantum key distribution using a two-way quantum channel," Theoretical Computer Science **560**, 46-61 (2014).

[193] M. Lucamarini, Alessandro Cerè, G. Di Giuseppe, S.

Mancini, D. Vitali, and P. Tombesi, "Two-way protocol with imperfect devices," Open Sys. & Information Dyn. **14**, 169 (2007).

[194] J. S. Shaari and I. Bahari, "Independent attacks in imperfect settings: A case for a two-way quantum key distribution scheme," Phys. Lett. A **374**, 4205 (2010).

[195] G. Chiribella, G. M. D'Ariano, and P. Perinotti, "Optimal Cloning of Unitary Transformation," Phys. Rev. Lett. **101**, 180504 (2008).

[196] A. Bisio, G. Chiribella, G. M. D'Ariano, P. Perinotti, "Information-disturbance tradeoff in estimating a unitary transformation," Phys. Rev. A **82**, 062305 (2010).

[197] J. S. Shaari, "Nonorthogonal unitaries in two-way quantum key distribution," Phys. Lett. **378**, 863 (2014).

[198] A. Laing, T. Rudolph, & J. L. O'Brien, "Experimental Quantum Process Discrimination," Phys. Rev. Lett. **102**, 160502 (2009).

[199] J. S. Shaari and Suryadi Soekardjo, "Indistinguishable encoding for bidirectional quantum key distribution: Theory to experiment," Europhys. Lett. **120**, 60001 (2018).

[200] J. S. Shaari, R. N. M. Nasir and S. Mancini, "Mutually unbiased unitary bases," Phys. Rev. A **94**, 052328 (2016).

[201] J.S. Shaari, M. Lucamarini and M. R. B. Wahiddin, "Deterministic six states protocol for quantum communication," Phys. Lett. A **358**, 2 (2006).

[202] J.S. Shaari, M. R. B. Wahiddin and S. Mancini, "Blind encoding into qudits," Phys. Lett. A **372**, 12 (2008).

[203] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system," Nat. Commun. **2**, 349 (2011).

[204] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," Nat. Photon. **4**, 686-689 (2010).

[205] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors," New J. Phys. **13**, 073024 (2011).

[206] F. Xu, B. Qi, and H.-K. Lo, "Experimental demonstration of phase-remapping attack in a practical quantum key distribution system," New J. Phys. **12**, 113026 (2010).

[207] B. S. Cirelson, "Quantum generalizations of Bell's inequality," Lett. Math. Phys. **4**, 93 (1980).

[208] B. S. Cirelson, "Some results and problems on quantum Bell-type inequalities," Hadronic Journal Supplement **8**, 329 (1993).

[209] L. A. Khalfin, and B. S. Tsirelson, "Quantum and Quasi-classical Analogs Of Bell Inequalities," Symposium on the foundations of modern physics 1985, ed. P. Lahti and P. Mittelstaedt, World Scientific, Singapore (1985).

[210] S. Popescu, and D. Rohrlich, "Quantum nonlocality as an axiom," Found. Phys. **24**, 379 (1994).

[211] M. Navascués, S. Pironio, and A. Acín, "Bounding the Set of Quantum Correlations," Phys. Rev. Lett. **98**, 010401 (2007).

[212] R. Arnon-Friedman, R. Renner, and T. Vidick, "Simple and tight device-independent security proofs," preprint arXiv:1607.01797 (2016).

[213] F. Dupuis, O. Fawzi, and R. Renner, "Entropy accumulation," preprint arXiv:1607.01796 (2016).

[214] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-Independent Security of Quantum Cryptography against Collective Attacks," Phys. Rev. Lett. **98**, 230501 (2007).

[215] M. Navascués, S. Pironio, and A. Acín, "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations," New J. Phys. **10**, 073013 (2008).

[216] E. Hänggi and R. Renner, "Device-Independent Quantum Key Distribution with Commuting Measurements," preprint arXiv:1009.1833 (2010).

[217] P. J. Brown, S. Ragy and R. Colbeck, "A framework for quantum-secure device-independent randomness expansion" arXiv:1810.13346 (2018).

[218] M. Winczewski, T. Das, and K. Horodecki, "Upper bounds on secure key against non-signaling adversary via non-signaling squashed secrecy monotones," preprint arXiv:1903.12154 (2019).

[219] E. Kaur, M. M. Wilde, and A. Winter, "Fundamental limits on key rates in device-independent quantum key distribution," preprint arXiv:1810.05627 (2018).

[220] J. Barrett, R. Colbeck, and A. Kent, "Memory attacks on device-independent quantum cryptography," Phys. Rev. Lett. **106**, 010503 (2013).

[221] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani, "Device-independent quantum key distribution secure against collective attacks," New J. Phys. **11**, 045021 (2009).

[222] M. McKague, "Device independent quantum key distribution secure against coherent attacks with memoryless measurement devices," New J. of Phys. **11**, 103037 (2009).

[223] E. Hänggi, R. Renner, and Stefan Wolf, "Efficient Device-Independent Quantum Key Distribution," Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt'10), pp. 216–234, ed. Henri Gilbert, French Riviera, Springer. Also available preprint arXiv:0911.4171 (2009).

[224] L. Masanes, R. Renner, M. Christandl, A. Winter, and J. Barrett, "Full security of quantum key distribution from no-signaling constraints," IEEE Trans. Inf. Theory **60**, 4973-4986 (2014).

[225] C. A. Miller and Y. Shi, "Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices," In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, STOC '14, 417 (ACM, New York, NY, USA, 2014).

[226] U. Vazirani, and T. Vidick, "Fully Device-Independent Quantum Key Distribution," Phys. Rev. Lett. **113**, 140501 (2014).

[227] B. W. Richardt, F. Unger, and U. Vazirani, "Classical command of quantum systems," Nature **496**, 456 (2013).

[228] F. Dupuis and O. Fawzi, "Entropy accumulation with improved second-order term," preprint arXiv:1805.11652 (2018).

[229] R. Colbeck and V. Vilasini. LPAssumptions (Mathematica package) (2019). URL https://github.com/rogercolbeck/LPAssumptions.

[230] P. H. Eberhard, "Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment," Phys. Rev. A **47**, 747–750 (1993).

[231] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, " Bell nonlocality," Rev. Mod. Phys. **86**, 419 (2014).

[232] T. P. W. Cope, "The Role of Entanglement in Quantum Communication, and Analysis of the Detection Loophole," (PhD thesis, University of York, UK 2018); see also preprint arXiv:1904.11769 (2019).

[233] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, and C. Abellan et al. "Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons," Phys. Rev. Lett. **115**, 250401 (2015).

[234] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M.S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, and C. Abella et al. "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres," Nature **526**, 682 (2015).

[235] L. K. Shalm, et al., "Strong Loophole-Free Test of Local Realism," Phys. Rev. Lett. **115**, 250402 (2015).

[236] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, "Finite-key analysis for measurement-device-independent quantum key distribution," Nat. Commun. **5**, 3732 (2014).

[237] X.-B. Wang, "Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors," Phys. Rev. A **87**, 012320 (2013).

[238] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, "Making the decoy-state measurement-device-independent quantum key distribution practically useful," Phys. Rev. A **93**, 042324 (2016).

[239] T. Heinosaari and M. Ziman, "Guide to Mathematical Concepts of Quantum Theory," Acta Physica Slovaca **58**, 487 (2008).

[240] S. Pirandola, C. Ottaviani Gaetana Spedalieri, Christian Weedbrook, Samuel L. Braunstein, Seth Lloyd, Tobias Gehring, Christian S. Jacobsen and Ulrik L. Andersen, "High-rate quantum cryptography in untrusted networks," Nature Photon. **9**, 397 (2015). See also preprint arXiv:1312.4104 (2013).

[241] Q. Wang, and X. B. Wang, "Simulating of the measurement-device independent quantum key distribution with phase randomized general sources," Sci. Rep., **4**, 4612 (2014).

[242] X. Y. Zhou et al, "Obtaining better performance in the measurement-device-independent quantum key distribution with heralded single-photon sources," Phys. Rev. A **96**, 052337 (2017).

[243] C. C. Mao et al, "Improved statistical fluctuation analysis for measurement-device-independent quantum key distribution with four-intensity decoy-state method," Opt. Express **26**, 13289 (2018).

[244] X.-B. Wang, X.-L. Hu, and Z.-W. Yu, "Practical long distance side channel free quantum key distribution," In publication on Physical Review Applied. See also arXiv:1811.01263 (2018).

[245] C. H. Zhang et al, "Efficient passive measurement-device-independent quantum key distribution, Phys. Rev. A **99**, 052325 (2019).

[246] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, "Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound,"preprint arXiv:1805.05511 (2018).

[247] X. Ma, P. Zeng, and H. Zhou, "Phase-matching quantum key distribution," Phys. Rev. X **8**, 031043 (2018).

[248] J. Lin and N. Lütkenhaus, "Simple security analysis of phase-matching measurement-device-independent quantum key distribution," Phys. Rev. A **98**, 042332 (2018).

[249] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, "Twin-field quantum key distribution with large misalignment error," Phys. Rev. A **98**, 062323 (2018).

[250] Z.-W. Yu, X.-L. Hu, C. Jiang, H. Xu and X.-B. Wang, "Sending-or-not-sending twin-field quantum key distribution in practice," Sci. Rep. **9**, 3080 (2019).

[251] C. Jiang, Z.-W. Yu, X.-L. Hu, and X.-B. Wang, "Unconditional security of sending or not sending twin-field quantum key distribution with finite pulses," preprint arXiv:1904.00192 (2019).

[252] H. Xu, Z.-W. Yu, C. Jiang, X.-L. Hu, and X.-B. Wang, "General theory of sending-or-not-sending twin-field quantum key distribution," preprint arXiv:1904.06331 (2019).

[253] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, "Twin-field Quantum Key Distribution without Phase Postselection," Phys. Rev. Applied **11**, 034053 (2019).

[254] F.-Y. Lu, Z.-Q. Yin, C.-H. Cui, G.-J. Fan-Yuan, S. Wang, D.-Y. He, W. Chen, G.-C. Guo, and Z.-F. Han, "Practical issues of twin-field quantum key distribution,"preprint arXiv:1901.04264v3 (2019).

[255] F.-Y. Lu, Z.-Q. Yin, C.-H. Cui, G.-J. Fan-Yuan, R. Wang, S. Wang, W. Chen, D.-Y. He, G.-C. Guo, and Z.-F. Han, "Improving the performance of Twin-Field Quantum Key Distribution," preprint arXiv:1901.02299 (2019).

[256] M. Curty, K. Azuma and H.-K. Lo, "Simple security proof of twin-field type quantum key distribution protocol," npj Quantum Inf. **5**, 64 (2019).

[257] F. Grasselli and M. Curty, "Practical decoy-state method for twin-field quantum key distribution," preprint arXiv:1902.10034 (2019).

[258] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, "Proof-of-principle experimental demonstration of twin-field type quantum key distribution," Phys. Rev. Lett. **123**, 100506 (2019).

[259] M. Takeoka, S. Guha, and M. M. Wilde, "Fundamental rate-loss tradeoff for optical quantum key distribution," Nat. Commun. **5**, 5235 (2014).

[260] H.-L. Yin, and Y. Fu, "Measurement-Device-Independent Twin-Field Quantum Key Distribution," Sci. Rep. **9**, 3045 (2019).

[261] H.-L. Yin, and Z.-B. Chen, "Twin-Field Quantum Key Distribution over 1000 km Fibre," preprint arXiv:1901.05009 (2019).

[262] H.-L. Yin, and Z.-B. Chen, "Finite-key analysis for twin-field quantum key distribution with composable security,"preprint arXiv:1903.09093 (2019).

[263] C. H. Zhang et al, "Twin-field quantum key distribution with modified coherent states," Opt. Lett. **44**, 1468 (2019).

[264] X. Y. Zhou et al, "Asymmetric sending or not sending twin-field quantum key distribution in practice," Phys. Rev. A **99**, 062316 (2019).

[265] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, "Experimental quantum key distribution beyond the re-

peaterless secret key capacity," Nat. Photon. **13**, 334-338 (2019).

[266] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system," Phys. Rev. X **9**, 021046 (2019).

[267] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, et al., "Experimental Twin-Field Quantum Key Distribution through Sending or Not Sending," Phys. Rev. Lett. **123**, 100505 (2019).

[268] H. Inamori, N. Lütkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution," Eur. Phys. J. D, **41**, 599 (2007).

[269] Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, "High speed single photon detection in the near infrared," Appl. Phys. Lett. **91**, 041114 (2007).

[270] M. Caloz, M. Perrenoud, C. Autebert, B. Korzh, M. Weiss, C. Schönenberger, and R. J. Warburton, "High-detection efficiency and low-timing jitter with amorphous superconducting nanowire single-photon detectors," Appl. Phys. Lett. **112**, 061103 (2018).

[271] A. You, M. A. Y. Be, and I. In, "Waveguide superconducting single-photon detectors for integrated quantum photonic circuits," Appl. Phys. Lett. **99**, 181110 (2011).

[272] P. Rath, O. Kahl, S. Ferrari, F. Sproll, G. Lewes-Malandrakis, D. Brink, W. Pernice, "Superconducting single-photon detectors integrated with diamond nanophotonic circuits". Light: Science and Applications **4**, e338 (2015).

[273] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental Quantum Key Distribution with Decoy States," Phys. Rev. Lett. **96**, 070502 (2006).

[274] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Simulation and Implementation of Decoy State Quantum Key Distribution over 60km Telecom Fiber," Proceedings of the 2006 IEEE International Symposium on Information Theory, Seattle, WA, 2006, pp. 2094-2098.

[275] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett. and C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt,"Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber," Phys. Rev. Lett. **98**, 010503 (2007).

[276] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, and J. G. Rarity et al. "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km," Phys. Rev. Lett. **98**, 010504 (2007).

[277] C.-Z. Peng, J. Z., D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, "Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding," Phys. Rev. Lett. **98**, 2 (2007).

[278] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate," Opt. Express **16**, 18790 (2008).

[279] Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Gigahertz quantum key distribution with InGaAs avalanche photodiodes," Appl. Phys. Lett. **92**, 201104 (2008).

[280] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Efficient decoy-state quantum key distribution with quantified security," Opt. Express **21**, 24550 (2013).

[281] A. Boaron, G. Boso, D. Rusca, C. Autebert, M. Caloz, M. Perrenoud, H. Zbinden, "Secure Quantum Key Distribution over 421 km of Optical Fiber," Phys. Rev. Lett. **121**, 190502 (2018).

[282] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, "2 GHz clock quantum key distribution over 260 km of standard telecom fiber," Opt. Lett. **37**, 1008 (2012).

[283] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307km of optical fibre," Nat. Photon. **9**, 163 (2015).

[284] F. Xu, K. Wei, S. Sajeed, S. Kaiser, S. Sun, Z. Tang, L. Qian, V. Makarov, and H.-K. Lo, "Experimental quantum key distribution with source flaws," Phys. Rev. A **92**, 032305 (2015).

[285] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, "Long-distance quantum key distribution secure against coherent attacks," Optica **4**, 163 (2017).

[286] T. Honjo, K. Inoue, and H. Takahashi, "Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit Mach-Zehnder interferometer," Opt. Lett. **29**, 2797 (2004).

[287] H. Takesue, S. W. Nam,Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," Nat. Photon. **1**, 357 (2007).

[288] Q. Zhang, H. Takesue, T. Honjo, K. Wen, T. Hirohata, M. Suyama, Y. Takiguchi, H. Kamada, Y. Tokura, O. Tadanaga, Y. Nishida, M. Asobe and Y. Yamamoto, "Megabits secure key rate quantum key distribution," New J. Phys. **11**, 045010 (2009).

[289] T. Honjo, T. Inoue, and K. Inoue, "Influence of light source linewidth in differential-phase-shift quantum key distribution systems," Optics Communications **284**, 5856 (2011).

[290] K. Shimizu, T. Honjo, M. Fujiwara, T. Ito, K. Tamaki, S. Miki, T. Yamashita, H. Terai, Z. Wang, and M. Sasaki, "Performance of Long-Distance Quantum Key Distribution Over 90-km Optical Links Installed in a Field Environment of Tokyo Metropolitan Area," Journal of Lightwave Technology **32**, 141 (2014).

[291] E. Waks, H. Takesue, and Y. Yamamoto, "Security of differential-phase-shift quantum key distribution against individual attacks," Phys. Rev. A **73**, 012344 (2006).

[292] T. Moroder, M. Curty, C. C. W. Lim, L. P. Thinh, H. Zbinden, and N. Gisin, "Security of Distributed-Phase-Reference Quantum Key Distribution," Phys. Rev. Lett. **109**, 260501 (2012).

[293] K. Inoue, and Y. Iwai, "Differential-quadrature-phase-shift quantum key distribution," Phys. Rev. A **79**, 022319 (2009).

[294] S. Kawakami, T. Sasaki, and M. Koashi, "Security of the differential-quadrature-phase-shift quantum key distribution," Phys. Rev. A **94**, 022322 (2016).

[295] G. L. Roberts, M. Lucamarini, J. F. Dynes, S. J. Savory, Z. Yuan, and A. J. Shields, "Manipulating photon coherence to enhance the security of distributed phase reference quantum key distribution," Appl. Phys. Lett. **111**, 261106 (2017).

[296] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," Appl. Phys. Lett. **87**, 194108 (2005).

[297] D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, and H. Zbinden, "Continuous high speed coherent one-way quantum key distribution," Opt. Express **17**, 13326 (2009).

[298] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, "High rate, long-distance quantum key distribution over 250km of ultra low loss fibres," New J. Phys. **11**, 075003 (2009).

[299] N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, and N. Kulesza et al. "A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing," New J. Phys. **16**, 013047 (2014).

[300] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, "Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks," Phys. Rev. Lett. **111**, 130501 (2013).

[301] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, and L. Li et al. "Experimental measurement-device-independent quantum key distribution," Phys. Rev. Lett. **111**, 130502 (2013).

[302] T. Ferreira Da Silva, D. Vitoreti, G. B. Xavier, G. C. Do Amaral, G. P. Temporao, and J. P. Von der Weid, "Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits," Phys. Rev. A **88**, 052303 (2013).

[303] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, and J.-Y. Guan et al. "Measurement-Device-Independent Quantum Key Distribution over 200 km," Phys. Rev. Lett. **113**, 190501 (2014).

[304] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, and W.-J. Zhang et al. "Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber," Phys. Rev. Lett. **117**, 190501 (2016).

