A Channel Frequency Response-Based Secret Key Generation Scheme in In-band Full-duplex MIMO-OFDM Systems

A Channel Frequency Response-Based Secret Key Generation Scheme in In-band Full-duplex MIMO-OFDM Systems

Haifeng Luo, Navneet Garg, *Member, IEEE*, and Tharmalingam Ratnarajah, *Senior Member, IEEE*

***Abstract*—Physical layer-based secret key generation (PHY-SKG) schemes have attracted significant attention in recent years due to their lightweight implementation and ability to achieve information-theoretical security. In this paper, we study a channel frequency response (CFR)-based SKG scheme for in-band full-duplex (IBFD)-multi-input and multi-output (MIMO) systems. We formulate the intrinsic practical imperfections and derive their effects on the probing errors. Then we derive closed-form expressions for the secret key capacity (SKC) in the presence of a passive eavesdropper accordingly. We analyze the asymptotic behavior of the SKC in the high-SNR regime and reveal the fundamental limits for IBFD and HD probing. Based on the asymptotic SKC, we investigate the conditions under which IBFD can outperform HD. Numerical results illustrate that effective analog self-interference cancellation (ASIC) depth is the basis for IBFD probing to gain benefits over HD. Finally, we analyze the properties of the collected samples of the CFR-based SKG scheme and propose an averaging pre-processing and a segmental quantization, which reduce the key disagreement rate and remove the effects of large-scale fading to guarantee randomness. 3GPP specification-based simulations and the National Institute of Standards and Technology (NIST) test suite verify the theoretical analysis and the effectiveness of the proposed SKG scheme.**

***Index Terms*—In-band full-duplex, MIMO, physical layer security, secret key generation**

I. Introduction

WIRELESS communication networks are vulnerable to eavesdropping due to the broadcast nature of wireless channels. The mobility and heterogeneity of users and limited resources (e.g., power supply and computing capacity) make it challenging to protect the wireless transmission from the physical layer [1]. Thus, the security of wireless networks is conventionally ensured by encryption schemes, where the message is encrypted with a secure key. Classical encryption schemes are applied in the upper layers of the protocol, which achieves computational complexity-based security. These schemes require key distribution by a secure management center and may become ineffective in the future due to the rapidly growing computational capacity. In contrast, physical layer security (PLS) can achieve information-theoretical security without aid from other users or infrastructures [2]. Thus, it has attracted increasing attention from the security community.

Physical layer-based secret key generation (PHY-SKG) schemes utilize the reciprocity and unpredictable randomness of wireless channels to generate the key. Eavesdroppers located more than one half-wavelength away from legitimate users will experience uncorrelated fading. This spatial decorrelation assumption guarantees the security of the generated key, which is claimed in most related papers [2]–[6].

In the literature, time-division duplexing (TDD) is usually considered for PHY-SKG schemes, where channel reciprocity is assumed to be held. Various characteristics are exploited to generate the key in the literature, which can be categorized into received signal strength (RSS)-based schemes and channel state information (CSI)-based schemes. The secret key capacity (SKC) of the two methods is compared in [7], which reveals that the RSS-based SKG is seriously penalized compared to the CSI-based scheme. However, CSI-based schemes need to estimate the CSI from the observations and quantize specific parameters of the channel (e.g., channel gain or phase), resulting in high implementation complexity. In [8], a 3D spatial angle-based SKG scheme is proposed for frequency-division duplexing (FDD) systems based on the assumption that reciprocity exists in terms of the angle of departure and angle of arrival of each dual path.

