Secure quantum signatures using insecure quantum channels

Secure Quantum Signatures Using Insecure Quantum Channels

Ryan Amiri[1],* Petros Wallden[2], Adrian Kent[3,4], and Erika Andersson[1]
[1] *SUPA, Institute of Photonics and Quantum Sciences,*
Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom
[2] *LFCS, School of Informatics, University of Edinburgh,*
10 Crichton Street, Edinburgh EH8 9AB, United Kingdom
[3] *Centre for Quantum Information and Foundations, DAMTP,*
Centre for Mathematical Sciences, University of Cambridge,
Wilberforce Road, Cambridge, CB3 0WA, United Kingdom
[4] *Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, ON N2L 2Y5, Canada*

Digital signatures are widely used for authenticity and transferability of messages. Currently used classical schemes have only computational security. We present an unconditionally secure quantum signature scheme where all trust assumptions on the quantum channels are removed, which also has reduced signature size compared to previous quantum schemes. We show that in practice, the noise threshold for out scheme is less strict than for distilling a highly secure key using quantum key distribution. This shows that "direct" quantum signature schemes can be preferable to signature schemes relying on quantum key distribution.

INTRODUCTION

Signature schemes allow for the exchange of messages from one sender to multiple recipients, with the guarantee that messages cannot be forged or tampered with. Additionally, messages can be transferred (it is highly unlikely that a message is accepted by one recipient and then, if forwarded, rejected by another recipient) and cannot be repudiated (if a recipient accepts a message, the sender cannot later successfully deny that she sent it). Digital signatures are widely used and may be considered to be one of the most important inventions of modern cryptography. Unfortunately, the security of commonly used signature protocols relies on the assumed computational difficulty of certain problems. In the United States, for example, there are currently three approved algorithms for generating digital signatures – RSA, DSA and ECDSA – all of which rely on the difficulty of finding discrete logarithms or factoring large primes. With the advent of quantum computers, such assumptions would no longer be valid. Due to their importance, it would be desirable to develop signature schemes with unconditional or information-theoretic security.

Unconditionally secure "classical" signature schemes are possible, but need, at the very least, shared secret keys, unless there is a third party trusted by everybody (who effectively provides each participant with secret information) [1–4]. Shared secret keys can of course be generated by quantum key distribution (QKD), so that an unconditionally secure signature scheme can proceed by first generating secret keys via QKD, and then running e.g. the protocol P2 in [4]. Unconditionally secure "direct" quantum signature schemes proceed without first distilling highly secure shared secret keys [4–7]. It is an open question what the best unconditionally secure signature schemes are, with respect to signature length, trust assumptions, requirements on communication channels, etc..

Previous quantum signature schemes [4, 6, 7] improved on the original Gottesman-Chuang scheme [5] by removing the need for quantum memory. Alice encoded her signature into quantum states and sent a copy to both Bob and Charlie, who were only able to gain partial information on the overall signature due to the quantum nature of the states. However, the security analysis assumed authenticated quantum channels that did not allow eavesdropping. This strong and unrealistic assumption meant that a potential forger (Bob) only had access to his own copy of the signature states sent from Alice. In reality an adversarial Bob would be able to gain extra information on Alice's signature through eavesdropping on the signature states sent from Alice to Charlie.

Here we present a new quantum signature protocol, with three improvements over previous protocols. First, we remove all trust assumptions on the quantum channels. This is crucial for actual practical use of quantum signature schemes. Second, Alice sends different signatures to Bob and Charlie, instead of the same signature states, which leads to increased efficiency. Third, we show that in this direct quantum signature protocol, the noise threshold for the Alice-Bob and Alice-Charlie quantum channels is in practice less strict than for distilling a secret key using quantum key distribution (QKD).

THE PROTOCOL

We outline our protocol for three parties, with a sender, Alice, and two receivers Bob and Charlie. Generalisation to more parties is possible, but special care should be taken to address colluding adversaries (see e.g. [8]). We assume that between Alice and Bob and between Alice and Charlie there exists authenticated classical channels as well as untrusted, imperfect quantum channels. In addition, Bob and Charlie share a QKD link which can be used to transmit classical messages in full secrecy. The protocol makes use of a key-generating protocol (KGP) performed in pairs separately by Alice-Bob and Alice-Charlie. The KGP uses the noisy untrusted quantum channels, and generates two correlated bit strings, one for the sender and one for the receiver. The Hamming distance between the receiver's string and the sender's string is smaller than the Hamming distance between any string an eavesdropper could produce and the sender's string. The KGP is further discussed below, after presenting the signature protocol itself.

The quantum signature protocol has two parts, a distribution stage and a messaging stage. We show how to sign a one-bit message. Longer messages can be signed for example by suitably iterating the one-bit protocol, as in [9].

Distribution Stage

(1) For each possible future message m=0 or 1, Alice uses the KGP to generate four different length L keys, $A_0^B, A_1^B, A_0^C, A_1^C$, where the superscript denotes the participant with whom she performed the KGP and the subscript denotes the future message, to be decided later by Alice. Bob holds the length L strings K_0^B, K_1^B and Charlie holds the length L strings K_0^C, K_1^C. Due to the KGP, we know that A_0^B is contains fewer mismatches with K_0^B than with any string produced by an eavesdropper, and the same applies to the other pairs of strings. Alice's signature for the future message m will be $Sig_m = (A_m^B, A_m^C)$.

(2) For each future message, Bob and Charlie symmetrise their keys by choosing half of the bit values in their K_m^B, K_m^C and sending them (as well as the corresponding positions) to the other participant using the Bob-Charlie secret classical channel. As will be explained below, this ensures that Alice cannot make Bob and Charlie disagree on the validity of a signature. If they chose to forward a bit value, they will not further use it to check the validity of a signature. They will only use the bits they kept and those received from the other participant [10]. We denote their symmetrised keys by S_m^B and S_m^C, with the superscript indicating whether the key is held by Bob or Charlie. Bob (and Charlie) will keep a record of whether an element in S_m^B came directly from Alice or whether it was forwarded to him by Charlie (or Bob).