[305] L. C. Comandar, S. W.-B. Tam, J. F. Dynes, M. Lucamarini, B. Fröhlich, Z. L. Yuan, A. W. Sharpe, R. V. Penty, and A. J. Shields, "Quantum key distribution without detector vulnerabilities using optically seeded lasers," Nat. Photon. **10**, 312 (2016).

[306] R. Valivarthi, Q. Zhou, J. Caleb, F. Marsili, V. B. Verma, M. D. Shaw, S. W. Nam, D. Oblak, and W. Tittel, "A cost-effective measurement-device-independent quantum key distribution system for quantum networks," Quantum Sci. Technol. **2**, 04LT01 (2017).

[307] Y. Choi, O. Kwon, M. Woo, K. Oh, S.-W. Han, Y.-S. Kim, and S. Moon, "Plug-and-play measurement-device-independent quantum key distribution," Phys. Rev. A **93**, 032319 (2016).

[308] G. Z. Tang, S. H. Sun, F. Xu, H. Chen, C. Y. Li, and L. M. Liang, "Experimental asymmetric plug-and-play measurement-device-independent quantum key distribution," Phys. Rev. A **94**, 032326 (2016).

[309] C. Wang, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, "Measurement-device-independent quantum key distribution robust against environmental disturbances," Optica **4**, 1016 (2017).

[310] C. H. Park, M. K. Woo, B. K. Park, M. S. Lee, Y. S. Kim, Y. W. Cho, S. Kim, S. W. Han, and S. Moon, "Practical Plug-and-Play Measurement-Device-Independent Quantum Key Distribution With Polarization Division Multiplexing," IEEE Access **6**, 58587 (2018).

[311] H. Liu, J. Wang, H. Ma, and S. Sun, "Polarization-multiplexing-based measurement-device-independent quantum key distribution without phase reference calibration," Optica **5**, 902 (2018).

[312] C.-H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental Quantum Cryptography," Journal of Cryptology **5**, 3 (1992).

[313] C. M Natarajan, M. G. Tanner, and R. H. Hadfield, "Superconducting nanowire single-photon detectors: physics and applications," Superconductor Science and Technology **25**, 063001 (2012).

[314] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. W. Sharpe, A. R. Dixon, E. Lavelle, J. F. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato and A. J. Shields, "10-Mb/s Quantum Key Distribution," Journal of Lightwave Technology **36**, 3427-3433 (2018).

[315] L. Zhang, C. Silberhorn, I. Walmsley, "Secure Quantum Key Distribution using Continuous Variables of Single Photons," Phys. Rev. Lett. **100**, 110504 (2008).

[316] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, "Quantum Cryptography Using Entangled Photons in Energy-Time Bell States," Phys. Rev. Lett. **84**, 4737 (2000).

[317] R. T. Thew, A. Acín, H. Zbinden, and N. Gisin, "Bell-Type Test of Energy-Time Entangled Qutrits," Phys. Rev. Lett. **93**, 010503 (2004).

[318] B. Qi, "Single-photon continuous-variable quantum key distribution based on the energy-time uncertainty relation," Opt. Lett. **31**, 2795 (2006).

[319] J. Nunn, L. J. Wright, C. Söller, L. Zhang, I. A. Walmsley, and B. J. Smith "Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion," Opt. Express **21**, 15959 (2013).

[320] C. Lee, Z. Zhang, G. R. Steinbrecher, H. Zhou, J. Mower, T. Zhong, L. Wang, X. Hu, R. D. Horansky, and V. B. Verma et al. "Entanglement-based quantum communication secured by nonlocal dispersion cancellation," Phys. Rev. A **90**, 062331 (2014).

[321] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, "Large-Alphabet Quantum Key Distribution Using Energy-Time Entangled Bipartite States," Phys. Rev. Lett. **98**, 060503 (2007).

[322] D. Bacco, J. B. Christensen, M. A. Usuga Castaneda, Y. Ding, S. Forchhammer, K. Rottwitt, L. K. Oxenløwe, "Two-dimensional distributed-phase-reference protocol for quantum key distribution," Sci. Reports **6**, 36756 (2016).

[323] B. Da Lio, D. Bacco, D. Cozzolino, Y. Ding, K. Dalgaard, K. Rottwitt, and L. Oxenløwe, "Experimental demonstration of the DPTS QKD protocol over a 170

km fiber link," Appl. Phys. Lett. **114**, 011101 (2019).

[324] A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, and B. Heim et al. "High-dimensional intracity quantum cryptography with structured photons," Optica **4**, 1006 (2017).

[325] M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, R. W. Boyd, "High-dimensional quantum cryptography with twisted light," New J. Phys. **17**, 033033 (2015).

[326] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, "Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases," Phys. Rev. A **88**, 032305 (2013).

[327] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of Quantum Key Distribution Using d-Level Systems," Phys. Rev. Lett. **88**, 127902 (2002).

[328] G. M. Nikolopoulos, and G. Alber, "Security bound of two-basis quantum-key-distribution protocols using qudits," Phys. Rev. A **72**, 032320 (2005).

[329] G. M. Nikolopoulos, K. S. Ranade, and G. Alber, "Error tolerance of two-basis quantum-key-distribution protocols using qudits and two-way classical communication," Phys. Rev. A **73**, 032325 (2006).

[330] J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, "High-dimensional quantum key distribution using dispersive optics," Phys. Rev. A **87**, 062322 (2013).

[331] Z. Zhang, J. Mower, D. Englund, F. N.C. Wong, and J. H. Shapiro, "Unconditional Security of Time-Energy Entanglement Quantum Key Distribution Using Dual-Basis Interferometry," Phys. Rev. Lett. **112**, 120506 (2014).

[332] T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, and T. Gerrits et al. "Photon-efficient quantum key distribution using time-energy entanglement with high-dimensional encoding," New J. Phys. **17**, 022002 (2015).

[333] C. Lee, D. Bunandar, Z. Zhang, G. R. Steinbrecher, P. B. Dixon, F. N. C. Wong, J. H. Shapiro, S. A. Hamilton, and D. Englund, "High-rate field demonstration of large-alphabet quantum key distribution," preprint arXiv:1611.01139 (2016).

[334] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim and D. J. Gauthier, "Provably secure and high-rate quantum key distribution with time-bin qudits," Science Advances 3, 1–7 (2017).

[335] D. Bunandar, Z. Zhang, J. H. Shapiro, and D. R. Englund, "Practical high-dimensional quantum key distribution with decoy states," Phys. Rev. A **91**, 022336 (2015).

[336] M. Yuezhen Niu, F. Xu, J. H. Shapiro, and F. Furrer, "Finite-key analysis for time-energy high-dimensional quantum key distribution," Phys. Rev. A **94**, (2016).

[337] C. Lee, J. Mower, Z. Zhang, J. H. Shapiro, and D. Englund, "Finite-key analysis of high-dimensional time-energy entanglement-based quantum key distribution," Quantum Information Processing **14**, 1005 (2015).

[338] M. Erhard, R. Fickler, M. Krenn, and A. Zeilinger, "Twisted Photons: New Quantum Perspectives in High Dimensions," Light: Science and Applications **7**, 17111 (2018).

[339] K. Brádler, M. Mirhosseini, R. Fickler, A. Broadbent, and R. Boyd, "Finite-key security analysis for multilevel quantum key distribution," New J. Phys. **18**, 073030 (2016).

[340] J. A. Neff, R. A. Athale, and S. H. Lee, "Two-dimensional spatial light modulators: A tutorial," Proceedings of the IEEE **78**, 826 (1990).

[341] P.-A. J. Blanche, D. N. Carothers, J. Wissinger, N. Peyghambarian, "Digital micromirror device as a diffractive reconfigurable optical switch for telecommunication," Journal of Micro/Nanolithography, MEMS, and MOEMS **13**, 011104 (2013).

[342] Z. Zhang, Z. You, and D. Chu, "Fundamentals of phase-only liquid crystal on silicon (LCOS) devices," Light: Science & Applications **3**, e213 (2014).

[343] S. Slussarenko, A. Murauski, T. Du, V. Chigrinov, L. Marrucci, and E. Santamato, "Tunable liquid crystal q-plates with arbitrary topological charge," Opt. Express **19**, 4085 (2011).

[344] Y. Ren, G. Xie, H. Huang, N. Ahmed, Y. Yan, L. Li, C. Bao, M. P. J. Lavery, M. Tur, and M. A. Neifeld et al., "Adaptive-optics-based simultaneous pre- and post-turbulence compensation of multiple orbital-angular-momentum beams in a bidirectional free-space optical link," Optica **1**, 376–382 (2014).

[345] D. Cozzolino, D. Bacco, B. Da Lio, K. Ingerslev, Y. Ding, K. Dalgaard, P. Kristensen, M. Galili, K. Rottwitt, S. Ramachandran, and L. K. Oxenløwe, "Orbital Angular Momentum States Enabling Fiber-based High-dimensional Quantum Communication," Phys. Rev. Applied **11**, 064058 (2019).

[346] E. Karimi, B. Piccirillo, E. Nagali, L. Marrucci, and E. Santamato, "Efficient generation and sorting of orbital angular momentum eigenmodes of light by thermally tuned q-plates," Appl. Phys. Lett. **94**, 231124 (2009).

[347] M. J. Strain, X. Cai, J. Wang, J. Zhu, D. B. Phillips, L. Chen, M. Lopez-Garcia, J. L. O'Brien, M. G. Thompson, M. Sorel, and S. Yu, "Fast electrical switching of orbital angular momentum modes using ultra-compact integrated vortex emitters," Nat. Commun. **5**, 4856 (2014).

[348] X. Cai, J. Wang, M. J. Strain, B. Johnson-Morris, J. Zhu, M. Sorel, J. L. O'Brien, M. G. Thompson, and S. Yu, "Integrated Compact Optical Vortex Beam Emitters," Science **338**, 363 (2012).

[349] J. Sun, M. Moresco, G. Leake, D. Coolbaugh, and M. R. Watts, "Generating and identifying optical orbital angular momentum with silicon photonic circuits," Opt. Lett. **39**, 5977 (2014).

[350] S. Han, T. J. Seok, N. Quack, B.-W. Yoo, and M. C. Wu, "Large-scale silicon photonic switches with movable directional couplers," Optica **2**, 370 (2015).

[351] S. Restuccia, D. Giovannini, G. Gibson and M. Padgett, "Comparing the information capacity of Laguerre-Gaussian and Hermite-Gaussian modal sets in a finite-aperture system," Opt. Express **24**, 27127 (2016).

[352] I. Choi, Y. R. Zhou, J. F. Dynes, Z. Yuan, A. Klar, A. Sharpe, A. Plews, M. Lucamarini, C. Radig, and J. Neubert et al. "Field trial of a quantum secured 10Gb/s DWDM transmission system over a single installed fiber," Opt. Express **22**, 23121 (2014).

[353] G. Cañas, N. Vera, J. Cariñe, P. González, J. Carde-

nas, P. W. R. Connolly, A. Przysiezna, E. S. Gómez, M. Figueroa, and G. Vallone et al. "High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers," Phys. Rev. A **96**, 022317 (2017).

[354] B. Qi, W. Zhu, L. Qian, and H.-K. Lo, "Feasibility of quantum key distribution through dense wavelength division multiplexing network," New J. Phys. **12**, 103042 (2010).

[355] N. Namekata, H. Takesue, T. Honjo, Y. Tokura, and S. Inoue, "High-rate quantum key distribution over 100 km using ultra-low-noise, 2-GHz sinusoidally gated InGaAs/InP avalanche photodiodes," Opt. Express **19**, 10632 (2011).

[356] K. Inoue, "Differential Phase-Shift Quantum Key Distribution Systems," IEEE J. Sel. Top. Quantum Electron. **21**, 6600207 (2015).

[357] J. F. Dynes, W. W-S. Tam, A. Plews, B. Fröhlich, A. W. Sharpe, M. Lucamarini, Z. Yuan, C. Radig, A. Straw, T. Edwards, and A. J. Shields, "Ultra-high bandwidth quantum secured data transmission," Sci. Rep. **6**, 35149 (2016).

[358] A.R. Dixon, J.F. Dynes, M. Lucamarini, B. Fröhlich, AW Sharpe, A Plews, W Tam, ZL Yuan, Y Tanizawa, and H Sato et al. "Quantum key distribution with hacking countermeasures and long term field trial," Sci. Rep. **7**, 1978 (2017).

[359] A. B. Price, P. Sibson, C. Erven, J. G. Rarity, and M. G. Thompson, "High-Speed Quantum Key Distribution with Wavelength-Division Multiplexing on Integrated Photonic Devices," Conference on Lasers and Electro-Optics, JTh2A.24 (2018).

[360] D. Bunandar, N. Harris, Z. Zhang, C. Lee, R. Ding, T. Baehr-Jones, M. Hochberg, J. Shapiro, F. Wong and D. Englund, "Wavelength-division multiplexed quantum key distribution on silicon photonic integrated devices," Bulletin of the American Physical Society, A18.00009 (2018).

[361] Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, L. K. Oxenløwe, "High-Dimensional Quantum Key Distribution based on Multicore Fiber using Silicon Photonic Integrated Circuits," npj Quantum Information **3**, 25 (2017).

[362] D. Bacco, Y. Ding, K. Dalgaard, K. Rottwit, and L. K. Oxenløwe, "Space division multiplexing chip-to-chip quantum key distribution," Scientific Reports **7**, 12459 (2017).

[363] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, and C. M. Natarajan et al. "Chip-based quantum key distribution," Nat. Commun. **8**, 13984 (2017).

[364] D. Bunandar, A. Lentine, C. Lee, H. Cai, C. M. Long, N. Boynton, N. Martinez, C. DeRose, C. Chen, and M. Grein et al. "Metropolitan Quantum Key Distribution with Silicon Photonics," Phys. Rev. X **8**, 021009 (2018).

[365] S. Bogdanov, M. Y. Shalaginov, A Boltasseva, and V. M. Shalaev, "Material platforms for integrated quantum photonics," Optical Materials Express **7**, 111 (2017).

[366] M. Smit, X. Leijtens, H. Ambrosius, E. Bente, J. van der Tol, B. Smalbrugge, T. de Vries, E.-J. Geluk, J. Bolk, and R. van Veldhoven et al. "An introduction to InP-based generic integration technology," Semiconductor Science and Technology **29**, 083001 (2014).

[367] G. Roelkens, L. Liu, D. Liang, R. Jones, A. Fang, B. Koch, and J. Bowers, "III-V/silicon photonics for on chip and intra chip optical interconnects," Laser & Photonics Reviews **4**, 751 (2010).

[368] D. A. B. Miller, D. S. Chemla, T. C. Damen, A. C. Gossard, W. Wiegmann, T. H. Wood, and C. A. Burrus, "Band-Edge Electroabsorption in Quantum Well Structures: The Quantum-Confined Stark Effect," Phys. Rev. Lett. **53**, 2173 (1984).

[369] Y.-J. Chiu, H.-F. Chou, V. Kaman, P. Abraham and J. E. Bowers, "High extinction ratio and saturation power traveling-wave electro-absorption modulator," IEEE Photonics Technology Letters **14**, 792 (2002).

[370] T. K. Paraïso, I. De Marco, T. Roger, D. G. Marangon, J. F. Dynes, M. Lucamarini, Z. Yuan, and A. J. Shields, "A Modulator-Free Quantum Key Distribution Transmitter Chip," npj Quantum Information **5**, 42 (2019).

[371] Z. L. Yuan, B. Fröhlich, M. Lucamarini, G. L. Roberts, J. F. Dynes, and A. J. Shields, "Directly Phase-Modulated Light Source," Phys. Rev. X **6**, 031044 (2016).

[372] K. Wörhoff, R. Heideman, A. Leinse, and M. Hoekman, "TriPleX: a versatile dielectric photonic platform," Advanced Optical Technologies **4**, 189 (2015).

[373] N. C. Harris, Y. Ma, J. Mower, T. Baehr-Jones, D. Englund, M. Hochberg and C. Galland, "Efficient, Compact and Low Loss Thermo-Optic Phase Shifter in Silicon," Opt. Express **22**, 10487 (2014).

[374] C. M. Wilkes, X. Qiang, J. Wang, R. Santagati, S. Paesani, X. Zhou, D. A. B. Miller, G. D. Marshall, M. G. Thompson, and J. L. O'Brien, "60dB high-extinction auto-configured Mach-Zehnder interferometer," Opt. Lett. **41**, 5318 (2016).

[375] R. A. Soref, and B. R. Bennett, "Electro-optical effects in silicon," IEEE J. Quantum Electron. **23**, 123 (1987).

[376] G. T. Reed, G. Mashanovich, F. Y. Gardes, and D. J. Thomson, "Silicon optical modulators," Nat. Photon. **4**, 518 (2010).

[377] H. Du, F. Siong Chau and G. Zhou, "Mechanically-Tunable Photonic Devices with On-Chip Integrated MEMS/NEMS Actuators," Micromachines **7**, 69 (2016).

[378] D. Liang, G. Roelkens, R. Baets, and J. E. Bowers, "Hybrid Integrated Platforms for Silicon Photonics," Materials **3**, 1782 (2010).

[379] D. Liang, and J. E. Bowers, "Recent progress in lasers on silicon," Nat. Photon. **4**, 511 (2010).

[380] S. Keyvaninia, G. Roelkens, D. Van Thourhout, C. Jany, M. Lamponi, A. Le Liepvre, F. Lelarge, D. Make, G.-H. Duan, D. Bordel, and J.-M. Fedeli, "Demonstration of a heterogeneously integrated III-V/SOI single wavelength tunable laser," Opt. Express **21**, 3784 (2013).

[381] M. J. R. Heck, J. F. Bauters, M. L. Davenport, J. K. Doylend, S. Jain, G. Kurczveil, S. Srinivasan, Y. Tang, and J. E. Bowers, "Hybrid silicon photonic integrated circuit technology," IEEE J. Sel. Top. Quantum Electron. **19**, 6100117 (2013).

[382] B. B. Bakir, A. Descos, N. Olivier, D. Bordel, P. Grosse, E. Augendre, L. Fulbert, and J. M. Fedeli, "Electrically driven hybrid Si/III-V Fabry-Perot lasers based on adiabatic mode transformers," Opt. Express **19**, 10317 (2011).

[383] F. Najafi, J. Mower, N. C. Harris, F. Bellei, A. Dane, C. Lee, X. Hu, P. Kharel, F. Marsili, and S. Assefa et al. "On-chip detection of non-classical light by scalable

integration of single-photon detectors," Nat. Commun. **6**, 5873 (2015).