However, many studies reveal that the asymmetric observations due to non-simultaneous measurements in half-duplex (HD) systems and the inherent transceiver hardware impairments (HWIs) reduce the PHY-SKG performance [5], [9], [10]. These effects are formulated and analyzed by deriving the SKC for the PHY-SKG scheme with HWIs in [9]. It reveals that although some signal processing and filtering techniques [4], [6], [10], including neural networks [5], can be employed to compensate for the imperfections, the imperfect channel reciprocity due to non-simultaneous measurements and transceiver HWIs fundamentally limit the performance of HD PHY-SKG. While a high key generation rate (KGR) is necessary for the real-time implementation of PHY-SKG; otherwise, the same key will be used for a long duration.

The simultaneous transmission and reception nature of in-band full-duplex (IBFD) could enable simultaneous measurements and provide more time-frequency resources for probing signals than HD, improving the key performance. It is analyzed in [3] that the key rate in IBFD is generally higher than its HD counterpart in the high-SNR regime at the cost of self-interference cancellation (SIC). However, the residual self-interference (RSI) and the overheads of SIC could lead to the IBFD key rate being less than its HD counterpart with low SNR and highly correlated channel observations. Numerical results in [1] illustrate that the key disagreement rate (KDR) dropped at least 60% and the KGR increases to up to 1.8 times

H. Luo, N. Garg, and T. Ratnarajah are with Institute for Digital Communications, School of Engineering, The University of Edinburgh, UK, e-mails: s1895225@ed.ac.uk, navneet.garg4@gmail.com, t.ratnarajah@ed.ac.uk.

with increased entropy of keys by IBFD probing than existing HD-based schemes. Authors in [11] compare the secret key rates with the rate-limited public channel by introducing the reconciliation function in IBFD and HD radios. Simulation results illustrate that IBFD improves the secret key rate and has negative effects on the eavesdropper's capacity. Although there are many studies exploring applying IBFD for PHY-SKG, a comprehensive derivation and analysis of the benefits and limits of the IBFD-based SKG are still lacking.

In addition to the probing errors, the coherence time of the channel is also a critical factor affecting the KGR [12]. For instance, the mobility of users is limited for wireless local area networks (WLAN), resulting in a relatively stable channel. In this case, a relatively low probing rate is needed to guarantee randomness, yielding a slow KGR. To address this issue, multiple-input and multiple-output (MIMO) systems, where more randomness is provided for key generation, are employed to increase the KGR. The SKC in MIMO-OFDM systems is analyzed in [13], which shows the benefits of antenna arrays on the SKC. In addition to the KGR improvement, studies also reveal the benefits of MIMO systems in security. In [14], a practical PHY-SKG scheme based on precoding matrix indices is proposed, where rotated reference signals are utilized to enhance security. This scheme guarantees the usage of full MIMO gain and can be employed in practice without reconciliation and privacy amplification. Besides, the antenna arrangements have dramatic impacts on the MIMO channel between legitimate users, which poses a greater challenge to the eavesdropper. An optimal beamforming design is proposed in [15] to reduce the pilot overhead of the reciprocal CSI acquisition. However, the realistic correlated MIMO channel may decrease the security due to the correlation between the generated key. To address this issue, a decorrelation vector is utilized in [16] to generate a uniformly-distributed bit sequence with the correlated MIMO channel.

Therefore, it is interesting to further study the application of PHY-SKG in IBFD-MIMO systems since IBFD and MIMO can improve the PHY-SKG performance and are promised to be widely employed in current and future wireless networks. In contrast, existing studies in this direction usually only consider single-antenna [1], [3], [5], [9], [11], [17] or HD systems [4], [5], [15], [18] or lack practical implementation [3], [11], [17] and imperfection considerations [1], [4], [7], [18]. In addition, most of the existing studies consider the spatial independence assumption [2]–[6], ignoring the effects of a possible close eavesdropper who can acquire a correlated channel. In this paper, we formulate the intrinsic practical imperfections via measurable metrics and derive the SKC in the presence of a passive eavesdropper who can be located anywhere, giving a deep insight into the limits of the SKC. Orthogonal frequency division multiplexing (OFDM) has been utilized in many wireless protocols [5], and the 5G NR and WLAN protocols provide the channel frequency response (CFR) measuring resources, e.g., the CSI-reference signal (CSI-RS) in 5G NR and the long permeable in Wi-Fi. Thus, we consider a CFR-based SKG scheme in OFDM systems for implementation and efficiency considerations. Our contributions can be summarized as follows.