At this point in the protocol, Bob's and Charlie's strings each contain half of K_m^B and half of K_m^C (in the honest case). For each future possible message m, Bob and Charlie each have a bit string of length L, and Alice has no information on whether it is Bob's S_m^B or Charlie's S_m^C which contains a particular element of the $2L$ length string (K_m^B, K_m^C). If Bob is dishonest, he knows all of K_m^B and half of K_m^C, but will not know the half of K_m^C that Charlie chose to keep. This will protect against forging by Bob, and vice versa for Charlie.

Messaging Stage

(1) To send a signed one-bit message m, Alice sends (m, Sig_m) to the desired recipient (say Bob).

(2) Bob checks whether (m, Sig_m) matches his S_m^B and records the number of mismatches he finds. He separately checks the part of his key received directly from Alice and the part of the key received from Charlie. If there are fewer than $s_a(L/2)$ mismatches in both halves of the key, where $s_a < 1/2$ is a small threshold determined by the parameters and the desired security level of the protocol, then Bob accepts the message.

(3) To forward the message to Charlie, Bob forwards the pair (m, Sig_m) that he received from Alice.

(4) Charlie tests for mismatches in the same way, but in order to protect against repudiation by Alice he uses a different threshold. Charlie accepts the forwarded message if the number of mismatches in both halves of his key is below $s_v(L/2)$ where s_v is another threshold, with $0 < s_a < s_v < 1/2$.

KEY GENERATION PROTOCOL

We now describe how two parties, for now called Alice and Bob, perform the KGP. Essentially, Alice and Bob perform the quantum part of QKD to generate raw keys, but do not proceed to error correction or privacy amplification. This means that Alice and Bob will generate different (but correlated) strings that are not entirely secret. These keys will be the A_i^B, K_i^B described above. Our aim is to show that $d(A_i^B, K_i^B) < d(E', K_i^B)$ except with negligible probability, where $d(.,.)$ is the Hamming distance and E' is Eve's guess (where it may be that Eve is Charlie). In what follows, the underlying QKD protocol upon which the KGP is built will be the prepare-and-measure decoy-state BB84 protocol using weak coherent pulses, considered in [11]. Other than the post-processing, the only difference is that here it is Bob who prepares the states and sends them along the quantum channel to Alice.

Specifically, we assume that Bob has a phase-randomised source of coherent states. The intensity of each light pulse is chosen by Bob to be either u_0 (signal), u_1 (decoy 1), or u_2 (decoy 2). The intensities are chosen with probabilities $(p_{u_0}, p_{u_1}, p_{u_2})$. To encode information, Bob randomly selects one of four possible polarisation states – $|0_Z\rangle, |1_Z\rangle$ (Z basis) and $|0_X\rangle, |1_X\rangle$ (X basis). The Z and X bases are chosen with probabilities $p_Z \geq 1/2$ and $p_X \leq 1/2$ respectively. Intensities and states are chosen independently by Bob to avoid correlations between intensity and information encoding. If states are transmitted and then measured in different bases, they are discarded (sifting). Bob's key will be the classical information encoded in states prepared in the Z basis with intensity u_0. Alice's key will be the results of her Z basis measurements on states sent with intensity u_0. Decoy state measurements, as well as X basis signal measurements, are used to parametrise Eve's possible attack strategies. It should be stressed that in signature schemes it cannot be assumed that either Alice or Bob are honest. However, as explained below, neither gain from dishonesty during the KGP, and therefore we can assume that they are honest.

In all that follows we will consider the finite case with Eve restricted to collective attacks, and show that she is further from Bob's bit string than Alice. Since we consider only collective attacks, successive states are independent. This means that if we can bound Eve's probability of making an error on a single element of Bob's key given her quantum systems, then we can apply that bound to all of Bob's key elements. Therefore, our strategy will be to bound Eve's uncertainty on a single element of Bob's key. We will use that to find a lower bound for Eve's probability of guessing Bob's key element incorrectly. Let us denote the i^{th} element of Bob's key by the binary random variable X_i. It is shown in [12], [13] that Eve's minimum uncertainty (consistent with parameter estimation) on X_i, given her auxiliary quantum system E_i, is given by

$$\begin{aligned} H_\xi(X_i|E_i) &:= \min_{\sigma_{XE}\in\Gamma_\xi} H(X_i|E_i)_\sigma \\ &= Y_0^L(u_0) + Y_1^L(u_0)[1-h(e_X^U(1))]. \end{aligned} \tag{1}$$

The set Γ_ξ arises due to the finite number of states used for parameter estimation. It is defined, as in [14], to be the set

$$\Gamma_\xi = \left\{\sigma : ||\lambda_m - \lambda_\infty|| \leq \xi := \sqrt{\frac{2\ln(1/\epsilon_{PE}) + 2\ln(m+1)}{m}}\right\}, \tag{2}$$

where λ_m are the statistics observed from measurements on m copies of a state. It contains all states whose asymptotic statistics are within ξ of the statistics observed during parameter estimation, i.e. it contains all states that could arise from Eve performing a collective attack consistent with parameter estimation. The actual state held by Bob-Eve will be in Γ_ξ, except with probability ϵ_{PE}. We say that parameter estimation is successful except with probability ϵ_{PE}.

The terms $Y_0(u_0)$ and $Y_1(u_0)$ are the fraction of the intensity u_0 signals reaching Alice, that come from pulses containing 0 and 1 photons respectively. They are defined as

$$Y_k(u) = \frac{f_k e^{-u_0} u_0^k/k!}{\sum_k f_k e^{-u_0} u_0^k/k!}, \tag{3}$$

where f_k is the probability that Eve forwards a photon to Alice if the signal contains k photons. The superscript L in (1) is included to indicate that we must take the worst-case (lowest) values consistent with parameter estimation and the finite number of states (equations (23) and (24) of [13]).

The quantity $e_X(1)$ in Eq. (1) is the bit error rate in X basis measurements on signal pulses containing a single photon. The superscript U indicates that we must take the worst-case (highest) value consistent with parameter estimation and the finite number of states (equation (25) of [13]). The terms $Y_0^L(u_0), Y_1^L(u_0)$ and $e_X^U(1)$ can all be found using decoy-state techniques.