[384] J. Michel, J. Liu, and L. C. Kimerling, "High-performance Ge-on-Si photodetectors," Nat. Photon. **4**, 527 (2010).

[385] F. Raffaelli, G. Ferranti, D. H Mahler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G. Thompson, and J. C. F. Matthews, "A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers," Quantum Sci. Technol. **3**, 025003 (2018).

[386] P. Sibson, J. E. Kennard, S. Stanisic, C. Erven, J. L. O'Brien, and M. G. Thompson, "Integrated silicon photonics for high-speed quantum key distribution," Optica **4**, 172 (2017).

[387] C. Ma, W. D. Sacher, Z. Tang, J. C. Mikkelsen, Y. Yang, F. Xu, T. Thiessen, H.-K. Lo, J. K. S. Poon, "Silicon photonic transmitter for polarization-encoded quantum key distribution," Optica **3**, 1274 (2016).

[388] J. Leuthold, C. Koos, and W. Freude, "Nonlinear silicon photonics," Nat. Photon. **4**, 535 (2010).

[389] N. C. Harris, D. Grassani, A. Simbula, M. Pant, M. Galli, T. Baehr-Jones, M. Hochberg, D. Englund, D. Bajoni, and C. Galland, "Integrated Source of Spectrally Filtered Correlated Photons for Large-Scale Quantum Photonic Systems," Phys. Rev. X **4**, 041047 (2014).

[390] H. Wang, Z.-C. Duan, Y.-H. Li, Si Chen, J.-P. Li, Y.-M. He, M.-C. Chen, Yu He, X. Ding, and Cheng-Zhi Peng et al. "Near-Transform-Limited Single Photons from an Efficient Solid-State Quantum Emitter," Phys. Rev. Lett. **116**, 213601 (2016).

[391] N. Somaschi, V. Giesz, L. De Santis, J. C. Loredo, M. P. Almeida, G. Hornecker, S. L. Portalupi, T. Grange, C. Anton, J. Demory, et al. 'Near-optimal single-photon sources in the solid state," Nat. Photon. **10**, 340 (2016).

[392] L. Hanschke, K. A. Fischer, S. Appel, Da. Lukin, J. Wierzbowski, S. Sun, R. Trivedi, J. Vuckovic, J. J. Finley, and K. Müller, "Quantum dot single-photon sources with ultra-low multi-photon probability," npj Quantum Information **4**, 43 (2018).

[393] Q. Xu and M. Lipson, "Carrier-induced optical bistability in silicon ring resonators," Opt. Lett. **31**, 341–343 (2006).

[394] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, "Detecting single infrared photons with 93% system efficiency," Nat. Photon. **7**, 210 (2013).

[395] S. F. Preble, M. L. Fanto, J. A. Steidle, C. C. Tison, G. A. Howland, Z. Wang, and P. M. Alsing, "On-Chip Quantum Interference from a Single Silicon Ring-Resonator Source," Phys. Rev. Applied **4**, 1 (2015).

[396] Y.-H. Li, Z.-Y. Zhou, L.-T. Feng, W.-T. Fang, S.-l. Liu, S.-K. Liu, K. Wang, X.-F. Ren, D.-S. Ding, L.-X. Xu, and B.-S. Shi, "On-Chip Multiplexed Multiple Entanglement Sources in a Single Silicon Nanowire," Phys. Rev. Applied **7**, 064005 (2017).

[397] S. Fathpour, "Emerging heterogeneous integrated photonic platforms on silicon Nanophotonics," Nanophotonics **4**, 143 (2015).

[398] J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography," New J. Phys. **4**, 82 (2002).

[399] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. Leeb, and A. Zeilinger, "Long-distance quantum communication with entangled photons using satellites," IEEE J. Sel. Top. Quantum Electron. **9**, 1541–1551 (2003).

[400] M. Pfennigbauer, M. Aspelmeyer, W. R. Leeb, G. Baister, T. Dreischer, T. Jennewein, G. Neckamm, J. M. Perdigues, H. Weinfurter, and A. Zeilinger, "Satellite-based quantum communication terminal employing state-of-the-art technology," Journal of Optical Networking **4**, 549 (2005).

[401] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, and P. Villoresi, "Feasibility Analysis for Quantum Key Distribution between a LEO Satellite and Earth, in Quantum Communication and Quantum Networking," vol. 36 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, eds. A. Sergienko, S. Pascazio, and P. Villoresi, Springer Berlin Heidelberg, pp. 96–99 (2010).

[402] A. Tomaello, C. Bonato, V. Da Deppo, G. Naletto, and P. Villoresi, "Link budget and background noise for satellite quantum key distribution," Advances in Space Research **47**, 802–810 (2011).

[403] R. Ursin, T. Jennewein, J. Kofler, J. M. Perdigues, L. Cacciapuoti, C. J. de Matos, M. Aspelmeyer, A. Valencia, T. Scheidl, and A. Acin et al. "Space-quest, experiments with quantum entanglement in space," Europhys. News **40**, 26 (2009).

[404] T. Scheidl, E. Wille, and R. Ursin, "Quantum optics experiments using the International Space Station: A proposal," New J. Phys. **15**, 1 (2013).

[405] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, "A step towards global key distribution," Nature **419**, 450 (2002).

[406] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," New J. Phys. **4**, 43 (2002).

[407] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, and P. Trojek et al. "Entanglement-based quantum communication over 144 km," Nat. Phys. **3**, 481 (2007).

[408] R. Fante, "Electromagnetic beam propagation in turbulent media," Proceedings of the IEEE **63**, 1669 (1975).

[409] L. C. Andrews; and R. L. Phillips, "Laser Beam Propagation through Random Media," 2nd Edition, SPIE Optical Engineering Press (2005).

[410] P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, A. Zeilinger, and C. Barbieri, "Experimental verification of the feasibility of a quantum channel between space and Earth," New J. Phys. **10**, 33038 (2008).

[411] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental Satellite Quantum Communications," Phys. Rev. Lett. **115**, 040502 (2015).

[412] G. Vallone, D. Dequal, M. Tomasin, F. Vedovato, M. Schiavon, V. Luceri, G. Bianco, and P. Villoresi, "Interference at the Single Photon Level Along Satellite-Ground Channels," Phys. Rev. Lett. **116**, 253601 (2016).

[413] D. K. Oi, A. Ling, G. Vallone, P. Villoresi, S. Greenland, E. Kerr, M. Macdonald, H. Weinfurter, H. Kuiper, E. Charbon, and R. Ursin, "CubeSat quantum com-

munications mission," EPJ Quantum Technology **4**, 6 (2017).

[414] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," npj Quantum Information **3**, 30 (2017).

[415] A. E. Siegman, "Lasers" (University Science Books, 1986).

[416] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, and P. Villoresi, "Feasibility of satellite quantum key distribution," New J. Phys. **11**, 45017 (2009).

[417] D. Bacco, M. Canale, N. Laurenti, G. Vallone, and P. Villoresi, "Experimental quantum key distribution with finite-key security analysis for noisy channels," Nat. Commun. **4**, 2363 (2013).

[418] J. H. Shapiro, "Near-field turbulence effects on quantum-key distribution," Phys. Rev. A **67**, 022309 (2003).

[419] J. H. Shapiro, "Scintillation has minimal impact on far-field Bennett-Brassard 1984 protocol quantum key distribution," Phys. Rev. A **84**, 032340 (2011).

[420] H. Xin, "Chinese Academy Takes Space Under Its Wing," Science **332**, 904 (2011).

[421] J. G. Ren, P. Xu, H. L. Yong, L. Zhang, S. K. Liao, J. Yin, W. Y. Liu, W. Q. Cai, M. Yang, and L. Li et al., "Ground-to-satellite quantum teleportation," Nature **549**, 70–73 (2017).

[422] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren,J. Yin, Q. Shen, Y. Cao, and Z.-P. Li et al., "Satellite-to-ground quantum key distribution," Nature **549**, 43 (2017).

[423] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, and H. Dai et al., "Satellite-based entanglement distribution over 1200 kilometers," Science **356**, 1140 (2017).

[424] J. Yin, Y. Cao, Y. H. Li, J. G. Ren, S. K. Liao, L. Zhang, W. Q. Cai, W. Y. Liu, B. Li, and H. Dai et al., "Satellite-to-Ground Entanglement-Based Quantum Key Distribution," Phys. Rev. Lett. **119**, 200501 (2017).

[425] S. K. Liao, J. Lin, J. G. Ren, W. Y. Liu, J. Qiang, J. Yin, Y. Li, Q. Shen, L. Zhang, and X. F. Liang et al., "Space-to-Ground Quantum Key Distribution Using a Small-Sized Payload on Tiangong-2 Space Lab," Chin. Phys. Lett. **34**, 090302 (2017).

[426] H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima, "Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite," Nat. Photon. **11**, 502 (2017).

[427] Z. Tang, R. Chandrasekara, Y. Y. Sean, C. Cheng, C. Wildfeuer, and A. Ling, "Near-space flight of a correlated photon system," Sci. Rep. **4**, 6366 (2015).

[428] Z. Tang, R. Chandrasekara, Y. C. Tan, C. Cheng, L. Sha, G. C. Hiang, D. K. L. Oi, and A. Ling, "Generation and Analysis of Correlated Pairs of Photons aboard a Nanosatellite," Phys. Rev. Applied **5**, 054022 (2016).

[429] D. Dequal, G. Vallone, D. Bacco, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental single-photon exchange along a space link of 7000 km," Phys. Rev. A **93**, 010301 (2016).

[430] L. Calderaro, C. Agnesi, D. Dequal, F. Vedovato, M. Schiavon, A. Santamato, V. Luceri, G. Bianco, G. Vallone, and P. Villoresi, "Towards Quantum Communication from Global Navigation Satellite System," Quantum Sci. Technol. **4**, 015012 (2019).

[431] K. Günthner, I. Khan, D. Elser, B. Stiller, Ö. Bayraktar, C. R. Müller, K. Saucke, D. Tröndle, F. Heine, S. Seel, and P. Greulich et. al., "Quantum-limited measurements of optical signals from a geostationary satellite," Optica **4**, 611 (2017).

[432] S. K. Liao, H. L. Yong, C. Liu, G. L. Shentu, D. D. Li, J. Lin, H. Dai, S. Q. Zhao, B. Li, and J. Y. Guan et al., "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," Nat. Photon. **11**, 509 (2017).

[433] H.-L. Yin, Y. Fu, H. Liu, Q.-J. Tang, J. Wang, L.-X. You, W.-J. Zhang, S.-J. Chen, Z. Wang, and Q. Zhang et al., "Experimental quantum digital signature over 102 km ," Phys. Rev. A **95**, 032334 (2017).

[434] J. F. Fitzsimons, "Private quantum computation: an introduction to blind quantum computing and related protocols," npj Quantum Information **3**, 23 (2017).

[435] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, "Satellite-based continuous-variable quantum communications: State of-the-art and a predictive outlook," IEEE Communications Surveys & Tutorials **21**, 881-919 (2019).

[436] N. Hosseinidehaj, R. Malaney, "Gaussian entanglement distribution via satellite," Phys. Rev. A **91**, 022304 (2015).

[437] N. Hosseinidehaj and R. Malaney, "Entanglement generation via non-Gaussian transfer over atmospheric fading channels," Phys. Rev. A **92**, 062336 (2015).

[438] N. Hosseinidehaj and R. Malaney, "CV-QKD with Gaussian and Non-Gaussian Entangled States over Satellite-Based Channels," 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 2016.

[439] C. Agnesi, F. Vedovato, M. Schiavon, D. Dequal, L. Calderaro, M. Tomasin, D. G. Marangon, A. Stanco, V. Luceri, and G. Bianco et al. "Exploring the boundaries of quantum mechanics: advances in satellite quantum communications," Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences **376**, 20170461 (2018).

[440] D. Rideout, T. Jennewein, G. Amelino-Camelia, T. F. Demarie, B. L. Higgins, A. Kempf, A. Kent, R. Laflamme, X. Ma, and R. B. Mann et al., "Fundamental quantum optics experiments conceivable with satellites reaching relativistic distances and velocities," Classical and Quantum Gravity **29**, 224011 (2012).

[441] D. E. Bruschi, T. C. Ralph, I. Fuentes, T. Jennewein, and M. Razavi, "Spacetime effects on satellite-based quantum communications," Phys. Rev. D **90**, 045041 (2014).

[442] D. E. Bruschi, A. Datta, R. Ursin, T. C. Ralph, and I. Fuentes, "Quantum estimation of the Schwarzschild spacetime parameters of the Earth," Phys. Rev. D **90**, 124001 (2014).

[443] J. Kohlrus, D. E. Bruschi, J. Louko, and I. Fuentes, "Quantum communications and quantum metrology in the spacetime of a rotating planet," EPJ Quantum Technology **4**,7 (2017).

[444] J. Kohlrus, D. E. Bruschi, and I. Fuentes, "Quantum-metrology estimation of spacetime parameters of the Earth outperforming classical precision," Phys. Rev. A **99**, 032350 (2019).

[445] F. Vedovato, C. Agnesi, M. Schiavon, D. Dequal, L. Calderaro, M. Tomasin, D. G. Marangon, A. Stanco,

V. Luceri, and G. Bianco et al., "Extending Wheeler's delayed-choice experiment to space," Science Advances **3**, e1701180 (2017).

[446] J. S. Bell, "On the Einstein-Podolsky-Rosen paradox," Physics **1**, 195 (1964).

[447] J. Gallicchio, A. S. Friedman, and D. I. Kaiser, "Testing Bell's Inequality with Cosmic Photons: Closing the Setting-Independence Loophole," Phys. Rev. Lett. **112**, 110405 (2014).

[448] J. Handsteiner, A. S. Friedman, D. Rauch, J. Gallicchio, B. Liu, H. Hosp, J. Kofler, D. Bricher, M. Fink, C. Leung, et al., "Cosmic Bell Test: Measurement Settings from Milky Way Stars," Phys. Rev. Lett. **118**, 060401 (2017).

[449] D. Rauch, J. Handsteiner, A. Hochrainer, J. Gallicchio, A. S. Friedman, C. Leung, B. Liu, L. Bulla, S. Ecker, F. Steinlechner, et al., "Cosmic Bell Test using Random Measurement Settings from High-Redshift Quasars," Phys. Rev. Lett. **121**, 080403 (2018).

[450] T. Inagaki, N. Matsuda, O. Tadanaga, M. Asobe, and H. Takesue, "Entanglement distribution over 300 km of fiber," Opt. Express **21**, 23241 (2013).

[451] J. A. Formaggio, D. I. Kaiser, M. M. Murskyj, T. E. Weiss, "Violation of the Leggett-Garg Inequality in Neutrino Oscillations," Phys. Rev. Lett. **117**, 050402 (2016).

[452] J. A. Wheeler, "The "past" and the "delayed-choice" double-slit experiment," in Mathematical Foundations of Quantum Theory, A. R. Marlow, Ed. Academic Press, (1978).

[453] X.-s. Ma, J. Kofler, A. Zeilinger, "Delayed-choice gedanken experiments and their realizations," Rev. Mod. Phys. **88**, 015005 (2016).

[454] V. Jacques, E. Wu, F. Grosshans, F. Treussart, P. Grangier, A. Aspect, and J.-F. Roch, "Experimental realization of Wheeler's delayed-choice GedankenExperiment," Science **315**, 966 (2007).

[455] T. C. Ralph, "Continuous variable quantum cryptography," Phys. Rev. A **61**, 010303 (1999).

[456] T. C. Ralph, "Security of continuous-variable quantum cryptography," Phys. Rev. A **62**, 062306 (2000).

[457] M. Hillery, "Quantum cryptography with squeezed states," Phys. Rev. A **61**, 022309 (2000).

[458] M. D. Reid, "Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations," Phys. Rev. A **62**, 062308 (2000).

[459] N. J. Cerf, M. Lévy, and G. V. Assche, "Quantum distribution of Gaussian keys using squeezed states," Phys. Rev. A **63**, 052311 (2001).

[460] G. Van Assche, J. Cardinal, and N. Cerf, "Reconciliation of a Quantum-Distributed Gaussian Key," IEEE Trans. Inf. Theory **50**, 3940 (2004).

[461] D. Gottesman and J. Preskill, "Secure quantum key distribution using squeezed states," Phys. Rev. A **63**, 022309 (2001).

[462] F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States," Phys. Rev. Lett. **88**, 057902 (2002).

[463] F. Grosshans and P. Grangier, "Quantum cloning and teleportation criteria for continuous quantum variables," Phys. Rev. A **64**, 010301 (2001).

[464] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, "Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit," Phys. Rev. Lett. **89**, 167901 (2002).

[465] F. Grosshans and P. Grangier, "Reverse reconciliation protocols for quantum cryptography with continuous variables," arXiv preprint quant-ph/0204127 (2002).

[466] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum Cryptography Without Switching," Phys. Rev. Lett. **93**, 170504 (2004).

[467] M. Navascués, F. Grosshans, and A. Acín, "Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography," Phys. Rev. Lett. **97**, 190502 (2006).

[468] R. García-Patrón and N. J. Cerf, "Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution," Phys. Rev. Lett. **97**, 190503 (2006).

[469] S. Pirandola, S.Lloyd and S.L. Braunstein, "Characterization of Collective Gaussian Attacks and Security of Coherent-State Quantum Cryptography," Phys. Rev. Lett. **101**, 200504 (2008).

[470] R. García-Patrón, "Quantum information with optical continuous variables," Ph.D. thesis, Université Libre de Bruxelles (2007).

[471] V. Usenko and R. Filip, "Trusted Noise in Continuous-Variable Quantum Key Distribution: A Threat and a Defense," Entropy **18**, 20 (2016).

[472] F. Laudenbach and C. Pacher, "Analysis of the Trusted-Device Scenario in Continuous-Variable Quantum Key Distribution," Advanced Quantum Technologies **2**, 1900055 (2019).

[473] N. Hosseinidehaj, N. Walk, and T. C. Ralph, "Optimal realistic attacks in continuous-variable quantum key distribution," Phys. Rev. A **99**, 052336 (2019).

[474] Z. Pan, K. P. Seshadreesan, W. Clark, M. R. Adcock, I. B. Djordjevic, J. H. Shapiro, and S. Guha, "Secret key distillation across a quantum wiretap channel under restricted eavesdropping," preprint arXiv:1903.03136 (2019).

[475] Y. Guo, Q. Liao, Y. Wang, D. Huang, P. Huang, and G. Zeng, "Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction," Phys. Rev. A **95**, 032304 (2017).