- *Closed-form expressions of SKC*: We formulate and analyze the effects of noise, asymmetric transceiver HWIs, non-simultaneous probing (for HD), self-interference cancellation (SIC) schemes (for IBFD), and channel estimation errors on the performance of the CFR-based SKG. We consider a feasible 3-step SIC scheme and derive the effects of RSI with measurable metrics (e.g., analog cancellation level and noise of RF cancellers). Finally, we derive the closed-form expression for the SKC in the IBFD-MIMO system in the presence of a passive eavesdropper under these intrinsic imperfections and compare it to its HD counterpart. Two cases of the eavesdropper's location are considered, where the eavesdropper may be very close to legitimate users and experience correlated fading, or the eavesdropper is far away and experience independent fading.
- *Fundamental limits and IBFD gain analysis*: We analyze the asymptotic behavior of the SKC in the high-SNR regime and reveal the fundamental limits in HD and IBFD systems. Based on the asymptotic behavior analysis, we investigate the condition under which IBFD can gain benefits over HD.
- *Pre-processing and segmental quantization scheme*: We analyze the properties of collected samples and propose a pre-processing and segmental quantization scheme to guarantee the effectiveness of the generated key sequences. The CFRs on subcarriers within the same coherence bandwidth are averaged to reduce the effects of estimation errors, and collected samples are segmented into multiple blocks and independently quantized within each block to remove the effects of large-scale fading and guarantee randomness.
- *Performance evaluation through 3GPP-specified simulations*: The performance of the SKG scheme is evaluated under various conditions (e.g., different transmit power and user speed) through 3GPP specification-based simulations and the randomness is verified by the National Institute of Standards and Technology (NIST) test suite.

The rest of the paper is organized as follows. In Section II, the system and attacker models are given, followed by introductions of the SKG protocol, transceiver HWIs, and key performance indicators. The 3-step SIC scheme is introduced in Section III, and the RSI is formulated accordingly. Then, the probing phase is detailed in Section IV, and the probing errors are derived. Based on the probing errors, the SKC for IBFD and HD probing is derived in Section V, followed by the asymptotic behavior and IBFD gain analysis. A practical SKG processing scheme is given in Section VI to describe the details of generating the key from the observations. In Section VII, numerical results are shown to verify the analysis and the effectiveness of the proposed SKG scheme. Finally, conclusions are drawn in Section VIII.

Notations: $\mathcal{A}$, $\mathbf{A}$, $\mathbf{a}$, and a represent an alphabet set, a matrix, a vector, and a scalar, respectively. $Cov(\mathbf{A})$, vec $(\mathbf{A})$, $|\mathbf{A}|$, $\mathbf{A}^{\dagger}$, $\mathbf{A}^{T}$, $\mathbf{A}^{*}$, and $\mathbf{A}^{-1}$ denote the covariance matrix, column-wise vectorization, determinant, Hermitian transpose, transpose, complex conjugate, and inverse of the matrix $\mathbf{A}$.

$\mathcal{D}(\mathbf{A})$ denotes a diagonal matrix containing the elements along the diagonal of $\mathbf{A}$. $\mathbf{I}$ represents an identity matrix. $I(A;B)$ denotes the mutual information between A and B, and $H(A)$ is the entropy of A. $\mathbb{E}\{\cdot\}$ denotes the expectation operation, and $\lfloor\cdot\rfloor$ denotes the floor operation. $\mathcal{CN}(0,\sigma^2)$ denotes a complex normal distribution with zero mean and variance of σ^2. $\mathcal{R}(\cdot)$ and $\mathcal{I}(\cdot)$ represent the real and imaginary parts of the complex number. $\max[\cdot]$ and $\min[\cdot]$ denote the maximum and minimum element of the set, respectively. In addition, some important and similar symbols are listed in Table II in Appendix A to help with reading.