Eve's goal is to correctly guess the value of X_i given her quantum systems $E_1, ..., E_N$ (where N is the number of states sent and received). In order to gain information on X_i, Eve will perform a general collective measurement on $E_1, ..., E_N$ to produce E', a classical random variable representing the possible outcomes of the collective measurement. Using results from [15] we find

$$\begin{aligned} H(X_i|E_1,...,E_N) &= H(X_i|E_i) \\ &\leq H(X_i|E') \\ &:= \sum_r P(E'=r)H(X_i|E'=r). \end{aligned} \tag{4}$$

The first equality follows since Eve performs a collective attack, and so the overall state before Eve's measurement will be of product form. The inequality follows (after some work) from the Holevo bound, and the last equality follows by definition of the conditional entropy. Note that for each possible $E' = r$, $X_i|E' = r$ is a classical random variable with two possible outcomes, and so $H(X_i|E' = r)$ must equal the binary entropy, $h(p_r)$, for some $p_r \leq 1/2$. Assume that, conditional on Eve's outcome being $E' = r$, we have $X_i = b$ with probability $1 - p_r \geq 1/2$. Eve's best strategy is then to guess $X_i = b$, leading to an error rate of p_r. Eve's average error probability is

$$p_e = \sum_r P(E'=r)p_r.$$

We can use the concavity of the binary entropy, together with (4), to bound p_e as

$$\begin{aligned} h(p_e) &= h\left(\sum_r P(E'=r)p_r\right) \\ &\geq \sum_r P(E'=r)h(p_r) \geq H(X_i|E_i). \end{aligned} \tag{5}$$

Thus $H_\xi(X_i|E_i)$ gives us a lower bound on $h(p_e)$, and since the binary entropy is a monotonically increasing function for $0 \leq p_e \leq 1/2$, this gives us a lower bound on p_e.

Alice's Z basis error rates (on signal pulses) with Bob are estimated directly from parameter estimation as e_Z^U. For Alice to be closer to Bob's string than Eve, we require that $e_Z^U < p_e$. If $p_e, e_Z^U \leq 1/2$, this condition is equivalent to $h(e_Z^U) < h(p_e)$, which is satisfied if

$$H_\xi(X_i|E_i) - h(e_Z^U) > 0. \tag{6}$$

If (6) is not satisfied, then Alice and Bob will abort the protocol. If it is satisfied, then they have the assurance that $p_e > e_Z^U$, except with probability ϵ_{PE}. This allows us to prove security against forging for the full quantum signature protocol.

SECURITY ANALYSIS

We will now prove the security of the main signature protocol, i.e. the robustness (probability of an honest run aborting), security against forging (probability that a recipient generates a signature, not originating from Alice, that is accepted as authentic) and repudiation (probability that Alice generates a signature that is accepted by Bob but then when forwarded, is rejected by Charlie). In what follows we assume that Alice-Bob and Alice-Charlie have each used the KGP to generate length L bit strings to use in the QDS protocol described above.

Robustness. Bob rejects a signed message if the $(1/2)L$ bits received from either Alice or Charlie have a mismatch rate higher than s_a with Alice's signature. For any fixed choice of parameter $\xi > 0$, parameter estimation in the KGP is successful except with probability ϵ_{PE}, which decreases exponentially in the size of the sample used, as can be seen from (19). Let $e_{Z,B}^U$, $e_{Z,C}^U$ be the worst-case Alice error rates with Bob and Charlie respectively. Set $e_Z^U := \max\{e_{Z,B}^U, e_{Z,C}^U\}$ and choose s_a such that $s_a > e_Z^U$. Using Hoeffding's inequalities [16], the probability that Bob will find an error rate higher than s_a is bounded by

$$\mathbb{P}(\text{Honest Abort}) \leq 2\exp\left(-(s_a - e_Z^U)^2 L\right) + 2\epsilon_{PE}, \tag{7}$$

where the ϵ_{PE} is added to account for a possible failure of the PE and the factors of 2 are since the abort can be due to either the states received from Alice or the states received from Charlie.

Security Against Forging. It is easier for either Bob or Charlie to forge than for any other external party, and we will therefore consider forging by an internal party. In order to forge a message, Bob must give a declaration (m, Sig_m) to Charlie that has fewer than $s_v(L/2)$ mismatches with the unknown (to Bob) half of S_m^C sent directly from Alice to Charlie, and fewer than $s_v(L/2)$ mismatches with the half he himself forwarded to Charlie. An adversarial Bob will obviously be able to meet the threshold on the part he forwarded to Charlie. We therefore consider only the unknown half that was received directly from Alice. If parameter estimation is successful in the KGP, then we know the worst-case rates at which Alice and Bob/Eve will make errors with Charlie's key; we denote them e_Z^U, p_e respectively. If the protocol was not aborted, then $e_Z^U < p_e$, so we can choose s_v such that $e_Z^U < s_v < p_e$. On each of the $L/2$ signature elements he is guessing, Bob will make an incorrect guess with probability at least p_e. Using Hoeffding's inequalities [16], the probability that Bob makes fewer than $s_v(L/2)$ errors is bounded by

$$\mathbb{P}(\text{Forge}) \leq \exp(-(p_e - s_v)^2 L) + \epsilon_{PE}, \tag{8}$$

where again the addition of ϵ_{PE} is to account for a possible failure of parameter estimation, in which case the bound $p_e > e_Z^U$ may not hold. Note that security against an adversarial Bob derives entirely from the Alice-Charlie KGP, in which Bob is already assumed to be an adversary. Thus, any dishonesty on Bob's part during the Alice-Bob KGP is cannot help him to forge.