[476] Y. Guo, W. Ye, H. Zhong, and Q. Liao, "Continuous-variable quantum key distribution with non-Gaussian quantum catalysis," Phys. Rev. A **99**, 032327 (2019).

[477] M. Ghalaii, C. Ottaviani, R. Kumar, S. Pirandola, M. Razavi, "Long-distance continuous-variable quantum key distribution with quantum scissors," IEEE J. Sel. Topics Quantum Electron. **26**, 6400212 (2020).

[478] P. Papanastasiou, C. Weedbrook, and S. Pirandola, "Continuous-variable quantum key distribution in fast fading channels," Phys. Rev. A **97**, 032311 (2018).

[479] S. Tserkis, N. Hosseinidehaj, N. Walk, and T. C. Ralph, "Teleportation-based collective attacks in Gaussian quantum key distribution," preprint arXiv:1908.07665 (2019).

[480] V. C. Usenko, "Generalized security analysis framework for continuous-variable quantum key distribution," preprint arXiv:1908.01127 (2019).

[481] M. Lasota, R. Filip, and V. C. Usenko, "Robustness of quantum key distribution with discrete and continuous variables to channel noise," Phys. Rev. A **95**, 062312 (2017).

[482] R. García-Patrón and N. J. Cerf, "Continuous-Variable Quantum Key Distribution Protocols Over Noisy Channels," Phys. Rev. Lett. **102**, 130501 (2009).

[483] R. García-Patrón, S. Pirandola, S. Lloyd, and J. H. Shapiro, "Reverse Coherent Information," Phys. Rev. Lett. **102**, 210501 (2009).

[484] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, "Continuous variable quantum key distribution with modulated entangled states," Nat. Commun. **3**, 1083 (2012).

[485] C. Ottaviani, R. Laurenza, T. P. W. Cope, G. Spedalieri, S. L. Braunstein, S. Pirandola, "Secret key capacity of the thermal-loss channel: improving the lower bound," SPIE proceedings Quantum Information Science and technology II, **9996**, 999609 (2016).

[486] G. Wang, C. Ottaviani, H. Guo, S. Pirandola, "Improving the lower bound to the secret-key capacity of the thermal amplifier channel," Eur. Phys. J. D **73**, 17 (2019).

[487] S. Pirandola, S. L Braunstein, R. Laurenza, C. Ottaviani, T. P. W. Cope, G. Spedalieri, and L. Banchi, "Theory of channel simulation and bounds for private communication," Quantum Sci. Technol. **3**, 035009 (2018).

[488] A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," Phys. Rev. A **81**, 062343 (2010).

[489] L. Ruppert, V. C. Usenko, and R. Filip, "Long-distance continuous-variable quantum key distribution with efficient channel estimation," Phys. Rev. A **90**, 062310 (2014).

[490] O. Thearle, S. M. Assad, and T. Symul, "Estimation of output-channel noise for continuous-variable quantum key distribution," Phys. Rev. A **93**, 042343 (2016).

[491] F. Furrer, "Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle," Phys. Rev. A **90**, 042325 (2014).

[492] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, "Security of continuous-variable quantum key distribution against general attacks," Phys. Rev. Lett. **110**, 030502 (2013).

[493] S. Pirandola, S. Mancini, S. Lloyd, S. L. Braunstein, "Continuous Variable Quantum Cryptography using Two-Way Quantum Communication," Nat. Phys. **4**, 726 (2008).

[494] C. Ottaviani, S. Mancini, and S. Pirandola, "Gaussian two-mode attacks in one-way quantum cryptography," Phys. Rev. A **92**, 062323 (2015).

[495] C. Ottaviani and S. Pirandola, "General immunity and superadditivity of two-way Gaussian quantum cryptography," Sci. Rep **6**, 22225 (2016).

[496] M. M. Wolf, G. Giedke, and J. I. Cirac, "Extremality of Gaussian Quantum States," Phys. Rev. Lett. **96**, 080502 (2006).

[497] S. Pirandola, "Entanglement reactivation in separable environments," New J. Phys. **15**, 113046 (2013).

[498] Q. Zhuang, Z. Zhang, N. Lütkenhaus, and J. H. Shapiro, "Security-proof framework for two-way Gaussian quantum-key-distribution protocols," Phys. Rev. A **98**, 032332 (2018).

[499] S. Ghorai, E. Diamanti, A. Leverrier, "Composable security of two-way continuous-variable quantum key distribution without active symmetrization," Phys. Rev. A **99**, 012311 (2019).

[500] M. Sun, X. Peng, Y. Shen, and H. Guo, "Security of new two-way continuous-variable quantum key distribution protocol," Int. J. Quantum Inf. **10**, 1250059 (2012).

[501] Y. Zhang, Z. Li, Y. Zhao, S. Yu, and H. Guo, " Numerical simulation of the optimal two-mode attacks for two-way continuous-variable quantum cryptography in reverse reconciliation," J. Phys. B: At., Mol., Opt. Phys. 50, 035501 (2017).

[502] Y. C. Zhang, Z. Li, C. Weedbrook, S. Yu, W. Gu, M. Sun, X. Peng, and H. Guo, " Improvement of two-way continuous-variable quantum key distribution using optical amplifiers," J. Phys. B **47**, 035501 (2014).

[503] Z. Zhang, M. Tengner, T. Zhong, F. N. Wong, and J. H. Shapiro, "Entanglement's benefit survives an entanglementbreaking channel," Phys. Rev. Lett. **111**, 010501 (2013).

[504] Q. Zhuang, Z. Zhang, J. Dove, F. N. C. Wong, and J. H. Shapiro, "Floodlight quantum key distribution: A practical route to gigabit-per-second secret-key rates," Phys. Rev. A **94**, 012322 (2016).

[505] Q. Zhuang, Z. Zhang, and J. H. Shapiro, "High-order encoding schemes for floodlight quantum key distribution," Phys. Rev. A **98**, 012323 (2018).

[506] Z. Zhang, Q. Zhuang, F. N. C. Wong, and J. H. Shapiro, "Floodlight quantum key distribution: Demonstrating a framework for high-rate secure communication," Phys. Rev. A **95**, 012332 (2017).

[507] Z. Zhang, C. Chen, Q. Zhuang, F. N. C. Wong, and J. H. Shapiro, "Experimental quantum key distribution at 1.3 gigabit-per-second secret-key rate over a 10 dB loss channel," Quantum Sci Tech. **3**, 025007 (2018).

[508] R. Filip, "Continuous-variable quantum key distribution with noisy coherent states," Phys. Rev. A **77**, 022310 (2008).

[509] V. C. Usenko and R. Filip, "Feasibility of continuous-variable quantum key distribution with noisy coherent states," Phys. Rev. A **81**, 022318 (2010).

[510] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, "Quantum Cryptography Approaching the Classical Limit," Phys. Rev. Lett. **105**, 110501 (2010).

[511] C. Weedbrook, S. Pirandola, and T. C. Ralph, "Continuous-variable quantum key distribution using thermal states," Phys. Rev. A **86**, 022318 (2012).

[512] C. Weedbrook, C. Ottaviani, S. Pirandola, "Two-way quantum cryptography at different wavelengths," Phys. Rev. A **89**, 012309 (2014).

[513] P. Papanastasiou, C. Ottaviani, and S. Pirandola, "Gaussian one-way thermal quantum cryptography with finite-size effects," Phys. Rev. A **98**, 032314 (2018).

[514] C. Ottaviani, M. J. Woolley, M. Erementchouk, J. F. Federici, P. Mazumder, S. Pirandola, and C. Weedbrook, "Terahertz quantum cryptography," Preprint arXiv:1805.03514v1 (2018). DOI:10.1109/JSAC.2020.2968973

[515] V. C. Usenko and F. Grosshans, "Unidimensional continuous-variable quantum key distribution," Phys. Rev. A **92**, 062337 (2015).

[516] T. Gehring, C. S. Jacobsen, and U. L. Andersen, "Single-quadrature continuous-variable quantum key distribution," Quantum Information and Computation **16**, 1081 (2016).

[517] X. Wang, W. Liu, P. Wang, and Y. Li, "Experimental study on all-fiber-based unidimensional continuous-variable quantum key distribution," Phys. Rev. A **95**,

062330 (2017).
[518] S. Pirandola, A. Serafini, S. Lloyd, "Correlation Matrices of Two-Mode Bosonic Systems," Phys. Rev. A **79**, 052327 (2009).
[519] F. Grosshans, "Collective Attacks and Unconditional Security in Continuous Variable Quantum Key Distribution," Phys. Rev. Lett. **94**, 020504 (2005).
[520] V. C. Usenko, "Unidimensional continuous-variable quantum key distribution using squeezed states," Phys. Rev. A **98**, 032321 (2018).
[521] X. Wang, Y. Cao, P. Wang, and Y. Li, "Advantages of the coherent state compared with squeezed state in unidimensional continuous variable quantum key distribution," Quant. Inf. Proc. **17**, 344 (2018).
[522] P. Wang, X. Wang, J. Li, and Y. Li, "Finite-size analysis of unidimensional continuous-variable quantum key distribution under realistic conditions," Opt. Express **25**, 27995 (2017).
[523] Q. Liao, Y. GuoEmail, C. Xie, D. Huang, P. Huang, and G. Zeng, "Composable security of unidimensional continuous-variable quantum key distribution," Quant. Inf. Proc. **17**, 113 (2018).
[524] A. Leverrier and P. Grangier, "Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation," Phys. Rev. Lett. **102**, 180504 (2009).
[525] Y.-B. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus, "Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks, " Phys. Rev. A **79**, 012307 (2009).
[526] M. Heid and N. Lütkenhaus, "Security of coherent state quantum cryptography in the presence of Gaussian noise," Phys. Rev. A **76**, 022313 (2007).
[527] K. Bradler and C. Weedbrook, "A security proof of continuous-variable QKD using three coherent states," Phys. Rev. A **97**, 022310 (2018).
[528] P. Papanastasiou, C. Lupo, C. Weedbrook, and S. Pirandola, "Quantum key distribution with phase-encoded coherent states: Asymptotic security analysis in thermal-loss channels,' Phys. Rev. A **98**, 012340 (2018).
[529] D. Sych and G. Leuchs, "Coherent state quantum key distribution with multi letter phase-shift keying," New J. Phys. **12**, 053019 (2010).
[530] Q. Liao, Y. Guo, D. Huang, P. Huang and G. Zeng, "Long-distance continuous-variable quantum key distribution using non-Gaussian state-discrimination detection," New J. Phys. **20**, 023015 (2018).
[531] Y. Guo, R. Li, Q. Liao, J. Zhou, and D. Huang, "Performance improvement of eight-state continuous-variable quantum key distribution with an optical amplifier," Phys. Lett. A **382**, 372-381 (2018).
[532] Z. Li, Y. Zhang and H. Guo, "User-defined quantum key distribution," preprint arXiv:1805.04249 (2018).
[533] M. Ghalaii, C. Ottaviani, R. Kumar, S. Pirandola, and M. Razavi, "Discrete-modulation continuous-variable quantum key distribution enhanced by quantum scissors," Preprint arXiv:1907.13405 (2019). DOI:10.1109/JSAC.2020.2969058
[534] U. M. Maurer, "Secret key agreement by public discussion from common information," IEEE Trans. Inf. Theory **39**, 733 (1993).
[535] C. Cachin and U. M. Maurer, "Linking information reconciliation and privacy amplification," J. of Cryptology **10**, 97 (1997).
[536] T. Symul, D. J. Alton, S. M. Assad, A. M. Lance, C. Weedbrook, T. C. Ralph, and P. K. Lam, "Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of Gaussian noise," Phys. Rev. A **76**, 030303(R) (2007).
[537] A. Leverrier and P. Grangier, "Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation," Phys. Rev. A **83**, 042312 (2011).
[538] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, "Asymptotic security of continuous-variable quantum key distribution with a discrete modulation," Phys. Rev. X **9**, 021059 (2019).
[539] P. Papanastasiou, and S. Pirandola, "Continuous-variable quantum cryptography with discrete alphabets: Composable security under collective Gaussian attacks," Preprint arXiv:1912.11418 (2019).
[540] Zhengyu Li, Yi-Chen Zhang, Feihu Xu, Xiang Peng, and Hong Guo, "Continuous-Variable Measurement-Device-Independent Quantum Key Distribution," Phys. Rev. A **89**, 052301 (2014).
[541] G. Spedalieri, C. Ottaviani, S. Pirandola, "Covariance matrices under Bell-like detections," Open Syst. Inf. Dyn. **20**, 1350011 (2013).
[542] C. Ottaviani, G. Spedalieri, S. L. Braunstein and S. Pirandola, "Continuous-variable quantum cryptography with an untrusted relay: Detailed security analysis of the symmetric configuration," Phys. Rev. A **91**, 022320 (2015).
[543] G. Spedalieri, C. Ottaviani, S. L Braunstein, T.Gehring, C. S. Jacobsen, U. L Andersen, S. Pirandola, "Quantum cryptography with an ideal local relay," Proceeding SPIE Security + Defence, 9648 (2015).
[544] P. Papanastasiou, C. Ottaviani, and S. Pirandola, "Finite-size analysis of measurement-device-independent quantum cryptography with continuous variables," Phys. Rev. A **96**, 042332 (2017).
[545] X. Zhang, Y.-C. Zhang, Y. Zhao, X. Wang, S. Yu, H. Guo, "Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution," Phys. Rev. A **96**, 042334 (2017).
[546] M. Tomamichel, "A Framework for Non-Asymptotic Quantum Information Theory," Ph.D. thesis, Swiss Federal Institute of Technology (ETH), Zurich, 2012, arXiv:1203.2142.
[547] J. Eisert, S. Scheel, and M. B. Plenio, "Distilling Gaussian States with Gaussian Operations is Impossible," Phys. Rev. Lett. **89**, 137903 (2002).
[548] Y. Zhang, Z. Li, C. Weedbrook, K. Marshall, S. Pirandola, S. Yu, and H. Guo, "Noiseless linear amplifiers in entanglement-based continuous-variable quantum key distribution," Entropy **17**, 4547-4562 (2015).
[549] Y. Zhao, Y. Zhang, B. Xu, S. Yu, and H. Guo, "Continuous-variable measurement-device-independent quantum key distribution with virtual photon subtraction," Phys. Rev. A **97**, 042328 (2018).
[550] H.-X. Ma, P. H., D.-Y. Bai, S.-Y. Wang, W.-S. Bao, and G.-H. Zeng, "Continuous-variable measurement-device-independent quantum key distribution with photon subtraction," Phys. Rev. A **97**, 042329 (2018).
[551] Y.-C. Zhang, Z. Li, S. Yu, W. Gu, X. Peng, and H. Guo, "Continuous-variable measurement-device-independent quantum key distribution using squeezed states," Phys.

Rev. A **90**, 052325 (2014).
[552] Z. Chen, Y. Zhang, G. Wang, Z. Li, and H. Guo, " Composable security analysis of continuous-variable measurement-device-independent quantum key distribution with squeezed states for coherent attacks," Phys. Rev. A **98**, 012314 (2018).
[553] P. Wang, X. Wang, and Y. Li, "Continuous-variable measurement-device-independent quantum key distribution using modulated squeezed states and optical amplifiers," Phys. Rev. A **99**, 042309 (2019).
[554] H.-X. Ma, P. Huang, D.-Y. Bai, T. Wang, S.-Y. Wang, W.-S. Bao, G.-H. Zeng, "Long-distance continuous-variable measurement-device-independent quantum key distribution with discrete modulation," Phys. Rev. A 99, 022322 (2019).
[555] H.-L. Yin, W. Zhu, and Y. Fu, "Phase self-aligned continuous-variable measurement-device-independent quantum key distribution," Sci. Rep. **9**, 49 (2019).
[556] H.-X. Ma, P. Huang, T. Wang, D.-Y. Bai, S.-Y. Wang, W.-S. Bao, and G.-H. Zeng, "Security bound of continuous-variable measurement-device-independent quantum key distribution with imperfect phase reference calibration", preprint arXiv:1904.09786 (2019).
[557] Q. Liao, Y. Wang, D. Huang, and Y. Guo, "Dual-phase-modulated plug-and-play measurement-device-independent continuous-variable quantum key distribution," Optics Express **26**, 19907-19920 (2018).
[558] Y. Guo, Q. Liao, D. Huang, and G. Zeng, "Quantum relay schemes for continuous-variable quantum key distribution," Phys. Rev. A **95**, 042326 (2017).
[559] N. Hosseinidehaj and R. Malaney, "CV-MDI Quantum Key Distribution via Satellite," Quant. Inf. Comput. **17**, 361-379 (2017).
[560] D. Bai, P. Huang, Y. Zhu, H. Ma, T. Xiao, T. Wang, and G. Zeng, "Unidimensional continuous-variable measurement-device-independent quantum key distribution," Preprint arXiv:1905.09029 (2019).
[561] C. Ottaviani, C. Lupo, R. Laurenza, and S. Pirandola, "Modular network for high-rate quantum conferencing," Commun. Phys. **2**, 118 (2019); See also preprint arXiv:1709.06988 (2017).
[562] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," Phys. Rev. A **59**, 1829 (1999).
[563] R. Cleve, D. Gottesman, and H.-K. Lo, "How to Share a Quantum Secret," Phys. Rev. Lett. **83**, 648 (1999).
[564] D. Markham, and B. C. Sanders, "Graph States for Quantum Secret Sharing," Phys. Rev. A **78**, 042309 (2008).
[565] D. Markham, and B. C. Sanders, "Erratum: Graph States for Quantum Secret Sharing," Phys. Rev. A **83**, 019901 (2011).
[566] A. Keet, B. Fortescue, D. Markham, and B. C. Sanders, "Quantum secret sharing with qudit graph states," Phys. Rev. A **82**, 062315 (2010).
[567] J. Ribeiro, G. Murta, and S. Wehner, "Fully device independent Conference Key Agreement," preprint arXiv:1708.00798 (2017).
[568] F. Grasselli, H. Kampermann and D. Bruß, "Conference key agreement with single-photon interference," preprint arxiv:1907.10288 (2019).
[569] Y. Wu, J. Zhou, X. Gong, Y. Guo, Z.-M. Zhang, and G. He, "Continuous-variable measurement-device-independent multipartite quantum communication," Phys. Rev. A **93**, 022325 (2016).
[570] P. van Loock and Samuel L. Braunstein, "Multipartite Entanglement for Continuous Variables: A Quantum Teleportation Network," Phys. Rev. Lett. **84**, 3482 (2000).
[571] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-Variable Quantum Key Distribution with Gaussian Modulation – The Theory of Practical Implementations," Adv. Quantum Technol. 1800011 (2018).
[572] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and Ph. Grangier,"Quantum key distribution using gaussian-modulated coherent states," Nature **421**, 238 (2003).
[573] A. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, "No-Switching Quantum Key Distribution Using Broadband Modulated Coherent Light," Phys. Rev. Lett. **95**, 180503 (2005).
[574] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, "Controlling excess noise in fiber-optics continuous-variable quantum key distribution," Phys. Rev. A **72**, 050303 (2005).
[575] S. Lorenz, N. Korolkova, and G. Leuchs, "Continuous-variable quantum key distribution using polarization encoding and post selection," App. Phys. B **79**, 273, (2004).
[576] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, "Long-distance continuous-variable quantum key distribution with a Gaussian modulation," Phys. Rev. A **84**, 062317 (2011).
[577] D. Huang, D. Lin, C. Wang, W. Liu, S. F.,J. Peng, P. Huang, and G. Zeng, "Continuous-variable quantum key distribution with 1 Mbps key rate," Opt. Express **23**, 17511 (2015).
[578] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, "High-speed continuous-variable quantum key distribution without sending a local oscillator," Opt. Lett. **40**, 3695 (2015).
[579] D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," Sci. Rep. **6**, 19201 (2016).
[580] Y.-M. Li, X.-Y. Wang, Z.-L. Bai, W.-Y. Liu, S.-S. Yang, and K.-C. Peng, "Continuous variable quantum key distribution," Chin. Phys. B **26**, 040303 (2017).
[581] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," Nat. Photon. **7**, 378, (2013).
[582] F. Laudenbach, B. Schrenk, C. Pacher, M. Hentschel, C. H. F. Fung, F. Karinou, A. Poppe, M. Peev, H. Hübel, "Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator," Quantum **3**, 193 (2019).
[583] B. Qi, L. L. Huang, L. Qian, and H.-K Lo, "Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers," Phys. Rev. A **76**, 052323 (2007).
[584] Y. Shen, Y. Chen, H. Zou, and J. Yuan, "A fiber-based quasi-continuous-wave quantum key distribution system," Sci. Rep. **4**, 4563 (2014).
[585] X. Y. Wang, Z.-L. Bai, S.-F. Wang, Y.-M Li, and K.-C. Peng, "Four-state modulation continuous variable quantum key distribution over a 30-km fiber and analysis of

excess noise," Chin. Phys. Lett. **30**, 1 (2013).