II. Preliminaries

We consider an OFDM-MIMO single-eavesdropper system where two legitimate users (i.e., Alice and Bob) communicate in the presence of a passive eavesdropper (i.e., Eve), as depicted in Fig. 1. Alice and Bob are equipped with N_A and N_B transmitting (Tx) and receiving (Rx) antennas, respectively. We consider half-wavelength antenna arrays so that the entries of the MIMO channel matrix are independent of each other [19]. We assume that there is a noiseless public channel among the nodes to send the reconciliation information, which is usually assumed in the related literature [2].

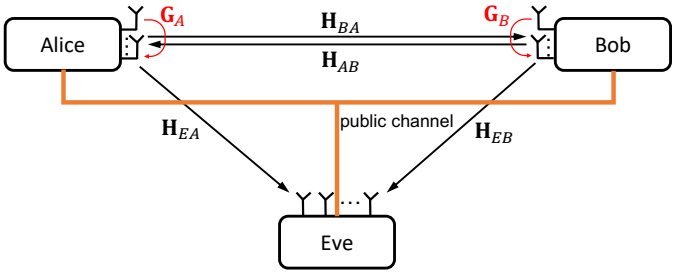


Fig. 1. An OFDM-MIMO single-eavesdropper system.

A. Attacker Model

In this paper, we consider a powerful passive attacker, Eve, who infers the secret key by eavesdropping on legitimate users' transmissions. Eve has access to the public channel and knows the communication protocols between legitimate users. In addition, Eve may have high-quality receivers (e.g., with a large dynamic range, high sampling rate, etc.) to capture the probing signal and acquire accurate estimates of the eavesdropping channel. Eve may have powerful storage and computational ability to perform advanced signal processing. Eve could be located anywhere, which means she may be located near legitimate users to experience highly-correlated fading with them. We assume Eve is located near Bob and infer the common randomness for key generation from the probing signal sent by Alice. This assumption does not lose the generality since we can always regard the party that is eavesdropped on as Bob. This attacker model is widely used in related studies [5], [10], [18].

B. SKG Protocol

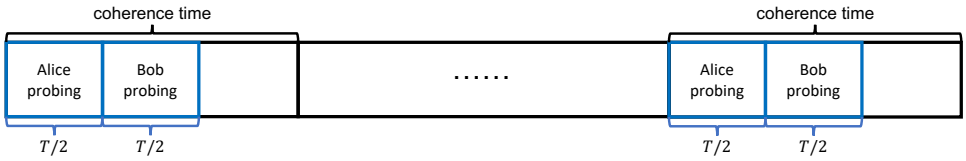
A typical secret key generation protocol consists of four phases: channel probing, quantization, information reconciliation, and privacy amplification. Legitimate users send probing signals to each other and measure the wireless channel between them (i.e., $\mathbf{H}_{AB}$ and $\mathbf{H}_{BA}$) at first. The probing interval is larger than the coherence time of the wireless channel; otherwise, the observations will be highly correlated, compromising the randomness of the key [8]. The probing can be performed in HD or IBFD mode as depicted in Fig. 2. Simultaneous measurements are challenging due to the transmission interval in HD mode, while non-simultaneous measurements could compromise the reciprocity. Besides, only half of the time resources can be utilized for one-direction probing in HD. In contrast, IBFD transceivers can enable simultaneous measurements and utilize more time-frequency resources for probing with the price of SIC overheads. The rest processing is the same for IBFD and HD systems. Legitimate users harness the common randomness from the measured channels to generate the secret key by quantizers, e.g., threshold-based quantizers [20], or bidirectional difference quantizers [2]. The bit sequences generated independently by legitimate users may not be identical due to flawed reciprocity caused by practical imperfections such as asymmetric transceiver HWIs, half-duplex probing interval, and noise. To eliminate the inconsistencies and achieve key agreement, information reconciliation will be employed by exchanging a message over a public channel. Reconciliation may leak information about the key and compromise security. Thus, privacy amplification is usually utilized to remove the leaked information by leveraging a one-way mapping function, e.g., Hash function [10].