Security Against Repudiation. Alice aims to send a declaration (m, Sig_m) which Bob will accept and, when forwarded, Charlie will reject. To do this, we must have that Bob accepts both the elements that Alice sent directly to him and the elements that Charlie forwarded to him. In order for Charlie to reject he needs only reject one of either the elements he received from Alice, or the elements Bob forwarded to him. Intuitively, security against repudiation follows because of the symmetrisation performed by Bob and Charlie using the secret classical channel. Even if Alice knows and can control the error rates between A_m^B, A_m^C and K_m^B, K_m^C, she cannot control whether the errors end up with Bob or Charlie. After symmetrisation the keys S_m^B and S_m^C will each have the same expected number of errors. To repudiate, one must contain significantly more errors than the other. Using results in [17], we can bound this probability as

$$\mathbb{P}(\text{Repudiation}) \leq 2\exp(-(s_v - s_a)^2 L/4). \tag{9}$$

For a more formal proof, please see the supplementary material. Note that security against repudiation derives entirely from the symmetrisation performed by Bob and Charlie, in which Alice plays no part. Even if Alice can control the choices of s_a, s_v by manipulating the error rates achieved during the Alice-Bob KGP and the Alice-Charlie KGP, the choice of L depends on s_a and s_v and the protocol will be secure for any valid choice.

COMPARISON TO QKD

For the finite setting BB84 protocol performed using decoy states as described above, [13] gives the secret key rate (per state sent and received in the Z basis) as

$$r = H_\xi(X_i|E_i) - (\text{Leak}_{EC} + \Delta)/n, \tag{10}$$

where n is the number of states sent and measured in the Z basis, and Δ is a constant depending on the probabilities of failure for PE, error correction and privacy amplification. The term Leak_{EC} depends on the implementation of error correction, but must be greater or equal to the asymptotic value of $nh(e_Z^U)$. In practice, error correction will not be perfect and it is common to write $\mathrm{Leak}_{EC} = nf_{EC}h(e_Z^U)$ where f_{EC} is a leakage parameter. To perform error correction, the total key is split into blocks and the leakage parameter, f_{EC}, depends on this block size, but not the overall length of the key. Increasing the block size reduces f_{EC} at the cost of decreasing the efficiency of the error correction protocol. Estimates of f_{EC} for practically feasible error correction is an area of active research [18], though it is commonly estimated to be in the range $1.11 - 1.2$, regardless of the length of the total key being distilled. For example, [14] assumes $f_{EC} = 1.2$ based on the performance of error correcting codes in use at ID Quantique. Rewriting (10), we get

$$r = H_\xi(X_i|E_i) - f_{EC}h(e_Z^U) - \frac{\Delta}{n}. \tag{11}$$

Comparing equations (6) and (11), we immediately see that there are channels for which quantum signatures are possible and yet practical QKD is not. As stated above, f_{EC} is independent of n and so cannot be decreased by simply increasing the size of the total key. The important point is that because the quantum signature scheme omits the inefficient process of error correction, there should always be some region where quantum signatures is possible but QKD is not.

DISCUSSION

In this paper we have presented a quantum unconditionally secure signature protocol which improves on previous quantum signature protocols by removing all trust assumptions on the quantum channels between participants. One could expect that by removing strong trust assumptions (authenticated quantum channel) the efficiency of the protocol would decrease. In fact the opposite is true – our protocol significantly reduces the length of the signature needed to sign a message. Finite sample size effects mean that it is inefficient to use the KGP to generate small keys (although it is possible for sample size as small as $O(10^5)$ [11]). Instead, we use the KGP to generate long strings which are split up and used to sign more than one message [19]. In this case, the values of p_e and e_Z^U must be slightly increased to account for further finite size variations (see supplementary material). To compare with previous papers, we say the protocol is secure if the probabilities in (20), (25), (24) are all below 10^{-4}. Using realistic experimental assumptions, we estimate that by running the KGP long enough to generate a reasonable number of counts, a signature length of $L = 3.5 \times 10^5$ is necessary to securely sign a single half bit over a distance of 50 km. This would require Bob/Charlie to transmit approximately 9.35×10^8 states to Alice during their KGP's. We compare this to previous quantum signature protocols which required $O(10^{10})$ states to be transmitted to achieve the same level of security over 1 km [20].

The increase in efficiency is largely due to the fact that in our protocol Alice sends *different* states to Bob and Charlie, whereas in previous protocols she sent them the same states. In those protocols, even without any eavesdropping, a potential forger had access to a legitimate copy of each of the states Alice sent to the participants and thus to reach same levels of security required longer signatures. Moreover, when generalising to N participants with up to t dishonest parties, potential forgers are even more powerful, since we need to assume they have t legitimate copies of each state. In our protocol, where we send different states to each participant, this problem is evaded. The only source of information for a potential forger is by eavesdropping on the quantum channels, an activity bypassed in previous protocols due to the assumption of "authenticated" quantum channels. We note here that our analysis considered only the scenario where Eve is restricted to collective attacks. For QKD it is shown that due to the symmetry of BB84, it is sufficient to consider only those attacks that leave Alice-Bob with a convex combination of product states [22]. We therefore conjecture that our protocol will be secure even against coherent attacks [23], but leave a rigorous proof for future work.

In this paper we showed that the noise threshold in the quantum channels connecting Alice-Bob and Alice-Charlie is less strict for quantum signatures than for distilling a secret key using QKD in practice. For some quantum channels, therefore, quantum signature protocols that use QKD (e.g. P2 of [4]) are not possible, while our direct quantum protocol remains possible. This is an example that direct quantum protocols are sometimes preferrable, and highlights that there is a lot more in quantum signatures than a simple application of QKD.

The authors would like to thank Vedran Dunjko for discussions. This work was supported by the UK Engineering and Physical Sciences Research Council (EPSRC) under EP/G009821/1 and EP/K022717/1. P.W. gratefully acknowledges support from the COST Action MP1006. A.K. was partially supported by a grant from FQXi and by Perimeter Institute for Theoretical Physics. Research at Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research and Innovation.