[586] Q.-D. Xuan, Z. Zhang, and P.-L. Voss, "A 24 km fiber-based discretely signaled continuous variable quantum key distribution system," Opt. Express **17**, 24244 (2009).

[587] T. Hirano et al., "Implementation of continuous variable quantum key distribution with discrete modulation," Quantum Sci. Technol. **2**, 024010 (2017).

[588] H. H. Brunner et al, "A Low-complexity heterodyne CV-QKD architecture," 19th International Conference on Transparent Optical Networks (ICTON) (2017).

[589] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, and S. W. McLaughlin et al., "Quantum key distribution over 25 km with an all-fiber continuous-variable system," Phys. Rev. A **76**, 042305 (2007).

[590] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache, and P. Painchault, "Field Test of Classical Symmetric Encryption with Continuous Variable Quantum Key Distribution," Opt. Express **20**, 14030, (2012).

[591] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, "Field test of a continuous-variable quantum key distribution prototype," New J. Phys. **11**, 045023 (2009).

[592] F. Karinou et al., "Toward the integration of CV Quantum key distribution in deployed optical networks," IEEE Photon. Tech. Lett. **30**, 1041 (2018).

[593] T.A. Eriksson et al., "Coexistence of Continuous Variable Quantum Key Distribution and 7x12.5 Gbit/s Classical Channels," IEEE Photonics Society Summer Topical Meeting Series (2018).

[594] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang, et al., "Continuous-variable QKD over 50km commercial fiber," Quantum Sci. Technol. **4** 035006 (2019).

[595] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, "Long-distance continuous-variable quantum key distribution over 202.81 km fiber," Preprint arxiv:2001.02555 (2020).

[596] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, "Self-referenced continuous-variable quantum key distribution protocol," Phys. Rev. X **5**, 041010 (2015).

[597] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, "Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection," Phys. Rev. X **5**, 041009 (2015).

[598] S. Kleis, M. Rückmann, and C. G.Schäffer "Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals," Opt. Lett. **42**, 1588 (2017).

[599] T. Wang, P. Huang, Y. Zhou, W. Liu, H. Ma, S. Wang, and G. Zeng, "High key rate continuous-variable quantum key distirbution with a real local oscillator," Opt. Express **26**, 2794 (2018).

[600] Y. Li, N. Wang, X. Wang, and Z. Bai, "Influence of guided acoustic wave Brillouin scattering on excess noise in fiber-based continuous variable quantum key distribution," J. Opt. Soc. Am. B **31**, 2379 (2014).

[601] D. Huang, J. Fang, C. Wang, P. Huang, and G..H. Zeng. "A 300-MHz bandwidth balanced homodyne detector for continuous variable quantum key distribution," Chin. Phys. Lett. **30**, 114209 (2013).

[602] R. Kumar, E. Barrios, A. MacRae, E. Cairns, E. H. Huntington, and A. I. Lvovsky "Versatile wideband balanced detector for quantum optical homodyne tomography," Optics Commun. **285**, 5259, (2012).

[603] X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, "Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum key distribution systems," Phys. Rev. A **88**, 022339 (2013).

[604] C. Zhou, X. Wang, Y. Zhang, Z. Zhang, S. Yu, H. Guo, "Continuous-Variable Quantum Key Distribution with Rateless Reconciliation Protocol", Phys. Rev. Appl. **12**, 054013 (2019).

[605] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," Phys. Rev. A **77**, 042325 (2008).

[606] D. Lin, D. Huang, P. Huang, J. Peng, and G. Zeng, "High performance reconciliation for continuous variable quantum key distribution with LDPC code," Int. J. of Quantum Info. **13**, 1550010 (2015).

[607] Mario Milicevic, Chen Feng, Lei M Zhang, and P Glenn Gulak, "Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography," npj Quantum Information **4**, 21 (2017).

[608] X. Wang, Y. Zhang, S. Li, B. Xu, S. Yu, and H. Guo, "Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution," Quant. Inf. Comput **17**, 1123-1134 (2017).

[609] X. Wang, Y. Zhang, S. Yu, and H. Guo, "High speed error correction for continuous-variable quantum key distribution with multi-edge type LDPC code," Sci. Rep. **8**, 10543 (2018).

[610] T. Gehring, V. Handchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner and R. Schnabel, "Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks," Nat. Commun. **6**, 8795 (2015).

[611] U.L. Andersen, T. Gehring, C. Marquardt, and G. Leuchs, "30 years of squeezed light generation," Phys. Scr. **91**, 053001 (2016).

[612] C. S. Scheffman, L.S. Madsen, V.C. Usenko, R. Filip, and U.L. Andersen, "Complete elimination of information leakage in continuous-variable quantum communication channels," npj Quantum Information **4**, 32 (2018).

[613] N. Wang, S. Du, W. Liu, X. Wang, Y. Li, and K. Peng, "Long-Distance Continuous-Variable Quantum Key Distribution with Entangled States," Phys. Rev. Applied **10**, 064028 (2018).

[614] M. Tomamichel, R. Colbeck, and R. Renner, "A Fully Quantum Asymptotic Equipartition Property," IEEE Trans. Inf. Theory **55**, 5840 (2009).

[615] M. Christandl, R. König, and R. Renner, "Postselection Technique for Quantum Channels with Applications to Quantum Cryptography," Phys. Rev. Lett. **102**, 020504 (2009).

[616] M. Hayashi and T. Tsurumaru, "Concise and Tight Security Analysis of the Bennett-Brassard 1984 Protocol with Finite Key Lengths," New J. Phys. **14**, 093014 (2012).

[617] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and

R. Renner, T"he Uncertainty Principle in the Presence of Quantum Memory," Nat. Phys. **6**, 659 (2010).

[618] M. Tomamichel and R. Renner, "Uncertainty Relation for Smooth Entropies," Phys. Rev. Lett. **106**, 110506 (2011).

[619] M. Tomamichel and A. Leverrier, "A largely self-contained and complete security proof for quantum key distribution," Quantum **1**, 14 (2017).

[620] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, "Practical device-independent quantum cryptography via entropy accumulation," Nat. Commun. **9**, 459 (2018).

[621] W. Heisenberg, "Über den Anschaulichen Inhalt der Quantentheoretischen Kinematik und Mechanik," Zeitschrift für Phys. **43**, 172 (1927).

[622] H. Maassen and J. Uffink, "Generalized Entropic Uncertainty Relations," Phys. Rev. Lett. **60**, 1103 (1988).

[623] F. Grosshans and N. J. Cerf, "Continuous-Variable Quantum Cryptography is Secure against Non-Gaussian Attacks," Phys. Rev. Lett. **92**, 047905 (2004).

[624] M. Koashi, "Simple Security Proof of Quantum Key Distribution via Uncertainty Principle," arXiv:0505108 (2005).

[625] A. Einstein, B. Podolsky, and N. Rosen, "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?," Phys. Rev. **47**, 777 (1935).

[626] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, "Entropic uncertainty relations and their applications," Rev. Mod. Phys. **89**, 015002 (2017).

[627] F. Furrer, M. Berta, M. Tomamichel, V. B. Scholz, and M. Christandl, "Position-Momentum Uncertainty Relations in the Presence of Quantum Memory," J. Math. Phys. **55**, 122205 (2014).

[628] M. Berta, F. Furrer, and V. B. Scholz, "The Smooth Entropy Formalism for von Neumann Algebras," J. Math. Phys. **57**, 015213 (2016).

[629] H. Everett, ""Relative State" Formulation of Quantum Mechanics," Rev. Mod. Phys. **29**, 454 (1957).

[630] I. I. Hirschman, A Note on Entropy, Am. J. Math. **79**, 152–156 (1957).

[631] L. Rudnicki, S. P. Walborn, and F. Toscano, "Optimal Uncertainty Relations for Extremely Coarse-Grained Measurements," Phys. Rev. A **85**, 042115 (2012).

[632] M. Christandl, R. König, G. Mitchison, and R. Renner, "One-and-a-half quantum de Finetti theorems," Commun. Math. Phys. **273**, 473–498 (2007).

[633] A. Leverrier, "Composable security proof for continuous-variablequantum key distribution with coherent states," Phys. Rev. Lett. **114**, 070501 (2015).

[634] A. Leverrier, "SU(p,q) coherent states and a Gaussian de Finetti theorem," J. Math. Phys.**59**, 042202 (2018).

[635] D. Moody, "Update on the nist post-quantum cryptography project," Tech. rep., National Institute of Standards and Technology (NIST) (2018).

[636] F. Xu, X. Ma. Q. Zhang, H.-K. Lo, and J.-W. Pan, "Quantum cryptography with realistic devices", preprint arXiv:1903.09051 (2019).

[637] M. Lucamarini, A. Shields, R. Allèaume, C. Chunnilall, I. P. Degiovanni, M. Gramegna, A. Hasekioglu, B. Huttner, R. Kumar, A. Lord, et al. "Implementation Security of Quantum Cryptography: Introduction, challenges, solutions," ETSI White Paper No. 27 (2018). Available at https://bit.ly/2Wi4Z4g

[638] V. Scarani and C. Kurtsiefer, "The black paper of quantum cryptography: real implementation problems," Theoretical Computer Science **560**, 27 (2014).

[639] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Theoretical Computer Science **560**, 7 (2014).

[640] A. A. Gaidash, V. I. Egorov, and A. V. Gleim, "Revealing of photon-number splitting attack on quantum key distribution system by photon-number resolving devices," J. of Phys. Conference Series **735**, 012072 (2016).

[641] A. Huang, S.-H. Sun, Z. Liu, and V. Makarov, "Decoy state quantum key distribution with imperfect source," preprint arXiv:1711.00597 (2017).

[642] Y.-Y. Fei, X.-d. Meng, M. Gao, Y. Yang, H. Wang, and Z. Ma, "Strong light illumination on gain-switched semiconductor lasers helps the eavesdropper in practical quantum key distribution systems," Opt. Commun. **419**, 83 (2018).

[643] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," Phys. Rev. A **73**, 022320 (2006).

[644] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, "Risk Analysis of Trojan-Horse Attacks on Practical Quantum Key Distribution System," IEEE J. Sel. Top. Quantum Electron. **21**, 168 (2015).

[645] A. Vakhitov, V. Makarov, and D. R. Hjelme, "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography," J. Mod. Opt. **48**, 2023 (2001).

[646] M. Lucamarini, I. Choi, M. Ward, J. Dynes, Z. Yuan, and A. Shields, "Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution," Phys. Rev. X, **5**, 031030 (2015).

[647] S. Sajeed, C. Minshull, N. Jain, and V. Makarov, "Invisible Trojan-horse attack," Sci. Rep. **7**, 1-7 (2017).

[648] K. Tamaki, M. Curty, and M. Lucamarini, "Decoy-state quantum key distribution with a leaky source," New J. Phys. **18**, 065008 (2016).

[649] S. Vinay and P. Kok, "Burning the Trojan Horse: Defending against Side-Channel Attacks in QKD," Phys. Rev. A **97**, 042335 (2018).

[650] C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter, "The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks?" J. Mod. Opt. **48**, 2039 (2001).

[651] P. V. P. Pinheiro, P. Chaiwongkhot, S. Sajeed, R. T. Horn, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, "Eavesdropping and countermeasures for backflash side channel in quantum cryptography," preprint arXiv:1804.10317 (2018).

[652] A. Meda, I. P. Degiovanni, A. Tosi, Z. L. Yuan, G. Brida, and M. Genovese, "Backflash light characterization to prevent QKD zero-error hacking," "Light: Science & Applications," **6**, e16261 (2017).

[653] V. Makarov and D. R. Hjelme, "Faked states attack on quantum cryptosystems," J. Mod. Opt. **52**, 691 (2005).

[654] M. Stipčević, "Preventing detector blinding attack and other random number generator attacks on quantum cryptography by use of an explicit random number generator," preprint arXiv:1403.0143 (2014).

[655] H.-W. Li, S. Wang, J.-Z. Huang, W. Chen, Z.-Q.Yin, F.-Y. Li, Z. Zhou, D. Liu, Y. Zhang, and G.-C. Guo et al., "Attacking practical quantum key distribution system with wavelength dependent beam splitter and

multi-wavelength sources," Phys. Rev. A **84**, 062308 (2011).

[656] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," Phys. Rev. A **74**, 022313 (2006).

[657] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Thermal blinding of gated detectors in quantum cryptography," Opt. Express **18**, 27938 (2010).

[658] Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Avoiding the blinding attack in QKD," Nat. Photon. **4**, 800 (2010).

[659] Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography," Applied Phys. Lett. **98**, 231104 (2011).

[660] A. Koehler-Sidki, M. Lucamarini, J. F. Dynes, G. L. Roberts, A. W. Sharpe, Z. Yuan, and A. J. Shields, "Intensity modulation as a preemptive measure against blinding of single-photon detectors based on self-differencing cancellation," Phys. Rev. A **98**, 022327 (2018).

[661] A. Koehler-Sidki, J. F. Dynes, M. Lucamarini, G. L. Roberts, A. W. Sharpe, Z. L. Yuan, and A. J. Shields, "Best-Practice Criteria for Practical Security of Self-Differencing Avalanche Photodiode Detectors in Quantum Key Distribution," Phys. Rev. Applied **9**, 044027 (2018).

[662] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, "Time-shift attack in practical quantum cryptosystems," preprint quant-ph/0512080 (2005).

[663] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," Phys. Rev. A **78**, 042333 (2008).

[664] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, "Security proof of quantum key distribution with detection efficiency mismatch," preprint arXiv:0802.3788 (2008).

[665] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, "Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch," Phys. Rev. A **91**, 062301, (2015).

[666] M. Rau, T. Vogl, G. Corrielli, G. Vest, L. Fuchs, S. Nauerth, and H. Weinfurter. "Spatial mode side channels in free-space QKD implementations," IEEE J. Sel. Top. Quantum Electron. **21**, 187 (2015).

[667] L. Lydersen and J. Skaar, "Security of quantum key distribution with bit and basis dependent detector flaws," preprint arXiv:0807.0767 (2008).

[668] M. Koashi, "Unconditional security of quantum key distribution and the uncertainty principle," J. Phys. Conf. Ser. **36**, 98 (2006).

[669] Y.-Y. Fei, X.-d. Meng, M. Gao, Z. Ma, and H. Wang, "Practical decoy state quantum key distribution with detector efficiency mismatch," Eur. Phys. J. D **72**, 107 (2018).

[670] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, "Analysis of imperfections in practical continuous-variable quantum key distribution," Phys. Rev. A **86**, 032309 (2012).

[671] H. Häseler, T. Moroder, and N. Lütkenhaus, "Testing quantum devices: Practical entanglement verification in bipartite optical systems," Phys. Rev. A **77**, 032303 (2008).

[672] J.-Z. Huang, C. Weedbrook, Z.-Q. Yin, S. Wang, H.-W. Li, W. Chen, G.-C. Guo, and Z.-F. Han, "Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack," Phys. Rev. A **87**, 062329 (2013).

[673] X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, "Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol," Phys. Rev. A **87**, 052309 (2013).

[674] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, "Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution," Phys. Rev. A **87**, 062313 (2013).

[675] J.-Z. Huang, S. Kunz-Jacques, P. Jouguet, C. Weedbrook, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, "Quantum hacking on quantum key distribution using homodyne detection," Phys. Rev. A **89**, 032304 (2014).

[676] C. Xie, Y. Guo, Q. Liao, W. Zhao, D. Huang, L. Zhang, and G. Zeng, "Practical security analysis of continuous-variable quantum key distribution with jitter in clock synchronization," Phys. Lett. A **382**, 811 (2018).

[677] Y. Zhao, Y. Zhang, Y. Huang, B. Xu, S. Yu and H. Guo, "Polarization attack on continuous-variable quantum key distribution," J. Phys. B: At. Mol. Opt. Phys. **52**, 015501 (2019).

[678] A. Marie and R. Alléaume, "Self-coherent phase reference sharing for continuous-variable quantum key distribution," Phys. Rev. A **95**, 012316 (2017).

[679] S. Ren, R. Kumar, A. Wonfor, X. Tang, R. Penty, and I. White, "Reference Pulse Attack on Continuous-Variable Quantum Key Distribution with Local Local Oscillator under trusted phase noise," J. Opt. Soc. Am. B **36**, B7 (2019).