C. Transceiver Imperfections

Practical transceivers have limited dynamic range, introducing hardware impairments (HWIs) to the transmitted and received signals. The limited dynamic range is a natural consequence of imperfect digital-to-analog converters (DACs), analog-to-digital converters (ADCs), oscillators, and power amplifiers (PAs). Experimental measurements demonstrate that the transceiver HWIs are independent of the transmitted or received signals, and a circular complex Gaussian model can closely approximate the combined effects of these non-ideal components. Let $\sigma_t^2 \ll 1$ and $\sigma_r^2 \ll 1$ characterize the dynamic range of transmitters and receivers, respectively, and the transceiver distortions can be described by a zero-mean Gaussian model with the variance of σ_t^2 times the power of the intended transmit signals (or σ_r^2 times the power of the received signals) on that antenna. Assume $\mathbf{X}_i \in \mathbb{C}^{N_t\times 1}$ denote the transmitted symbols on the N_t transmitting antennas and $\mathbf{Y}_j \in \mathbb{C}^{N_r\times 1}$ denote the received symbols on the N_r receiving antennas, then the associated transmitter and receiver HWIs are modeled as

$$\begin{aligned}\mathbf{\Phi}_i &\sim \mathcal{CN}\left(\mathbf{0}, \sigma_t^2\mathcal{D}\left(\mathbf{X}_i\mathbf{X}_i^\dagger\right)\right),\\ \mathbf{\Psi}_j &\sim \mathcal{CN}\left(\mathbf{0}, \sigma_r^2\mathcal{D}\left(\mathbf{Y}_j\mathbf{Y}_j^\dagger\right)\right),\end{aligned} \tag{1}$$

where $i \in \{A,B\}$ and $j \in \{B,A\}$ denote a pair of legitimate users, i.e., $i=A, j=B$ or $i=B, j=A$, throughout this paper. The values of σ_t^2 and σ_r^2 are related to the measurable



(a) Half-duplex mode.

(b) In-band Full-duplex mode.

Fig. 2. Channel probing in IBFD mode and HD mode.

error vector magnitudes (EVMs) of RF transceivers. The HWIs model utilized is a verified model based on experiments and has been adopted by many studies in the field of wireless communications (see [9], [21], [22] and references therein).

In addition to the HWIs, receivers have additive white Gaussian noise (AWGN) that are described as $\mathbf{W}_i \sim \mathcal{CN}\left(\mathbf{0}, \sigma_{w,i}^2 \mathbf{I}\right)$, where $\sigma_{w,i}^2$ is the thermal noise power.

D. Key Performance Indicators

The generated key is used to encrypt the signals for secure communications, which have specific randomness, consistency, and refresh rate requirements. Thus, we use the following three metrics to evaluate the performance of a practical SKG protocol, which are commonly utilized in the literature [1], [6], [8], [10], [12].

1) Key generation rate: The KGR, which is the number of bits generated per second, measures the efficiency of the SKG protocol. A high KGR indicates that the protocol has high efficiency and is desired for the real-time SKG process. KGR can be described as

$$KGR = \frac{N_b}{\Delta_\tau}, \tag{2}$$

where Δ_τ is the interval between two probing rounds, and N_b is the averaged number of generated bits per probing round.