Supplementary Material for *Secure Quantum Signatures Using Insecure Quantum Channels*

Ryan Amiri[1*], Petros Wallden[2], Adrian Kent[3,4] and Erika Andersson[1]

[1]*SUPA, Institute of Photonics and Quantum Sciences, Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom*
[2]*LFCS, School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, United Kingdom*
[3]*Centre for Quantum Information and Foundations, DAMTP, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge, CB3 0WA, United Kingdom*
[4]*Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, ON N2L 2Y5, Canada*
*ra2@hw.ac.uk

KEY GENERATION PROTOCOL

Equation 1

In the entanglement-based view of the protocol, as in equation (8) of [12], Bob prepares the states

$$|\Psi_j\rangle_{ABR_1} = \sum_{n\geq 0} \sqrt{p_n} |\Psi_j^n\rangle_{AB} |n\rangle_{R_1} \tag{12}$$

Where $j = X, Z$ represents the choice of basis and $|\Psi_j^n\rangle_{AB} = 1/\sqrt{2}(|0\rangle_B |0_j\rangle_A^{\otimes n} + |1\rangle_B |1_j\rangle_A^{\otimes n})$. The system R_1 keeps track of how many photons are contained in the pulse sent by Bob. As in [12], we assume an uncalibrated device scenario (all errors/losses are attributed to Eve) and the squashing model for Alice's detectors (which, for BB84 was proven to exist in [25]). Under these assumptions, we can assume that, after interaction, Eve forwards a single photon state to Alice so that the state shared by Alice and Bob is a two qubit state. Bob can then perform an X or Z basis measurement to prepare Alice's system at a distance. Alice will also make the usual X or Z basis measurements. Under the assumption of collective attacks, Eve performs the same unitary to each state and so after transmission (but before measurements) the state is

$$|\chi\rangle_{ABER_1R_2} = \sum_j A_j U_{AE}(|\Psi_j\rangle_{ABR_1}|0\rangle_E)|j\rangle_{R_2} \tag{13}$$

Where A_j is the operation performed by Alice on single qubit states ($A_Z = \mathbb{I}_A$ and $A_X = H$, where H is the Hadamard transformation). The system R_2 keeps track of the basis used by Bob to encode information. We aim to find Eve's uncertainty on X, a random variable representing the outcome of a Z-basis measurement made by Bob on his system. That is, we aim to find $H(X|E, j = Z)$. As in [12], we find

$$H(X|E, j = Z) \geq \sum_{n=0}^{\infty} P(n) H(X|E, n, j = Z) \tag{14}$$

Where $H(X|E, n, j = Z)$ is the uncertainty Eve has on the outcome of Bob's Z-basis measurement, given there were n photons in the pulse Bob sent to Alice. In the main paper, we do not explicitly write $j = Z$ since it is stated that Bob's key comes from Z-basis measurements. We consider three different cases.

- For $n > 1$ Eve has full information on the outcome of Bob's measurement, and so $H(X|E, n > 1, j = Z) = 0$.
- For $n = 1$, Bob sends a single photon pulse to Alice and we are in the usual single photon QKD scenario. We use standard results in QKD (see, for example, Appendix A of [21]) to say Eve's uncertainty is $H(X|E, n = 1, j = Z) = 1 - h(e_X(1))$.
- For $n = 0$, Bob sends nothing along the quantum channel, so Eve has full uncertainty on the outcome of Bob's measurement, so $H(X|E, n = 0, j = Z) = 1$ as shown in [26].

As a last step, we must minimise $H(X|E, j = Z)$ over all possible states consistent with the parameters estimated by Alice and Bob. This gives equation (1) of the main paper.

Alternative Strategy

We take this opportunity to mention a possible improvement to the bound on Eve's average error probability. Using the argument in equation (5) of the main paper, we can show that Eve's average error probability when guessing the value of X_i is at least p_e, where $h(p_e) \geq H(X_i|E_i)_\sigma$, where σ is the state in Γ_ξ minimising $H(X_i|E_i)_\sigma$. We assume the worst case scenario and take $h(p_e) = H(X_i|E_i)_\sigma$. Consider instead if we were to estimate Eve's error probability *given* a pulse containing n photons. Let q_n be the bound on average error probability that Eve has when guessing the value of X, given the pulse contained n photons - i.e. q_n is such that $h(q_n) = H(X|E,n)_\sigma$. Note that $q_n = 0$ for $n > 1$. Eve's overall error rate would be

$$q = P(n=0)q_0 + P(n=1)q_1$$

and so

$$h(q) = h(P(n=0)q_0 + P(n=1)q_1) \geq P(n=0)h(q_0) + P(n=1)h(q_1) = h(p_e)$$

Note that in fact the first inequality is strict as long as neither q_0 nor q_1 is zero. Therefore, this method actually gives a better estimate of Eve's average error rate. The former method is used however to highlight similarities with QKD, as well as to avoid difficulties in optimising Eve's strategy. Namely, it may be that under this analysis the collective attack represented by σ is not actually optimal for Eve. Instead, an attack giving a larger average uncertainty may actually lead to fewer errors with Bob's key. Nevertheless, p_e will still hold as an overall lower bound.

Equation 4

We start from equation (13) above. The overall state shared by Alice, Bob and Eve is the product state $|\chi\rangle\langle\chi|^{\otimes N}$. The state held by Alice and Bob is the two qubit state $\rho_{AB}^{\otimes N}$ obtained by tracing out systems E, R_1 and R_2. Following their measurements, Alice and Bob share the state $\sigma_{YX}^{\otimes N}$, and the Bob-Eve state can be written $\sigma_{XE}^{\otimes N}$. Let us denote the i^{th} element of the product state by $\sigma_{X_iE_i}$. Since we have a product state, it is easy to verify using the definition of the quantum conditional entropy that

$$H(X_i|E)_{\sigma^{\otimes N}} = H(X_i|E_i)_\sigma \tag{15}$$

This gives us the first equality in equation (4) of the main paper.