[680] H. Qin, R. Kumar, and R. Alléaume, "Quantum hacking: saturation attack on practical continuous-variable quantum key distribution," Phys. Rev. A **94**, 012325 (2016).

[681] J. Fiurášek and N. J. Cerf, "Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution," Phys. Rev. A **86**, 060302 (2012).

[682] N. Walk, T. C. Ralph, T. Symul, and P. K. Lam, "Security of continuous-variable quantum cryptography with Gaussian postselection," Phys. Rev. A **87**, 020303 (2013).

[683] H. Qin, R. Kumar, V. Makarov, and R. Alléaume, "Homodyne detector blinding attack in continuous-variable quantum key distribution," Phys. Rev. A **98**, 012312 (2018).

[684] B. Stiller, I. Khan, N. Jain, P. Jouguet, S. Kunz-Jacques, E. Diamanti, C. Marquardt, and G. Leuchs, "Quantum hacking of continuous-variable quantum key distribution systems: realtime trojan-horse attacks," in CLEO: 2015, OSA, (2015).

[685] I. Derkach, V. C. Usenko, and R. Filip, "Preventing side-channel effects in continuous-variable quantum key distribution," Phys. Rev. A **93**, 032309 (2016).

[686] I. Derkach, V. C. Usenko, and R. Filip, "Continuous-variable quantum key distribution with a leakage from state preparation," Phys. Rev. A **96**, 062309 (2017).

[687] J. Pereira and S. Pirandola, "Hacking Alice's box in

CV-QKD," Phys. Rev. A **98**, 062319 (2018).
[688] H.-X. Ma, W.-S. Bao, H.-W. Li, and C. Chou, "Quantum hacking of two-way continuous-variable quantum key distribution using Trojan-horse attack," Chin. Phys. B **25**, 080309 (2016).
[689] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, "Device Calibration Impacts Security of Quantum Key Distribution," Phys. Rev. Lett. **107**, 110501 (2011).
[690] Y.-y. Fei, X.-d. Meng, M. Gao, H. Wang, and Z. Ma, "Quantum man-in-the-middle attack on the calibration process of quantum key distribution," Sci. Rep. **8**, 4283 (2018).
[691] A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, "Laser Damage Helps the Eavesdropper in Quantum Cryptography," Phys. Rev. Lett. **112**, 070503 (2014).
[692] V. Makarov, J.-P. Bourgoin, P. Chaiwongkhot, M. Gagné , T. Jennewein, S. Kaiser, R. Kashyap, M. Legré, C. Minshull, and S. Sajeed, "Creation of backdoors in quantum communications via laser damage," Phys. Rev. A **94**, 030302 (2016).
[693] S.-H. Sun, F. Xu, M.-S. Jiang, X.-C. Ma, H.-K. Lo, and L.-M. Liang, "Effect of source tampering in the security of quantum cryptography," Phys. Rev. A **92**, 022304 (2015).
[694] M. Daschner, D. I. Kaiser, and J. A. Formaggio, " Exploiting Faraday Rotation to Jam Quantum Key Distribution via Polarized Photons," Preprint arxiv:1905.01359 (2019).
[695] K. Marshall and C. Weedbrook, "Device-independent quantum cryptography for continuous variables," Phys. Rev. A **90**, 042311 (2014).
[696] I. Devetak, M. Junge, C. King, and M. B. Ruskai, "Multiplicativity of Completely Bounded p-Norms Implies a New Additivity Result," Commun. Math. Phys. **266**, 37 (2006).
[697] B. Schumacher and M. A. Nielsen, "Quantum data processing and error correction," Phys. Rev. A **54**, 2629 (1996).
[698] S. Lloyd, "Capacity of the noisy quantum channel," Phys. Rev. A **55**, 1613 (1997).
[699] M. Christandl, "The Structure of Bipartite Quantum States: Insights from Group Theory and Cryptography," PhD thesis, University of Cambridge (2006).
[700] V. Vedral, "The role of relative entropy in quantum information theory," Rev. Mod. Phys. **74**, 197 (2002).
[701] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, "Quantifying Entanglement," Phys. Rev. Lett. **78**, 2275 (1997).
[702] V. Vedral and M. B. Plenio, "Entanglement measures and purification procedures," Phys. Rev. A **57**, 1619 (1998).
[703] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, "Secure Key from Bound Entanglement," Phys. Rev. Lett. **94**, 160502 (2005).
[704] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," IEEE Trans. Inf. Theory **51**, 44 (2005).
[705] R. Laurenza, S. L. Braunstein, and S. Pirandola, "Finite-resource teleportation stretching for continuous-variable systems," Sci. Rep. **8**, 15267 (2018).
[706] E. Chitambar and G. Gour, "Quantum resource theories," Rev. Mod. Phys. **91**, 025001 (2019).
[707] S. Pirandola, and C. Lupo, "Ultimate Precision of Adaptive Noise Estimation," Phys. Rev. Lett. **118**, 100502 (2017).
[708] M. E. Shirokov, "Energy-constrained diamond norms and their use in quantum information theory," Problems of Information Transmission **54**, 20 (2018).
[709] A. Winter, "Energy-constrained diamond norm with applications to the uniform continuity of continuous variable channel capacities," Preprint arXiv:1712.10267 (2017).
[710] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," Phys. Rev. A **54**, 3824 (1996).
[711] G. Bowen and S. Bose, "Teleportation as a Depolarizing Quantum Channel, Relative Entropy, and Classical Capacity," Phys. Rev. Lett. **87**, 267901 (2001).
[712] M. Horodecki, P. Horodecki, and R. Horodecki, "General teleportation channel, singlet fraction, and quasidistillation," Phys. Rev. A **60**, 1888 (1999).
[713] G. Giedke and J. I. Cirac, "Characterization of Gaussian operations and distillation of Gaussian states," Phys. Rev. A **66**, 032316 (2002).
[714] J. Niset, J. Fiurasek, and N. J. Cerf, "No-Go Theorem for Gaussian Quantum Error Correction," Phys. Rev. Lett. **102**, 120501 (2009).
[715] A. Muller-Hermes, "Transposition in quantum information theory," Master's thesis, Technical University of Munich (2012).
[716] D. Leung and W. Matthews, "On the power of PPT-preserving and non-signalling codes," IEEE Trans. Inf. Theory **61**, 4486-4499 (2015).
[717] S. Ishizaka and T. Hiroshima, "Asymptotic Teleportation Scheme as a Universal Programmable Quantum Processor," Phys. Rev. Lett. **101**, 240501 (2008).
[718] S. Ishizaka and T. Hiroshima, "Quantum teleportation scheme by selecting one of multiple output ports," Phys. Rev. A **79**, 042306 (2009).
[719] S. Ishizaka, "Some remarks on port-based teleportation," arXiv:1506.01555 (2015).
[720] M. Studzinski, S. Strelchuk, M.Mozrzymas and M. Horodecki, "Port-based teleportation in arbitrary dimension," Sci. Rep. **7**, 10871 (2017).
[721] S. Pirandola, R. Laurenza, C. Lupo, and J. L. Pereira, "Fundamental limits to quantum channel discrimination," npj Quantum Information **5**, 50 (2019).
[722] S. Pirandola, R. Laurenza, L. Banchi, "Conditional channel simulation," Ann. Phys. **400**, 289 (2019).
[723] F. Leditzky, D. Leung, and G. Smith, "Dephrasure channel and superadditivity of the coherent information," Phys. Rev. Lett. **121**, 160501 (2018).
[724] R. Laurenza, C. Lupo, G. Spedalieri, S. L. Braunstein, and S. Pirandola, "Channel simulation in quantum metrology," Quantum Meas. Quantum Metrol. **5**, 1-12 (2018).
[725] S. Pirandola, B. R. Bardhan, T. Gehring, C. Weedbrook and S. Lloyd, "Advances in Photonic Quantum Sensing," Nat. Photon. **12**, 724 (2018).
[726] S. Lloyd, "Enhanced sensitivity of photodetection via quantum illumination," Science **321**, 1463 (2008).
[727] S.-H. Tan *et al.*, "Quantum illumination with Gaussian States," Phys. Rev. Lett. **101**, 253601 (2008).
[728] S. Pirandola, "Quantum Reading of a Classical Digital Memory," Phys. Rev. Lett. **106**, 090504 (2011).
[729] M. Tsang, R. Nair, X.-M. Lu, "Quantum theory of su-

perresolution for two incoherent optical point sources," Phys. Rev. X **6**, 031033 (2016).
[730] C. Lupo and S. Pirandola, "Ultimate precision bound of quantum and subwavelength imaging," Phys. Rev. Lett. **117**, 190802 (2016).
[731] R. Nair and M. Tsang, "Far-Field Superresolution of thermal electromagnetic sources at the quantum limit," Phys. Rev. Lett. **117**, 190801 (2016).
[732] P. Liuzzo-Scorpo, A. Mari, V. Giovannetti, and G. Adesso, "Optimal Continuous Variable Quantum Teleportation with Limited Resources," Phys. Rev. Lett. **119**, 120503 (2017).
[733] P. Liuzzo-Scorpo, A. Mari, V. Giovannetti, and G. Adesso, "Erratum: Optimal Continuous Variable Quantum Teleportation with Limited Resources," Phys. Rev. Lett. **120**, 029904 (2018).
[734] E. Kaur and M. M. Wilde, "Upper bounds on secret-key agreement over lossy thermal bosonic channels," Phys. Rev. A **96**, 062318 (2017).
[735] S. Tserkis, J. Dias, and T. C. Ralph, "Simulation of Gaussian channels via teleportation and error correction of Gaussian states," Phys. Rev. A **98**, 052335 (2018).
[736] R. Laurenza, S. Tserkis, L. Banchi, S. L. Braunstein, T. C. Ralph, S. Pirandola, "Tight bounds for private communication over bosonic Gaussian channels based on teleportation simulation with optimal finite resources," Phys. Rev. A **100**, 042301 (2019).
[737] L. Vaidman, "Teleportation of quantum states," Phys. Rev. A **49**, 1473-1476 (1994).
[738] A. S. Holevo, "Single-Mode Quantum Gaussian Channels: Structure and Quantum Capacity," Problems of Information Transmission **43**, 1-11 (2007).
[739] F. Caruso and V. Giovannetti, "Degradability of Bosonic Gaussian channels," Phys. Rev. A **74**, 062307 (2006).
[740] F. Caruso, V. Giovannetti, and A. S. Holevo, "One-mode Bosonic Gaussian channels: a full weak-degradability classification," New J. Phys. **8**, 310 (2006).
[741] M. M. Wilde, M. Tomamichel, and M. Berta, "Converse Bounds for Private Communication Over Quantum Channels," IEEE Trans. Inf. Theory **63**, 1792 (2017).
[742] M. Christandl and A. Müller-Hermes, "Relative Entropy Bounds on Quantum, Private and Repeater Capacities," Commun. Math. Phys. **353**, 821 (2017).
[743] A. S. Holevo and R. F. Werner, "Evaluating capacities of bosonic Gaussian channels," Phys. Rev. A **63**, 032312 (2001).
[744] M. M. Wolf, D. Pérez-García, and G. Giedke, "Quantum Capacities of Bosonic Channels," Phys. Rev. Lett. **98**, 130501 (2007).
[745] I. Devetak, and P. W. Shor, "The Capacity of a Quantum Channel for Simultaneous Transmission of Classical and Quantum Information," Commun. Math. Phys. **256**, 287–303 (2005).
[746] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin, "Capacities of Quantum Erasure Channels," Phys. Rev. Lett. **78**, 3217 (1997).
[747] K. Goodenough, D. Elkouss, and S. Wehner, "Assessing the performance of quantum repeaters for all phase-insensitive Gaussian bosonic channels," New J. Phys. **18**, 063005 (2016). See also arXiv:1511.08710 (2015).
[748] L. Banchi, J. Pereira, S. Lloyd, and S. Pirandola, "Convex optimization of programmable quantum computers," Preprint arXiv:1905.01316 (2019).
[749] L. Banchi, J. Pereira, S. Lloyd, and S. Pirandola, "Optimization and learning of quantum programs," Preprint arXiv:1905.01318 (2019).
[750] K. Noh, S. Pirandola, and L. Jiang, "Enhanced energy-constrained quantum communication over bosonic Gaussian channels," Nat. Commun. **11**, 457 (2020).
[751] K. Noh, S. M. Girvin, and L. Jiang, "Encoding an oscillator into many oscillators," Preprint arXiv:1903.12615 (2019).
[752] K. Noh, V. V. Albert, and L. Jiang, "Improved quantum capacity bounds of Gaussian loss channels and achievable rates with Gottesman-Kitaev-Preskill codes," IEEE Trans. Inf. Theory 65, 2563 (2019).
[753] V. V. Albert, K. Noh, K. Duivenvoorden, D. J. Young, R. T. Brierley, P. Reinhold, C. Vuillot, L. Li, C. Shen, S. M. Girvin, B. M. Terhal, L. Jiang, "Performance and structure of single-mode bosonic codes," Phys. Rev. A **97**, 032346 (2018).
[754] D. Gottesman, A. Yu. Kitaev, and J. Preskill, "Encoding a qubit in an oscillator," Phys. Rev. A **64**, 012310 (2001).
[755] B. C. Travaglione and G. J. Milburn, "Preparing encoded states in an oscillator," Phys. Rev. A **66**, 052322 (2002).
[756] S. Pirandola, S. Mancini, D. Vitali, and P. Tombesi, "Constructing finite-dimensional codes with optical continuous variables," EPL **68**, 323 (2004).
[757] S. Pirandola, S. Mancini, D. Vitali, and P. Tombesi, "Continuous variable encoding by ponderomotive interaction," Eur. Phys. J. D **37**, 283 (2006).
[758] S. Pirandola, S. Mancini, D. Vitali, and P. Tombesi, "Generating continuous variable quantum codewords in the near-field atomic lithography," J. Phys. B At. Mol. Opt. Phys. **39**, 997 (2006).
[759] H. M. Vasconcelos, L. Sanz, and S. Glancy, "All-optical generation of states for Encoding a qubit in an oscillator," Opt. Lett. **35**, 3261 (2010).
[760] M. Pollack, "The maximum capacity through a network," Operations Research **8**, 733–736 (1960).
[761] T. Cormen, C. Leiserson, and R. Rivest, "Introduction to Algorithms," (MIT Press Cambridge, MA, 1990).
[762] A. S. Tanenbaum and D. J. Wetherall, "Computer Networks," (5th Edition, Pearson, 2010).
[763] J. B. Orlin, "Max flows in O(nm) time, or better," STOC'13 Proceedings of the 45th annual ACM symposium on theory of computing, pp. 765–774 (2013).
[764] H. J. Kimble, "The quantum internet," Nature **453**, 1023 (2008).
[765] S. Lloyd, M. S. Shahriar, J. H. Shapiro, and P. R. Hemmer, "Long Distance, Unconditional Teleportation of Atomic States via Complete Bell State Measurements," Phys. Rev. Lett. **87**, 167903 (2001).
[766] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," Rev. Mod. Phys. **83**, 33 (2011).
[767] M. Varnava, D. E. Browne, T. Rudolph, "Loss Tolerance in One-Way Quantum Computation via Counterfactual Error Correction," Phys. Rev. Lett. **97**, 120501 (2006).
[768] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, "Quantum communication without the necessity of quantum memories," Nat. Photon. **6**, 771 (2012).

[769] K. Azuma, K. Tamaki, and H.-K. Lo, "All-photonic quantum repeaters," Nat. Commun. **6**, 6787 (2015).

[770] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, "Ultrafast and Fault-Tolerant Quantum Communication across Long Distances," Phys. Rev. Lett. **112**, 250501 (2014).

[771] R. Namiki, L. Jiang, J. Kim, and N. Lütkenhaus, "Role of syndrome information on a one-way quantum repeater using teleportation-based error correction," Phys. Rev. A **94**, 052304 (2016).

[772] S. Muralidharan, C.-L. Zou, L. Li, J. Wen, and L. Jiang, "Overcoming erasure errors with multilevel systems," New J. Phys **19**, 013026 (2017).

[773] M. Razavi, "An Introduction to Quantum Communications Networks," Morgan & Claypool Publishers (2018).

[774] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, W. K. Wootters, "Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels," Phys. Rev. Lett. **76**, 722 (1996).

[775] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, Mikhail, and L. Jiang, "Optimal architectures for long distance quantum communication," Sci. Rep. **6**, 20463 (2016).

[776] W. J. Munro, K. Azuma , K. Tamaki, K. Nemoto, "Inside Quantum Repeaters," IEEE J. Sel. Top. Quantum Electron. **21**, 78 (2015).

[777] C.-W. Chou, J. Laurat, H. Deng, K. S. Choi, H. de Riedmatten, D. Felinto, and H. J. Kimble,"Functional Quantum Nodes for Entanglement Distribution over Scalable Quantum Networks," Science **316**, 1316 (2007).

[778] B. Zhao, Z.-B. Chen, Y.-A. Chen, J. Schmiedmayer, and J.-W. Pan, "Robust Creation of Entanglement between Remote Memory Qubits," Phys. Rev. Lett. **98**, 240502 (2007).

[779] J. Calsamiglia and N. Lütkenhaus, "Maximum efficiency of a linear-optical Bell-state analyzer," Appl. Phys. B **72**, 67 (2001).

[780] W. P. Grice, "Arbitrarily complete Bell-state measurement using only linear optical elements," Phys. Rev. A **84**, 042331 (2011).

[781] H. A. Zaidi, and P. van Loock, "Beating the One-Half Limit of Ancilla-Free Linear Optics Bell Measurements," Phys. Rev. Lett. **110**, 260501 (2013).

[782] D. E. Bruschi, T. M. Barlow, M. Razavi, and A. Beige, "Repeat-until-success quantum repeaters," Phys. Rev. A **90**, 032306 (2014).

[783] F. Ewert and P. van Loock, "3/4-Efficient Bell Measurement with Passive Linear Optics and Unentangled Ancillae," Phys. Rev. Lett. **113**, 140403 (2014).

[784] M. Razavi, M. Piani and N. Lütkenhaus, "Quantum repeaters with imperfect memories: Cost and scalability," Phys. Rev. A **80**, 032301 (2009).

[785] E. Saglamyurek, N. Sinclair, J. Jin, J. A. Slater, D. Oblak, F. Bussières, M. George, R. Ricken, W. Sohler, and W. Tittel, "Broadband waveguide quantum memory for entangled photons," Nature **469**, 512 (2011).