2) Key disagreement rate: The KDR is the mismatch rate between the binary key bit sequences generated by Alice and Bob, which describes the robustness of the SKG protocol. Low KDR indicates that the protocol is robust and requires fewer resources for reconciliation. The KDR has to be within the correction capacity of reconciliation to eliminate the inconsistencies between the two keys. Let $\mathcal{K}_A$ and $\mathcal{K}_B$ denote the key generated by Alice and Bob containing L_K binary bits, and the KDR can be denoted as

$$KDR = \frac{1}{L_K} \sum_{l=1}^{L_K} \left| \mathcal{K}_A(l) - \mathcal{K}_B(l) \right|. \tag{3}$$

3) Randomness: The randomness of the generated key is the most important metric for a practical SKG protocol since the key should be unpredictable to ensure the security level. Randomness could be verified by the statistical test suite provided by National Institute of Standards and Technology (NIST). The test suite consists of 15 statistical tests, which focus on different randomness features. The tests are formulated to test the null hypothesis that the sequence being tested is random. Each test calculates a P-value based on a calculated test statistic value. We refer to [23] for a detailed description of the test suite. The P-value summarizes the strength of the evidence against the null hypothesis that a larger P-value indicates better randomness. 0.01 is usually used as a significance level, which means the null hypothesis is accepted (i.e., the tested sequence is considered random) if P-value$\geq$ 0.01. The entropy of the key is also used as a performance metric in some studies (e.g., [1]). However, the Monobit test can evaluate the entropy of a binary bit sequence since they are both determined by the proportion of zeros and ones of the entire sequence. A larger P-value calculated under the Monobit test indicates higher entropy of the key. Therefore, we do not calculate the entropy in this paper.

III. Self-Interference Cancellation

Studies expose SI as the key issue of the practical implementation of IBFD. The SI could be 100dB higher than the probing signals from the other legitimate user due to the proximity of the transmitter and receiver so that communication parties cannot harness the common randomness. Recent studies propose various SIC techniques and demonstrate the feasibility of efficient IBFD radios (see [22], [24]–[26] and references therein). We employ a conventional 3-step method to minimize the effects of SI, which consists of passive antenna isolation, RF cancellation, and digital cancellation. These existing SIC technologies are not the novel contributions of this paper, while we derive the corresponding RSI strength with measurable metrics in this paper, revealing their effects on the key performance from the practical perspective.

We assume that a probing spans over T OFDM symbols within the coherence time of wireless channels, and SIC needs αT symbols of overheads, where $0 \leqslant \alpha \leqslant 1$. During the SIC phase, Alice and Bob will work in TDD mode to have an accurate estimate of the SI channel and tune the parameters of cancellers. Alice and Bob send orthogonal pilot signals $\mathbf{X}_A^{FD,0}[k] \in \mathbb{C}^{N_A \times \frac{\alpha T}{2}}$ and $\mathbf{X}_B^{FD,0}[k] \in \mathbb{C}^{N_B \times \frac{\alpha T}{2}}, \forall k \in [1, K]$

$$\hat{\mathbf{G}}_i[k] = \tilde{\mathbf{Y}}_i^{FD,0}[k] \left(\mathbf{X}_i^{FD,0}[k]\right)^{\dagger} \left(\mathbf{R}_{GG,i}\mathbf{X}_i^{FD,0}[k] \left(\mathbf{X}_i^{FD,0}[k]\right)^{\dagger} + N_i\sigma_{n,i,0}^2\mathbf{I}\right)^{-1} \mathbf{R}_{GG,i} = \tilde{\mathbf{G}}_i[k] - \boldsymbol{\Delta}_i[k] \tag{4}$$

during the first and last $\frac{\alpha T}{2}$ OFDM symbols, respectively. Assume the transmit power is P_A and P_B per OFDM symbol, the entries of $\mathbf{X}_A^{FD,0}[k]$ and $\mathbf{X}_B^{FD,0}[k]$ are independent and identically distributed (i.i.d.) to complex Gaussian distribution with zero mean and variance of $\frac{P_A}{N_A}$ and $\frac{P_B}{N_B}$, respectively.