To see the inequality, consider that the maximum amount of information Eve can gain on X_i from measurements on $E_1, ..., E_N$ is quantified by the accessible information:

$$I_{acc} = \max_\Lambda I(X_i; E') \tag{16}$$

where E' represents the classical random variable induced by the measurement Λ, and the maximisation is over all possible collective measurements on $E_1, ..., E_N$. A useful upper bound on the accessible information is the Holevo quantity which, for classical quantum states, is given by the quantum mutual information [15], $I(X_i; E_1, ..., E_N)$. So we have

$$I(X_i; E_1, ..., E_N) \geq I_{acc} = \max_\Lambda I(X_i; E') \tag{17}$$

From the definitions of quantum mutual information and conditional quantum entropy, (17) implies

$$H(X_i|E_1, ..., E_N) \leq H(X_i|E') \tag{18}$$

This gives the inequality in equation (4).

QDS PROTOCOL SECURITY PROOFS

Robustness

Bob aborts if either the $(1/2)L$ states received from Alice have an error rate higher than s_a or the $(1/2)L$ states received from Charlie have error rate higher than s_a. Parameter estimation in the KGP is successful except with probability ϵ_{PE}, which decreases exponentially in the size of the sample used, according to

$$\epsilon_{PE} = (m+1)e^{-\frac{1}{2}m\xi^2}, \tag{19}$$

where m is the sample size. Let $e^U_{Z,B}$, $e^U_{Z,C}$ be Alice's worst case Z basis error rates found during PE with Bob and Charlie respectively. Set $e^U_Z := \max\{e^U_{Z,B}, e^U_{Z,C}\}$. Choose s_a such that $s_a > e^U_Z$; then, using Hoeffding's inequalities [16], the probability that Bob will find an error rate higher than s_a is bounded by

$$\mathbb{P}(\text{Honest Abort}) \leq 2\exp\left(-(s_a - e^U_Z)^2 L\right) + 2\epsilon_{PE}. \tag{20}$$

The ϵ_{PE} is added to account for the possibility of failure of PE. The factors of 2 arise due to the possibility of abort due to either the states received from Alice or the states received from Charlie.

Repudiation

Alice aims to send a declaration (m, Sig_m) which Bob will accept and which Charlie will reject. For this to happen, Bob must accept both the elements that Alice sent directly to him, and the elements that Charlie forwarded to him. In order for Charlie to reject he need only reject either the elements he received from Alice, or the elements Bob forwarded to him (or both). Intuitively, security against repudiation follows because of the symmetrisation performed by Bob and Charlie using the secret classical channel. In the distribution stage, to send the future message m, Alice will use the KGP with Bob and Charlie so that they hold the strings $(b_1, ..., b_L)$ and $(c_1, ..., c_L)$ respectively. We give Alice full power and assume that later on, in the messaging stage, she is able to fully control the number of mismatches her signature declaration contains with $(b_1, ..., b_L)$ and $(c_1, ..., c_L)$. Call the mismatch rates e_B and e_C respectively. Now, the symmetrisation process means that Bob and Charlie will randomly (and unknown to Alice) receive $L/2$ elements of the of the other's string. We aim to show that any choice of e_C, e_B leads to an exponentially decaying probability of repudiation.

Suppose $e_C > s_a$: In this case, Bob is selecting (without replacement) $L/2$ elements from the set $\{c_1, ..., c_L\}$, which contains exactly $e_C L$ mismatches with Alice's future declaration. The number of mismatches Bob selects then follows a hypergeometric distribution $H(L, e_C L, L/2)$ with expected value $e_C L/2$. In order to accept the message, Bob must select fewer than $s_a L/2$ errors. Using [17] we can bound the probability that Bob selects fewer than $s_a L/2$ mismatches as

$$\mathbb{P}(\text{Bob receives fewer than } s_a L/2 \text{ mismatches from Charlie}) \leq \exp(-(e_C - s_a)^2 L). \tag{21}$$

To repudiate, Alice must make Bob accept the message, which means Bob must accept both the part received from Alice and the part received from Charlie. Since $\mathbb{P}(A \cap B) \leq \min\{\mathbb{P}(A), \mathbb{P}(B)\}$ the probability of repudiation must be less than or equal to the above expression, and so must also decrease exponentially.

Suppose $e_C \leq s_a$: In this case, if $e_B > s_a$, the above argument shows that it is highly likely that Bob will reject the message, so we consider only the case where $e_B \leq s_a$. Consider first the set $\{b_1, ..., b_L\}$. We can use the same arguments as above to bound the probability of selecting more than $s_v L/2$ mismatches as

$$\mathbb{P}(\text{Charlie selects more than } s_v L/2 \text{ mismatches from Bob}) \leq \exp(-(s_v - e_B)^2 L). \tag{22}$$

Alice succeeds if Charlie selects more than $s_v L/2$ mismatches from either the set $\{b_1, ..., b_L\}$ or the set $\{c_1, ..., c_L\}$. Using $\mathbb{P}(A \cup B) \leq \mathbb{P}(A) + \mathbb{P}(B)$, we can see that, for the choice of $e_B, e_C \leq s_a$, we have

$$\mathbb{P}(\text{Charlie selects more than } s_v L/2 \text{ mismatches}) \leq 2\exp(-(s_v - s_a)^2 L). \tag{23}$$

So again, the probability of Alice successfully repudiating decreases exponentially in the size of the signature. Similar to [4], Alice's best strategy would be to pick $e_B = e_C = \frac{1}{2}(s_v + s_a)$, in which case

$$\mathbb{P}(\text{Repudiation}) \leq 2\exp\left(-\frac{1}{4}(s_v - s_a)^2 L\right) \tag{24}$$

Forging

In order to forge a message, Bob must give a declaration (m, Sig_m) to Charlie that has fewer than $s_v(L/2)$ mismatches with the unknown (to Bob) half of S^C_m sent directly from Alice to Charlie, and fewer than $s_v(L/2)$ with the half he himself forwarded to Charlie. We can assume that Bob will make fewer than $s_v(L/2)$ errors on the half that he forwarded to Charlie, and we consider only the unknown half. If parameter estimation is successful in the KGP, then we know the worst-case rates at which Alice and Bob/Eve (Charlie) will make errors with Charlie's (Bob's) key; denote them e_Z^U, p_e respectively. If the protocol was not aborted, then $e_Z^U < p_e$, so we can choose s_v such that $e_Z^U < s_v < p_e$. On each of the $L/2$ signature elements he is guessing, Bob will make an incorrect guess with probability p_e, independent of all other guesses (since we consider only collective attacks). Using Hoeffding's inequalities [16], the probability that Bob makes fewer than $s_v(L/2)$ errors is bounded by

$$\mathbb{P}(\text{forge}) \leq \exp(-(p_e - s_v)^2 L) + \epsilon_{PE}. \tag{25}$$

The addition of ϵ_{PE} is to account for the possibility that parameter estimation fails, in which case the bound $p_e > e_Z^U$ may not hold. Note that for simplicity we did not consider the scenario where Charlie is the forger, but it can be seen that exactly the same argument applies.