[786] C. Clausen, I. Usmani, F. Bussières, N. Sangouard, M. Afzelius, H. de Riedmatten, and N. Gisin, "Quantum storage of photonic entanglement in a crystal," Nature **469**, 508 (2011).

[787] N. Sinclair, E. Saglamyurek, H. Mallahzadeh, J. A. Slater, M. George, R. Ricken, M. P. Hedges, D. Oblak, C. Simon, W. Sohler, and W. Tittel," Spectral Multiplexing for Scalable Quantum Photonics using an Atomic Frequency Comb Quantum Memory and Feed-Forward Control," Phys. Rev. Lett. **113**, 053603 (2014).

[788] S. Abruzzo, H. Kampermann, and D. Bruß, "Measurement-device-independent quantum key distribution with quantum memories," Phys. Rev. A **89**, 012301 (2014).

[789] C. Panayi, M. Razavi, X. Ma, and Norbert Lütkenhaus, "Memory-assisted measurement-device-independent quantum key distribution," New J. Phys. **16**, 043005 (2014).

[790] N. Lo Piparo, M. Razavi, and C. Panayi, "Measurement-device-independent quantum key distribution with ensemble-based memories," IEEE J. Sel. Top. Quantum Electron. **21**, 138 (2015).

[791] N. Lo Piparo, M. Razavi, W. J. Munro, "Measurement-device-independent quantum key distribution with nitrogen vacancy centers in diamond," Phys. Rev. A **95**, 022338 (2017).

[792] N. Lo Piparo, N. Sinclair, and M. Razavi, "Memory-assisted quantum key distribution resilient against multiple-excitation effects," Quantum Sci. Technol. **3**, 014009 (2018).

[793] N. Lo Piparo, M. Razavi, and W. J. Munro, "Memory-assisted quantum key distribution with a single nitrogen-vacancy center," Phys. Rev. A **96**, 052313 (2017).

[794] F. Rozpedek, K. Goodenough, J. Ribeiro, N. Kalb, V. Caprara Vivoli, A. Reiserer, R. Hanson, S. Wehner, and D Elkouss, "Parameter regimes for a single sequential quantum repeater," Quantum Sci. Technol. **3**, 034002 (2018).

[795] F. Rozpedek, R. Yehia, K. Goodenough, M. Ruf, P. C. Humphreys, R. Hanson, S. Wehner, and D. Elkouss, "Near-term quantum-repeater experiments with nitrogen-vacancy centers: Overcoming the limitations of direct transmission," Phys. Rev. A **99**, 052330 (2019).

[796] J. Amirloo, M. Razavi, and A. H. Majedi, "Quantum key distribution over probabilistic quantum repeaters," Phys. Rev. A **82**, 032304 (2010).

[797] N. Lo Piparo, and M. Razavi, Mohsen, "Long-distance quantum key distribution with imperfect devices," Phys. Rev. A **88**, 012332 (2013).

[798] N. Lo Piparo and M. Razavi, "Long-distance trust-free quantum key distribution," J. Select. Topics Quantum Electron. **21**, 6600508 (2015).

[799] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, "Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels," Phys. Rev. Lett. **77**, 2818 (1996).

[800] H. Aschauer, "Quantum communication in noisy environments," PhD thesis, Ludwig-Maximilians-Universität München, 2005.

[801] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, "Quantum Repeater with Encoding," Phys. Rev. A **79**, 032325 (2009).

[802] W. J. Munro, K. A. Harrison, A. M. Stephens, S. J. Devitt, and K. Nemoto, "From quantum multiplexing to high-performance quantum networking," Nature Photon. **4**, 792-796 (2010).

[803] F. Ewert, M. Bergmann, and P. van Loock, "Ultrafast Long-Distance Quantum Communication with Static Linear Optics," Phys. Rev. Lett. **117**, 210501 (2016).

[804] F. Ewert and P. van Loock, "Ultrafast fault-tolerant long-distance quantum communication with static lin-

ear optics," Phys. Rev. A **95**, 012327 (2017).
[805] F. Schmidt and P. van Loock, "Efficiencies of logical Bell measurements on Calderbank-Shor-Steane codes with static linear optics," Phys. Rev. A **99**, 062308 (2019).
[806] S. Pirandola and S. L. Braunstein, "Unite to build the quantum internet," Nature **532**, 169 (2016).
[807] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," Science **362**, eaam9288 (2018).
[808] J. Eisert, D.E. Browne, S. Scheel, M. B. Plenio, "Distillation of continuous-variable entanglement with optical means," Ann. Phys. **311**, 431-458 (2004).
[809] A. Datta, L. Zhang, J. Nunn, N. K. Langford, A. Feito, M. B. Plenio, and I. A. Walmsley, "Compact Continuous-Variable Entanglement Distillation," Phys. Rev. Lett. **108**, 060502 (2012).
[810] A. P. Lund and T. C. Ralph, "Continuous-variable entanglement distillation over a general lossy channel," Phys. Rev. A **80**, 032309 (2009).
[811] J. Fiurášek, "Distillation and purification of symmetric entangled Gaussian states," Phys. Rev. A **82**, 042331 (2010).
[812] J. Dias and T. C. Ralph, " Quantum error correction of continuous-variable states with realistic resources," Phys. Rev. A **97**, 032335 (2018).
[813] K. P. Seshadreesan, H. Krovi, and S. Guha, "Continuous-variable entanglement distillation over a pure loss channel with multiple quantum scissors," Phys. Rev. A **100**, 022315 (2019).
[814] T. C. Ralph, "Quantum error correction of continuous-variable states against Gaussian noise," Phys. Rev. A **84**, 022339 (2011).
[815] E. T. Campbell, M. G. Genoni, and J. Eisert, "Continuous-variable entanglement distillation and noncommutative central limit theorems," Phys. Rev. A **87**, 042330 (2013).
[816] F. Furrer and W. J. Munro, "Repeaters for continuous-variable quantum communication," Phys. Rev. A **98**, 032335 (2018).
[817] K. P. Seshadreesan, H. Krovi, and S. Guha, "A continuous-variable quantum repeater with quantum scissors," preprint arXiv:1811.12393 (2018).
[818] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, Kae Nemoto, W. J. Munro, and Y. Yamamoto, "Hybrid quantum repeater using bright coherent light," Phys. Rev. Lett. **96**, 240501 (2006).
[819] T. D. Ladd, P. van Loock, K. Nemoto, W. J. Munro, and Y. Yamamoto, "Hybrid quantum repeater based on dispersive CQED interactions between matter qubits and bright coherent light," New J. Phys. **8**, 164 (2006).
[820] P. van Loock, N. Lütkenhaus, W. J. Munro, and K. Nemoto, "Quantum Repeaters using Coherent-State Communication," Phys. Rev. A **78**, 062319 (2008).
[821] N. K. Bernardes, L. Praxmeyer, and P. van Loock, "Rate analysis for a hybrid quantum repeater," Phys. Rev. A **83**, 012323 (2011).
[822] D. Gonta, P. van Loock, "Quantum repeater based on cavity-QED evolutions and coherent light," Appl. Phys. B **122**, 118 (2016).
[823] D. Gonta and P. van Loock, "Dynamical quantum repeater using cavity QED and optical coherent states," Phys. Rev. A **88**, 052308 (2013).
[824] M. Bergmann, P. van Loock. "A hybrid quantum repeater for qudits," Phys. Rev. A **99**, 032349 (2019).
[825] I. B. Damgaard, S. Fehr, R. Renner, L. Salvail, and C. Schaffner, "A Tight High-Order Entropic Quantum Uncertainty Relation With Applications," *In Advances in Cryptology, CRYPTO 2007; Lecture Notes in Computer Science*, (Springer, Berlin/Heidelberg, Germany, 2007)
[826] C. Schaffner, "Cryptography in the Bounded-Quantum-Storage Model," PhD Thesis, University of Aarhus, (2007).
[827] S. Wehner, C. Schaffner, and B. M. Terhal, "Cryptography from Noisy Storage," Phys. Rev. Lett. **100**, 220502 (2008).
[828] S. Wehner and A. Winter, "Entropic uncertainty relations - A survey," New J. Phys. **12**, 025009 (2010).
[829] H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner, "Possibility, Impossibility and Cheat-Sensitivity of Quantum Bit String Commitment," Phys. Rev. A **78**, 022316 (2008).
[830] S. Wehner, M. Curty, C. Schaffner, and H.-K. Lo, "Implementation of two-party protocols in the noisy-storage model," Phys. Rev. A **81**, 052336 (2010).
[831] R. König, S. Wehner, and J. Wullschleger, "Unconditional Security From Noisy Quantum Storage," IEEE Trans. Info. Theory **58**, 1962 (2012).
[832] C. Lupo, "Quantum Data Locking for Secure Communication against an Eavesdropper with Time-Limited Storage," Entropy **17**, 3194 (2015).
[833] J. Sanchez, "Entropic uncertainty and certainty relations for complementary observables," Phys. Lett. A **173**, 233 (1993).
[834] P. Hayden, D. Leung, P. W. Shor, and A. Winter, "Randomizing quantum states: Constructions and applications," Commun. Math. Phys. **250**, 371 (2004).
[835] O. Fawzi, P. Hayden, and P. Sen, "From Low-Distortion Norm Embeddings to Explicit Uncertainty Relations and Efficient Information Locking," J. ACM **60**, 44 (2013).
[836] R. Adamczak, R. Latala, Z. Puchala, and K. Zyczkowski, "Asymptotic entropic uncertainty relations," J. Math. Phys. **57**, 032204 (2016).
[837] R. Adamczak, "Metric and classical fidelity uncertainty relations for random unitary matrices," J. Phys. A: Math. Theor. **50**, 105302 (2017).
[838] N. H. Y. Ng, M. Berta, S. Wehner, "Min-entropy uncertainty relation for finite-size cryptography," Phys. Rev. A **86**, 042315 (2012).
[839] F. Dupuis, O. Fawzi, and S. Wehner, "Entanglement Sampling and Applications," IEEE Trans. Info. Theory **61**, 1093 (2015)
[840] C. Erven, N. Ng, N. Gigov, R. Laflamme, S. Wehner, and G. Weihs, "An experimental implementation of oblivious transfer in the noisy storage model," Nat. Commun. **5**, 3418 (2014).
[841] F. Furrer, T. Gehring, C. Schaffner, C. Pacher, R. Schnabel, S. Wehner, "Continuous-variable protocol for oblivious transfer in the noisy-storage model," Nat. Commun. **9**, 1450 (2018).
[842] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, "Locking Classical Correlations in Quantum States," Phys. Rev. Lett. **92**, 067902 (2004).
[843] C. Shannon, "Communication Theory of Secrecy Systems," Bell Syst. Tech. J. **28**, 656 (1949).
[844] M. S. Pinsker, "Information and Information Stability of Random Variables and Processes," (San Francisco,

Holden Day, 1964).
[845] S. Lloyd, "Quantum enigma machines," arXiv:1307.0380 (2013).
[846] S. Guha, P. Hayden, H. Krovi, S. Lloyd, C. Lupo, J. H. Shapiro, M. Takeoka, and M. M. Wilde, "Quantum enigma machines and the locking capacity of a quantum channel," Phys. Rev. X **4**, 011016 (2014).
[847] A. Winter, "Weak locking capacity of quantum channels can be much larger than private capacity," J. Cryptology **30**, 1-21 (2017).
[848] C. Lupo and S. Lloyd, "Continuous-variable quantum enigma machines for long-distance key distribution," Phys. Rev. A **92**, 062312 (2015).
[849] C. Lupo and S. Lloyd, "Quantum-locked key distribution at nearly the classical capacity rate," Phys. Rev. Lett. **113**, 160502 (2014).
[850] C. Lupo, M. M. Wilde and S. Lloyd, "Robust quantum data locking from phase modulation," Phys. Rev. A **90**, 022326 (2014).
[851] C. Lupo and S. Lloyd, "Quantum data locking for high-rate private communication," New J. Phys. **17**, 033022 (2015).
[852] Z. Huang, P. P. Rohde, D. W. Berry, P. Kok, J. P. Dowling, and C. Lupo, "Boson Sampling Private-Key Quantum Cryptography," preprint arXiv:1905.03013 (2019).
[853] S. Aaronson and A. Arkhipov, "The computational complexity of linear optics," in Proceedings of the forty-third annual ACM symposium on Theory of computing (ACM, 2011) pp. 333-342
[854] Y. Liu, Z. Cao, C. Wu, D. Fukuda, L. You, J. Zhong, T. Numata, S. Chen, W. Zhang, S.-C. Shi, C.-Y. Lu, Z. Wang, X. Ma, J. Fan, Q. Zhang and J.-W. Pan, "Experimental quantum data locking," Phys. Rev. A **94**, 020301 (2016).
[855] D. J. Lum, J. C. Howell, M. S. Allman, T. Gerrits, V. B. Verma, S. Woo Nam, C. Lupo, and S. Lloyd, "Quantum enigma machine: Experimentally demonstrating quantum data locking," Phys. Rev. A **94**, 022315 (2016).
[856] J. Notaros, J. Mower, M. Heuck, C. Lupo, N. C. Harris, G. R. Steinbrecher, D. Bunandar, T. Baehr-Jones, M. Hochberg, and S. Lloyd, et al., "Programmable dispersion on a photonic integrated circuit for classical and quantum applications," Opt. Express **25**, 21275 (2017).
[857] A. K. Lenstra, et al."Ron was wrong, Whit is right," IACR Cryptology Report 2012/064 (2012).
[858] N. Heninger, Z. Durumeric, E. Wustrow, and J. A. Halderman, "Mining your Ps and Qs: Detection of widespread weak keys in network devices," In *Proceedings of the 21st USENIX Conference on Security Symposium*, Security'12, 35, (2012).
[859] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden and N. Brunner, "Self-Testing Quantum Random Number Generator," Phys. Rev. Lett. **114**, 150501 (2015).
[860] R. Colbeck, and R. Renner, "No extension of quantum theory can have improved predictive power," Nat. Commun. **2**, 411 (2011).
[861] R. Colbeck, and R. Renner, "The completeness of quantum theory for predicting measurement outcomes," In *Quantum Theory: Informational Foundations and Foils*, G. Chiribella, and R. W. Spekkens, eds., (Springer, 2016).
[862] R. Colbeck, "Quantum and Relativistic Protocols For Secure Multi-Party Computation," Ph.D. thesis, University of Cambridge (2007). See also arXiv:0911.3814 (2009).
[863] R. Colbeck, and A. Kent, "Private randomness expansion with untrusted devices," J. of Phys. A **44**, 095305 (2011).
[864] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, C. Monroe, "Random numbers certified by Bell's theorem," Nature **464**, 1021 (2010).
[865] S. Fehr, R. Gelles, and C. Schaffner, "Security and composability of randomness expansion from Bell inequalities," Phys. Rev. A **87**, 012335 (2013).
[866] S. Pironio and S. Massar, "Security of practical private randomness generation," Phys. Rev. A **87**, 012336 (2013).
[867] U. Vazirani, T. Vidick, "Certifiable quantum dice or, testable exponential randomness expansion," In *Proceedings of the 44th Annual ACM Symposium on Theory of Computing (STOC-12)*, 61 (2012).
[868] C. A. Miller and Y. Shi, "Universal security for randomness expansion from the spot-checking protocol," Siam Journal of Computing **46**, 1304 (2017).
[869] Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, and X. Yuan et al., "Device independent quantum random number generation," Nature **562**, 548 (2018).
[870] M. Herrero-Collantes, and J. C Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys. **89**, 015004 (2017).
[871] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," npj Quantum Information **2**, 16021 (2016).
[872] A. Acín, and L. Masanes "Certified randomness in quantum physics," Nature **540**, 213 (2016).
[873] M. W. Mitchell, C. Abellan and W. Amaya, "Strong experimental guarantees in ultrafast quantum random number generation," Phys. Rev. A **91**, 012314 (2015).
[874] M. Santha, and U. V. Vazirani, "Generating quasi-random sequences from slightly-random sources," In *Proceedings of the 25th IEEE Symposium on Foundations of Computer Science (FOCS-84)*, 434 (1984).
[875] R. Colbeck, and R. Renner, "Free randomness can be amplified," Nat. Phys. **8**, 450 (2012).
[876] R. Gallego et al. "Full randomness from arbitrarily deterministic events," Nat. Commun. **4**, 3654 (2013).
[877] F. G. S. Brandão, et al. "Realistic noise-tolerant randomness amplification using finite number of devices," Nat. Commun. **7**, 11345 (2016).
[878] M. Kessler, and R. Arnon-Friedman, "Device-independent randomness amplification and privatization," preprint arXiv:1705.04148 (2017).
[879] K.-M. Chung, Y. Shi, and X. Wu, "Physical randomness extractors: Generating random numbers with minimal assumptions," preprint arXiv:1402.4797 (2014).
[880] E. Hänggi, R. Renner, and S. Wolf, "The impossibility of non-signalling privacy amplification," preprint arXiv:0906.4760 (2009).
[881] R. Arnon Friedman, E. Hänggi, and A. Ta-Shma, "Towards the impossibility of non-signalling privacy amplification from time-like ordering constraints," preprint arXiv:1205.3736 (2012).
[882] D. Gottesman, and I. Chuang, "Quantum Digital Signatures," preprint arXiv:0105032 (2001).
[883] D. Boneh, and M. Zhandry, "Secure Signatures and

Chosen Ciphertext Security in a Quantum Computing World," in *Advances in Cryptology - CRYPTO 2013. CRYPTO 2013. Lecture Notes in Computer Science* **8043**, R. Canetti, J. A. Garay, eds. (Springer, Berlin, Heidelberg, 361 2013).

[884] S. B. David and O. Sattath, "Quantum Tokens for Digital Signatures," preprint arXiv:1609.09047 (2016).

[885] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM review **41**, 303 (1999).

[886] L. Lamport, "Constructing digital signatures from a one-way function," Technical Report CSL-98, SRI International Palo Alto, 1979.

[887] R. C. Merkle, "A Certified Digital Signature," in *Advances in Cryptology - CRYPTO' 89 Proceedings*, pp. 218-238, New York, NY, 1990. Springer New York.

[888] V. Lyubashevsky, "Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures," in *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security*, 598 (Tokyo, Japan, 2009).

[889] N. T. Courtois, M. Finiasz, and N. Sendrier, "How to achieve a McEliece-based Digital Signature Scheme," in *ASIACRYPT '01 Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology* (Springer-Verlag Berlin, Heidelberg 2001).