A. Passive Antenna Isolation

The passive approach mainly focuses on minimizing the direct path component and is agnostic to the surrounding environment. A high-isolation antenna design is reported in [27], which provides 65-70 dB of direct path isolation. Theoretically, the passive isolation is frequency-independent, although it could have minor performance differences in different frequency bands due to imperfect hardware conditions. Thus, the effects of passive antenna isolation can be reflected in the pathloss of the direct path. For instance, the pathloss of the direct path is increased by 20dB if there is 20dB of passive antenna isolation applied. The passive antenna isolation does not require additional operation and is valid as long as the antenna configuration is placed. The antenna design is out of the scope of this paper, so we assume the direct path of the SI channel is attenuated to reflect the effects of passive antenna isolation, while we do not restrict technologies to achieve it nor the realized suppression depth.

B. RF Cancellation

Due to the presence of multiple reflection paths, passive antenna isolation cannot solely suppress the SI to be within the dynamic range of receivers, especially in a rich multipath environment. To deal with the reflection components, a multi-tap canceller is utilized. Such a canceller consists of multiple tuneable delay lines, where the delay lines have different lengths to cause delays uniformly distributed within the delay spread of the SI channel. The amplitude and phase of each delay line could be adjusted to match the SI channel so that the canceller can generate a replica of the received SI to cancel it out. The canceller can be tuned in the frequency or time domain, and the achievable cancellation depth depends on the number of tuneable delay lines of the canceller with a specific SI channel condition. Recent studies explore optical components to construct the delay lines, which can provide a large number of true delay lines and operational bandwidth to achieve effective RF cancellation for beyond 5G networks [25], [28]. The parameters of the RF canceller (i.e., phases and weights of delay lines) are tuned during the first αT symbols duration. Then it can mitigate the SI during the rest time of a coherence time period since the parameters are determined by the SI channel condition while they are independent of the transmitted symbols. We assume ϑ_i dB of analog self-interference cancellation (ASIC) depth is realized by the RF canceller at node i, which the strength of SI channel is reduced by ϑ_i dB and it is frequency-independent (i.e., ϑ_i is identical for all subcarriers k). The readers are referred to our previous work in [25] for details of implementing the multi-tap canceller.

C. Digital Cancellation

A digital canceller could effectively suppress the RSI after the ADCs as long as the RSI is within the dynamic range of receivers. We use a minimum mean-squared error-based digital canceller, which estimates the effective SI channel and reconstructs the RSI in the frequency domain. After the RF cancellation, the received RSI signal at the legitimate user i can be given as

$$\begin{aligned}\tilde{\mathbf{Y}}_i^{FD,0}[k] &= \tilde{\mathbf{G}}_i[k]\left(\mathbf{X}_i^{FD,0}[k] + \boldsymbol{\Phi}_i^{FD,0}[k]\right) \\ &\quad + \mathbf{D}_i^{FD,0}[k] + \mathbf{W}_i^{FD,0}[k] + \boldsymbol{\Psi}_i^{FD,0}[k], \\ &= \tilde{\mathbf{G}}_i[k]\mathbf{X}_i^{FD,0}[k] + \mathbf{N}_{i,0}^{FD,0}[k],\end{aligned} \tag{5}$$