Parameters and Constraints

The correctness and security of the protocol depends on the three equations (20), (24) and (25), which in turn depend on the choice of parameters s_a and s_v. The parameters must be such that $e_Z^U < s_a < s_v < p_e$. Here, and in all that follows, e_Z^U is the maximum of the worst-case error rates Alice makes with Bob's key (found from the Alice-Bob KGP), and the worst-case error rates Alice makes with Charlie's key (found from the Alice-Charlie KGP). Similarly, p_e is the minimum of the eavesdroppers error rates found from the Alice-Bob and Alice-Charlie KGP. The aim is to choose the parameters which minimise the value of the overall signature length, L.

In the next section, we will calculate the length of the signature necessary to sign a message with a security level of 10^{-4}. By this, we mean that the probabilities of honest abort, repudiation and forging, given respectively by (20), (24) and (25), are all less than 10^{-4}. To find the length of the signature necessary to securely sign a half bit, we must first choose the parameters s_a and s_v. Ideally, our choice would minimise the total length of the signature, L. For simplicity, we choose to make ϵ_{PE} small, $\epsilon_{PE} = 10^{-6}$, so that we can neglect the possibility of PE failing. Since there seems no reason to prioritise one security over any other, we choose s_a and s_v so as to make the exponential terms in (20), (24) and (25) all (approximately) equal. This means that

$$s_a = e_Z^U + \frac{p_e - e_Z^U}{4}, \qquad s_v = e_Z^U + \frac{3(p_e - e_Z^U)}{4}. \tag{26}$$

Nevertheless, it can be seen that if a certain application desires a higher security against one particular threat (e.g. forging), it is simple to choose the parameters to prioritise security against that threat.

CALCULATION OF SIGNATURE LENGTH

In this section, we use experimental data provided by [11] to give a rough estimate the number of states that Bob needs to transmit over the quantum channel to securely sign a half bit at 50km. We set $\epsilon_{PE} = 10^{-6}$ in all equations that follow. The experiment in [11] approximately achieves the values

- Basis probabilities: $p_Z = 93.75\%$, $p_X = 6.25\%$.
- Intensity levels: $(u_0, u_1, u_2) = (0.425, 0.0435, 0.0022)$.
- Detection rates per qubit sent: $R_{u_0} = 4.82 \times 10^{-3}$, $R_{u_1} = 7.45 \times 10^{-4}$, $R_{u_2} = 3.01 \times 10^{-4}$.
- Error rates (per detected qubit): $e_X^{u_0} = 0.0364$, $e_X^{u_1} = 0.146$, $e_X^{u_2} = 0.333$, $e_Z^{u_0} = e_Z = 0.0426$ (for the Z basis error rates we drop the superscript as we are only interested in signal pulse error rates).

Let N_{Z,u_i} be the number of counts registered in the Z basis for intensity u_i. If we choose intensities with probabilities $p_{u_0} = 88\%$, $p_{u_1} = 8\%$ and $p_{u_2} = 4\%$, then if we send 10^{13} states in total (which would take under 3 hours), we expect to get $N_{Z,u_0} = 3.73 \times 10^{10}$, $N_{Z,u_1} = 5.24 \times 10^8$, $N_{Z,u_2} = 1.06 \times 10^8$ and $N_{X,u_0} = 1.65 \times 10^8$.

Let us define

$$\xi(m, 2) := \frac{1}{2}\sqrt{\frac{2\ln(1/\epsilon_{PE}) + 2\ln(m+1)}{m}}$$

and

$$p(k|u_i) = e^{-u_i}\frac{u_i^k}{k!}$$

Using [13] we can use these to estimate $Y_0^L(u_0)$, $Y_1^L(u_0)$ and $e_X^U(1)$. Note that we use the approximation that u_2 is the vacuum intensity. In practice, with high rate sources it is difficult to reduce the intensity down to exactly the vacuum, and there is often a small residual intensity. Nevertheless the following analysis should give good results. Equation (18) of [13]:

$$f_0 = R_{u_2} \tag{27}$$

Equation (19) of [13]:

$$f_1 = \frac{1}{u_0 - u_1}\left[R_{u_1}\frac{u_0}{p(1|u_1)} - R_{u_0}\frac{u_1}{p(1|u_0)}\right] - f_0\frac{u_0 + u_1}{u_1 u_0} \tag{28}$$

Note that these estimates should include finite size variations. However, we follow [13] in making the simplifying approximation that the f_k are as above (the asymptotic values), and we add finite size fluctuation terms onto the $Y_k(u_i) = p(k|u_i)f_k$, given below. For reasonably large count samples (as considered here) this should be a good approximation. Equation (23) of [13]:

$$Y_0^L(u_i) = \left[p(0|u_i)R_{u_2} - \xi(N_{Z,u_2}, 2)\right]/R_{u_i} \tag{29}$$

Equation (24) of [13]:

$$Y_1^L(u_i) = \left[p(1|u_i)f_1 - \xi(N_{Z,u_i}, 2)\right]/R_{u_i} \tag{30}$$

Equation (25) of [13], with u_0 chosen as the signal intensity:

$$e_X^U(1) = \frac{e_X^{u_0,U} - Y_0^L(u_0)e_X^{u_2,L}}{Y_1^L(u_0)} \tag{31}$$

Where $e_X^{u_0,U} = e_X^{u_0} + \xi(N_{X,u_0}, 2)$ and $e_X^{u_2,L} = e_X^{u_2} + \xi(N_{Z,u_2} + N_{X,u_2}, 2)$.