[890] Z. Brakerski, E. Kirshanova, D. Stehlé, and W. Wen, "Learning With Errors and Extrapolated Dihedral Cosets," preprint arXiv:1710.08223 (2017).

[891] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp, "Authentication of quantum messages," in Foundations of Computer Science, 2002. Proceedings of the 43rd Annual IEEE Symposium on, pp. 449–458. IEEE, 2002.

[892] E. Andersson, M. Curty, and I. Jex, "Experimentally realizable quantum comparison of coherent states and its applications," Phys. Rev. A **74**, 022304 (2006).

[893] V. Dunjko, P. Wallden, and E. Andersson, "Quantum Digital Signatures without Quantum Memory," Phys. Rev. Lett. **112**, 040502 (2014).

[894] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, "Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light," Nat. Commun. **3**, 1174 (2012).

[895] A. Peres, "How to differentiate between non-orthogonal states," Phys. Lett. A **128**, 19 (1988).

[896] D. Dieks, "Overlap and distinguishability of quantum states," Phys. Lett. A **126**, 303 (1988).

[897] I. D. Ivanovic, "How to differentiate between non-orthogonal states," Phys. Lett. A **123**, 257 (1987).

[898] P. Wallden, V. Dunjko, A. Kent, and E. Andersson, "Quantum digital signatures with quantum key distribution components," Phys. Rev. A **91**, 042304 (2015).

[899] R. Amiri, P. Wallden, A. Kent, and E. Andersson, "Secure quantum signatures using insecure quantum channels," Phys. Rev. A **93**, 032325 (2016).

[900] H.-L. Yin, Y. Fu, and Z.-B. Chen, "Practical quantum digital signature," Phys. Rev. A **93**, 032316 (2016).

[901] R. Amiri, A. Abidin, P. Wallden, and E. Andersson, "Efficient unconditionally secure signatures using universal hashing," in *International Conference on Applied Cryptography and Network Security*, pp. 143–162. Springer, 2018.

[902] J. M. Arrazola, P. Wallden, E. Andersson, "Multiparty quantum signature schemes," Quantum Info. Comput. **16**, 435 (2016).

[903] M. şahin and İhsan Yilmaz, "Multi-Partied Quantum Digital Signature Scheme Without Assumptions On Quantum Channel Security," J. of Phys.: Conference Series **766**, 012021 (2016).

[904] T.-Y. Wang, Z.-Q Cai, Y.-L. Ren, and R.-L. Zhang, "Security of quantum digital signatures for classical messages," Sci. Rep. **5**, 9231 (2015).

[905] A. Huang, S. Barz, E. Andersson, and V. Makarov, "Implementation vulnerabilities in general quantum cryptography," New J. Phys. **20**, 103016 (2018).

[906] I. V. Puthoor, R. Amiri, P. Wallden, M. Curty, and E. Andersson, "Measurement-device-independent quantum digital signatures," Phys. Rev. A **94**, 022328 (2016).

[907] R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, "Realization of Quantum Digital Signatures without the Requirement of Quantum Memory," Phys. Rev. Lett. **113**, 040502 (2014).

[908] R. J. Donaldson, R. J. Collins, K. Kleczkowska, R. Amiri, P. Wallden, V. Dunjko, J. Jeffers, E. Andersson, and G. S. Buller, "Experimental demonstration of kilometer-range quantum digital signatures," Phys. Rev. A **93**, 012329 (2016).

[909] C. Croal, C. Peuntinger, B. Heim, I. Khan, C. Marquardt, G. Leuchs, P. Wallden, E. Andersson, and N. Korolkova, "Free-Space Quantum Signatures Using Heterodyne Measurements," Phys. Rev. Lett. **117**, 100503 (2016).

[910] R. J. Collins, R. Amiri, M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, M. Takeoka, E. Andersson, G. S. Buller, and M. Sasaki, "Experimental transmission of quantum digital signatures over 90 km of installed optical fiber using a differential phase shift quantum key distribution system," Opt. Lett. **41**, 4883 (2016).

[911] R. J. Collins, R. Amiri, M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, M. Takeoka, M. Sasaki, E. Andersson, and G. S. Buller, "Experimental demonstration of quantum digital signatures over 43 dB channel loss using differential phase shift quantum key distribution," Sci. Rep. **7**, 3235 (2017).

[912] H.-L.Yin, W.-L. Wang, Y.-L. Tang, Q. Zhao, H. Liu, X.-X. Sun, W.-J. Zhang, H. Li, I. Vergheese Puthoor, and L.-X. You et al., "Experimental measurement-device-independent quantum digital signatures over a metropolitan network," Phys. Rev. A **95**, 042338 (2017).

[913] G. L. Roberts, M. Lucamarini, Z. L. Yuan, J. F. Dynes, L. C. Comandar, A. W. Sharpe, A. J. Shields, M. Curty, I. V. Puthoor, and E. Andersson, "Experimental measurement-device-independent quantum digital signatures," Nat. Commun. **8**, 1098 (2017).

[914] D. Chaum and S. Roijakkers, "Unconditionally Secure Digital Signatures," In *Proceeding CRYPTO '90 Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology*, Lecture Notes in Computer Science, pp. 206–214 (Springer-Verlag Berlin, Heidelberg 1991).

[915] C. M. Swanson and D. R. Stinson, "Unconditionally Se-

cure Signature Schemes Revisited," in *Information theoretic security. 5th international conference, ICITS 2011*, (Amsterdam, The Netherlands, 2011).

[916] J. Shikata, G. Hanaoka, Y. Zheng, and H. Imai, "Security notions for unconditionally secure signature schemes," in EUROCRYPT 2002, pp. 434-449, Springer (2002).

[917] G. Hanaoka, J. Shikata, and Y. Zheng, "Efficient Unconditionally Secure Digital Signatures," IEICE transactions on fundamentals of electronics, communications and computer sciences **87**, 120 (2004).

[918] G. Hanaoka, J. Shikata, Y. Zheng, and H. Imai, "Unconditionally Secure Digital Signature Schemes Admitting Transferability," in *Proceeding ASIACRYPT '00 Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*, (Springer-Verlag Berlin, Heidelberg 2000).

[919] D. J. Bernstein, J. Buchmann, and E. Dahmen, "Post Quantum Cryptography," (Springer Publishing Company, Incorporated, 1st edition, 2008).

[920] V. Rijmen, and J. Daemen, "Advanced encryption standard," Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology (2001), pp. 19-22.

[921] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia, "Breaking Symmetric Cryptosystems Using Quantum Period Finding," In: Robshaw M., Katz J. (eds) Advances in Cryptology - CRYPTO 2016. CRYPTO 2016. Lecture Notes in Computer Science, vol 9815. Springer, Berlin, Heidelberg.

[922] M. Ajtai, "Generating hard instances of lattice problems," Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. ACM, 1996.

[923] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," Journal of the ACM **56**, 34 (2009).

[924] R. J. McEliece, "A public-key cryptosystem based on algebraic," Coding Thv **4244**, 114-116 (1978).

[925] E. Berlekamp, "Goppa codes," IEEE Trans. Inf. Theory, **19**, 590-592 (1973).

[926] M. J. Dworkin, "SHA-3 standard: Permutation-based hash and extendable-output functions," No. Federal Inf. Process. Stds.(NIST FIPS)-202. 2015.

[927] D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry, "Random oracles in a quantum world," In D. Hoon Lee and X. Wang, editors, Advances in Cryptology ASI-ACRYPT 2011, pages 41-69, Berlin, Heidelberg, 2011, Springer Berlin Heidelberg.

[928] J. Patarin, "Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms," In: Maurer U. (eds) Advances in Cryptology - EUROCRYPT 1996. EUROCRYPT 1996. Lecture Notes in Computer Science, vol 1070. Springer, Berlin, Heidelberg.

[929] D. Jao, and L. De Feo, "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies," In: Yang BY. (eds) Post-Quantum Cryptography. PQCrypto 2011. Lecture Notes in Computer Science, vol 7071. Springer, Berlin, Heidelberg.

[930] I. Damgård, J. Funder, J. B. Nielsen, and L. Salvail, "Superposition attacks on cryptographic protocols," In C. Padró, editor, Information Theoretic Security, pp. 142-161, Cham, 2014. Springer International Publishing.

[931] A. Ambainis, A. Rosmanis, and D. Unruh, "Quantum attacks on classical proof systems: The hardness of quantum rewinding," In Proceedings of the 2014 IEEE 55th Annual Symposium on Foundations of Computer Science, FOCS '14, pp. 474-483, Washington, DC, USA, 2014. IEEE Computer Society.

[932] P. Wallden and E. Kashefi, "Cyber security in the quantum era," Commun. ACM **62**, 120 (2019).

[933] A. Broadbent and C. Schaffner, "Quantum cryptography beyond quantum key distribution," Designs, Codes and Cryptography **78**, 351-382 (2016).

[934] D. Mayers, "Unconditionally secure quantum bit commitment is impossible," Phys. Rev. Lett. **78**, 3414 (1997).

[935] H.-K. Lo, and H. F. Chau, "Why quantum bit commitment and ideal quantum coin tossing are impossible," Physica D: Nonlinear Phenomena **120**, 177-187 (1998).

[936] A. Chailloux, and I. Kerenidis, "Optimal bounds for quantum bit commitment," 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science. IEEE, 2011.

[937] A. Kent, "Unconditionally secure bit commitment by transmitting measurement outcomes," Phys. Rev. Lett. **109**, 130501 (2012).

[938] I. B. Damgard, S. Fehr, L. Salvail, and C. Schaffner, "Cryptography In the Bounded Quantum-Storage Model," In Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS '05). IEEE Computer Society, Washington, DC, USA, 449-458.

[939] A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis, and E. Diamanti, "Experimental plug and play quantum coin flipping," Nat. Commun. **5**, 3717 (2014).

[940] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, "Quantum fingerprinting," Phys. Rev. Lett. **87**, 167902 (2201).

[941] H. Kobayashi, "General properties of quantum zero-knowledge proofs," Theory of Cryptography Conference. Springer, Berlin, Heidelberg, 2008.

[942] D. Unruh, "Quantum proofs of knowledge," Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2012.

[943] S. Wiesner. "Conjugate coding," SIGACT News **15**, 78-88 (1983).

[944] S. Aaronson, and P. Christiano, "Quantum money from hidden subspaces," Proceedings of the forty-fourth annual ACM symposium on Theory of computing. ACM, 2012.

[945] M. Bozzio, A. Orieux, L. T. Vidarte, I. Zaquine, I. Kerenidis, and E. Diamanti, "Experimental investigation of practical unforgeable quantum money," npj Quantum Information **4**, 5 (2018).

[946] M. Ben-Or, and A. Hassidim, "Fast quantum Byzantine agreement," Proceedings of the thirty-seventh annual ACM symposium on Theory of computing. ACM, 2005.

[947] D. Aggarwal, G. K. Brennen, T. Lee, M. Santha, and M. Tomamichel "Quantum attacks on Bitcoin, and how to protect against them," Ledger **3** (2018).

[948] M. Hillery, M. Ziman, V. Bužek, M. Bieliková, "Towards quantum-based privacy and voting," Phys. Lett. A. **349**,

75-81 (2006).
[949] M. Arapinis, E. Kashefi, N. Lamprou, and A. Pappa, "A Comprehensive Analysis of Quantum E-voting Protocols," preprint arXiv:1810.05083 (2018).
[950] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, "Position-based quantum cryptography: Impossibility and constructions," SIAM Journal on Computing **43**, 150-178 (2014).
[951] I. Kerenidis, and R. De Wolf "Quantum symmetrically-private information retrieval," Information Processing Letters **90**, 109-114 (2004).
[952] G. M. Nikolopoulos, "Applications of single-qubit rotations in quantum public-key cryptography," Phys. Rev. A **77**, 032348 (2008).
[953] A. Broadbent, G. Gutoski, and D. Stebila, "Quantum One-Time Programs," In: Canetti R., Garay J.A. (eds) Advances in Cryptology - CRYPTO 2013. CRYPTO 2013. Lecture Notes in Computer Science, vol 8043. Springer, Berlin, Heidelberg.
[954] C. Portmann, "Quantum Authentication with Key Recycling,". In: Coron JS., Nielsen J. (eds) Advances in Cryptology - EUROCRYPT 2017. EUROCRYPT 2017. Lecture Notes in Computer Science, vol 10212. Springer, Cham.
[955] G. M. Nikolopoulos and E. Diamanti, "Continuous-variable quantum authentication of physical unclonable keys," Sci. Rep. **7**, 46047 (2017).
[956] A. Broadbent, J. Fitzsimons, and E. Kashefi, "Universal blind quantum computation," 2009 50th Annual IEEE Symposium on Foundations of Computer Science. IEEE, 2009.
[957] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, "Demonstration of blind quantum computing," Science **335**, 303-308 (2012).
[958] J. F. Fitzsimons, and E. Kashefi, "Unconditionally verifiable blind quantum computation," Phys. Rev. A **96**, 012303 (2017).
[959] A. Broadbent, "How to Verify a Quantum Computation," Theory oF Computing **14**, 1-37 (2018).
[960] S. Barz, J. F. Fitzsimons, E. Kashefi, and P. Walther, "Experimental verification of quantum computation," Nat. Phys. **9**, 727 (2013).
[961] Y. Dulek, C. Schaffner, and F. Speelman, "Quantum Homomorphic Encryption for Polynomial-Sized Circuits," In: Robshaw M., Katz J. (eds) Advances in Cryptology - CRYPTO 2016. CRYPTO 2016. Lecture Notes in Computer Science, vol 9816. Springer, Berlin, Heidelberg.
[962] F. Dupuis, J. B. Nielsen, and L. Salvail, "Actively Secure Two-Party Evaluation of Any Quantum Operation," In: Safavi-Naini R., Canetti R. (eds) Advances in Cryptology - CRYPTO 2012. CRYPTO 2012. Lecture Notes in Computer Science, vol 7417. Springer, Berlin, Heidelberg.
[963] E. Kashefi, and A. Pappa, "Multiparty delegated quantum computing," Cryptography **1**, 12 (2017).
[964] U. Mahadev, "Classical homomorphic encryption for quantum circuits," 2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS). IEEE, 2018.
[965] U. Mahadev, "Classical verification of quantum computations," 2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS). IEEE, 2018.
[966] A. Cojocaru, L. Colisson, E. Kashefi, and P. Wallden, "QFactory: classically-instructed remote secret qubits preparation," preprint arXiv:1904.06303 (2019).
[967] A. Gheorghiu, and T. Vidick, "Computationally-secure and composable remote state preparation," preprint arXiv:1904.06320 (2019).
[968] A. Ferraro, S. Olivares, M.G.A. Paris, *Gaussian States in Quantum Information*. Napoli Series on physics and Astrophysics, Bibliopolis (2005).
[969] L. Banchi, S. L. Braunstein, and S. Pirandola, "Quantum fidelity for arbitrary Gaussian states," Phys. Rev. Lett. **115**, 260501 (2015).
[970] L. Bombelli, R. K. Koul, J. Lee, and R. D. Sorkin, "Quantum source of entropy for black holes," Phys. Rev. D **34**, 373 (1986).
[971] A. S. Holevo, "The entropy gain of infinite-dimensional quantum channels," Doklady Mathematics **82**, 730-731 (2010).
[972] G. Spedalieri, C. Weedbrook, and S. Pirandola, "A limit formula for the quantum fidelity," J. Phys. A: Math. Theor. **46**, 025304 (2013).
[973] R. Simon, S. Chaturvedi, and V. Srinivasan, "Congruences and canonical forms for a positive matrix: Application to the Schweinler-Wigner extremum principle," J. Math. Phys. **40**, 3632 (1999).
[974] S. Pirandola and S. Lloyd, "Computable bounds for the discrimination of Gaussian states," Phys. Rev. A **78**, 012331 (2008).
[975] A. Uhlmann, " The 'transition probability' in the state space of *-algebra," Rep. Math. Phys. **9**, 273 (1976).
[976] H. Nha, and H. J. Carmichael, "Distinguishing two single-mode Gaussian states by homodyne detection: An information-theoretic approach," Phys. Rev. A **71**, 032336 (2005).
[977] S. Olivares, M. G. A. Paris, and U. L. Andersen, "Cloning of Gaussian states by linear optics," Phys. Rev. A **73**, 062330 (2006).
[978] H. Scutaru, "Fidelity for displaced squeezed thermal states and the oscillator semigroup," J. Phys. A **31**, 3659 (1998).
[979] P. Marian and T. A. Marian, "Uhlmann fidelity between two-mode Gaussian states," Phys. Rev. A **86**, 022340 (2012).
[980] Gh.-S. Părăoanu, H. Scutaru, "Fidelity for multimode thermal squeezed states," Phys. Rev. A **61**, 022306 (2000).
[981] C. W. Helstrom, *Quantum Detection and Estimation Theory*, *Mathematics in Science and Engineering*, Vol. 123 (Academic Press, New York, 1976).
[982] C. A. Fuchs and J. van de Graaf, "Cryptographic Distinguishability Measures for Quantum Mechanical States," IEEE Trans. Inf. Theory **45**, 1216 (1999).
[983] C. A. Fuchs and C. M. Caves, "Mathematical techniques for quantum communication," Open Syst. Inf. Dyn. **3**, 345 (1995).
[984] C. Oh, C. Lee, L. Banchi, S. Lee, C. Rockstuhl, and H. Jeong, " Optimal Measurements for Quantum Fidelity between Gaussian States," preprint arXiv:1901.02994 (2019).
[985] S. Scheel and D.-G. Welsch, "Entanglement generation and degradation by passive optical devices," Phys. Rev. A **64**, 063811 (2001).
[986] X.-y. Chen, "Gaussian relative entropy of entanglement," Phys. Rev. A **71**, 062320 (2005).
[987] M. Tomamichel and M. Hayashi, "A Hierarchy of Infor-

mation Quantities for Finite Block Length Analysis of Quantum Tasks," IEEE Trans. Inf. Theory **59**, 7693–7710 (2013).

[988] K. Li, "Second-order asymptotics for quantum hypothesis testing," Ann. Statist. **42**, 171–189, (2014).

[989] M. M. Wilde, M. Tomamichel, S. Lloyd, and M. Berta, "Gaussian Hypothesis Testing and Quantum Illumination," Phys. Rev. Lett. **119**, 120501 (2017).

[990] A. Monras and F. Illuminati, "Information geometry of Gaussian channels," Phys. Rev. A **81**, 062326 (2010).

[991] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, Leftover Hashing Against Quantum Side Information, IEEE Trans. Inf. Theory **57**, 5524-5535 (2011).