Using these equations together with equation (1) of the main paper, we find

$$H_\xi(X_i|E_i) = 0.392 \tag{32}$$

This gives $p_e = 7.71\%$. Further, if we used 10^8 states of the Z basis signal pulse counts to estimate e_Z, then $e_Z^U = e_Z + \xi(10^8, 2) = 4.3\%$. This bound holds except with probability ϵ_{PE}. These hold as error rates over the entire 3.73×10^{10} key generated. If we are to split this key into chunks of length 3.5×10^5, we must make additional finite size estimates. Namely, we must decrease p_e by $\xi(3.5 \times 10^5, 2)$ and increase e_Z^U by $\xi(3.5 \times 10^5, 2)$ where $\xi(3.5 \times 10^5, 2) = 6.16 \times 10^{-3}$. This gives our new estimates for Alice and Eve's worst case error rates as $\tilde{p}_e = 7.09\%$ and $\tilde{e}_Z^U = 4.92\%$. For these new error rates, the protocol is secure for $L = 3.5 \times 10^5$. This means that from the 3.73×10^{10} key bits generated, we can sign 1.07×10^5 messages. Since we originally sent 10^{13} states, this means it takes 9.35×10^8 states sent to securely sign a single bit over 50km.

It should be stressed that this analysis is rough, and has not been optimised. Using the statistical techniques in [11] could significantly increase the quoted rates. Further, if we instead use the method suggested in the "Alternative Strategy" subsection above, we would find Eve's error rate (on Bob's entire key) to be $p_e = 10.2\%$, a significant improvement.

* ra2@hw.ac.uk

[1] D. Chaum and S. Roijakkers, Unconditionally-secure digital signatures, Advances in Cryptology-CRYPTO'90, LNCS, Santa Barbara, USA, 1990, vol. **537**, pp. 206-2014 (1991), Springer, Berlin, Heidelberg.

[2] G. Hanaoka, J. Shikata, Y. Zheng, H. and Imai, Unconditionally secure digital signature schemes admitting transferability, Advances in Cryptology-ASIACRYPT 2000, LNCS, Kyoto, Japan, 2000, vol. **1976**, pp. 130-142 (2000), Springer, Berlin, Heidelberg.

[3] C. M. Swanson, and D. R. Stinson,, Unconditionally secure signature schemes revisited, Information Theoretic Security, Proceedings of ICITS 2011, LNCS, Amsterdam, The Netherlands, vol. **6673**, pp. 100-116 (2011), Springer, Berlin, Heidelberg.

[4] P. Wallden, V. Dunjko, A. Kent, and E. Andersson, "Quantum digital signatures with quantum-key-distribution components", Phys. Rev. A **91**, 042304 (2015).

[5] D. Gottesman and I. Chuang, “Quantum Digital Signatures”, arXiv:quant-ph/0105032v2 (2001).

[6] V. Dunjko, P. Wallden, and E. Andersson, “Quantum Digital Signatures without quantum memory”, Phys. Rev. Lett. 112, 040502 (2014).

[7] 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).

[8] J. M. Arrazola, P. Wallden and E. Andersson, “Multiparty Quantum Signature Schemes”, In Preparation (2015).

[9] T.-Y. Wang, X.-Q. Cai, Y.-L. Ren and R.-L. Zhang, “Security of quantum digital signatures for classical messages”, Sci. Rep. **5**, 9231 (2014).

[10] This is not essential, but simplifies the analysis when participants are honest, since each measurement result carries the same weight.

[11] M. Lucamarini et al. “Efficient decoy-state quantum key distribution with quantified security”, Opt. Express **21**, 24550 (2013).

[12] Kraus, Barbara, Cyril Branciard, and Renato Renner, “Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses.” Physical Review A **75**, 012316 (2007).

[13] Y. Q. Cai and V. Scarani, “Finite-key analysis for practical implementations of quantum key distribution.” New Journal of Physics **11**, 045024 (2009).

[14] 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).

[15] M. Wilde, “From Classical to Quantum Shannon Theory”, arXiv:1106.1445 [quant-ph] (2011).

[16] W. Hoeffding, “Probability inequalities for sums of bounded random variables”, J. Amer. Statist. Assoc., **58**, 301 (1963).

[17] V. Chvatal, “Tails of Hypergeometric Distributions”, Discrete Math. **25**, pp. 285-287 (1979).

[18] M. Tomamichel, J. Martinez-Mateo, C. Pacher, D. Elkouss, “Fundamental Finite Key Limits for Information Reconciliation in Quantum Key Distribution”, arXiv:1401.5194v1 [quant-ph] (2014).

[19] This splitting of the generated keys does not compromise security for Eve restricted to collective attacks, but composability should be considered more carefully when Eve is allowed coherent attacks.

[20] R. Donsldson, R. Collins, K. Kleczkowska, R. Amiri, P. Wallden, V. Dunjko, E. Andersson, J. Jeffers and G. Buller, “Experimental demonstration of kilometre range quantum digital signatures”, in preparation (2015).

[21] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, “The Security of Practical Quantum Key Distribution”, Rev. Mod. Phys. **81**, 1301 (2009).

[22] R. Renner, N. Gisin, and B. Kraus, “Information-theoretic security proof for quantum-key-distribution protocols”, Phys. Rev. A **72**, 012332 (2005).

[23] Indeed, for the case of asymptotically large signature lengths, unconditional security follows from the exponential de Finetti theorem [24].

[24] R. Renner, “Symmetry implies independence”, Nat. Phys. **3**, 645 (2007).

[25] Beaudry, Normand J., Tobias Moroder, and Norbert Lütkenhaus. “Squashing models for optical measurements in quantum communication.” Phys. Rev. Lett. **101**, 093601 (2008).

[26] Koashi, Masato. “Efficient quantum key distribution with practical sources and detectors.” arXiv preprint quant-ph/0609180 (2006).