where $\bar{\mathbf{G}}_i[k] \in \mathbb{C}^{N_i \times N_i}$ denotes the effective SI channel with the passive antenna isolation effects (i.e., the direct path is attenuated); $\tilde{\mathbf{G}}_i[k] = \eta_i\bar{\mathbf{G}}_i[k]$ denotes the effective SI channel after the RF cancellation with $\eta_i = 10^{-\frac{\vartheta_i}{10}}$; $\mathbf{D}_i[k]$ represents the noise and distortions induced by RF cancellers. The noise and distortions of RF cancellers can also be described by the circular complex Gaussian model as in Section II-C since it is composed of similar phase noise and nonlinearities. Let $\sigma_{d,i}^2$ describe the power of the canceller noise, then the entries of $\mathbf{D}_i[k]$ are i.i.d. to complex Gaussian distribution with zero mean and variance of $\sigma_{d,i}^2$. Legitimate users estimate the effective SI channel $\tilde{\mathbf{G}}_i[k]$ form the persevered RSI $\tilde{\mathbf{Y}}_i^{FD,0}[k]$ during the SIC phase. The effective SI channel remains unchanged during the same coherence time, so legitimate users are able to generate a replica of the RSI during the IBFD probing phase and cancel the received RSI out. The MMSE channel estimator is utilized to estimate the effective SI channel in this paper. The noise for channel estimation is given as $\mathbf{N}_{i,0}^{FD,0}[k] = \tilde{\mathbf{G}}_i[k]\boldsymbol{\Phi}_i^{FD,0}[k] + \mathbf{D}_i^{FD,0}[k] + \mathbf{W}_i^{FD,0}[k] + \boldsymbol{\Psi}_i^{FD,0}[k]$. Assume the transmitted signals are uncorrelated with the noise, we have the entries of $\mathbf{N}_{i,0}^{FD,0}[k]$ i.i.d. to complex Gaussian distribution with zero mean and variance of $\sigma_{n,i,0}^2 = \sigma_t^2 P_i\eta_i\varrho_i + \sigma_{d,i}^2 + \sigma_{w,i}^2 + \sigma_r^2[(1+\sigma_t^2)P_i\eta_i\varrho_i + \sigma_{d,i}^2]$. According to Appendix B, the estimate of the effective SI channel can be denoted as Equation (4), where $\mathbf{R}_{GG,i} = \mathbb{E}\left\{\left(\tilde{\mathbf{G}}_i[k]\right)^{\dagger}\tilde{\mathbf{G}}_i[k]\right\}$ and $\boldsymbol{\Delta}_i[k]$ has i.i.d zero-mean complex Gaussian elements with variance of $\sigma_{\Delta,i,0}^2 = \frac{\sigma_{n,i,0}^2}{\frac{\alpha T P_i}{2N_i} + \frac{\sigma_{n,i,0}^2}{\eta_i\varrho_i}}$. To have an appropriate estimation, we should have

$$\frac{\alpha T}{2} \geqslant \max\{N_A, N_B\}, \tag{6}$$

as stated in Appendix B.

$$\hat{\mathbf{H}}_{AB}^{HD}[k] = \mathbf{Y}_{A}^{HD}[k]\left(\mathbf{X}_{B}^{HD}[k]\right)^{\dagger}\left(\mathbf{R}_{HH,\tau_1}\mathbf{X}_{B}^{HD}[k]\left(\mathbf{X}_{B}^{HD}[k]\right)^{\dagger} + N_A\sigma_{n,A}^2\mathbf{I}\right)^{-1}\mathbf{R}_{HH,\tau_1} = \mathbf{H}_{AB}^{(\tau_2)}[k] + \mathbf{\Delta}_{AB}^{HD}[k] \tag{9}$$

$$\hat{\mathbf{H}}_{BA}^{HD}[k] = \mathbf{Y}_{B}^{HD}[k]\left(\mathbf{X}_{A}^{HD}[k]\right)^{\dagger}\left(\mathbf{R}_{HH,\tau_2}\mathbf{X}_{A}^{HD}[k]\left(\mathbf{X}_{A}^{HD}[k]\right)^{\dagger} + N_B\sigma_{n,B}^2\mathbf{I}\right)^{-1}\mathbf{R}_{HH,\tau_2} = \mathbf{H}_{BA}^{(\tau_1)}[k] + \mathbf{\Delta}_{BA}^{HD}[k] \tag{10}$$

IV. Channel Probing

The key performance of the CFR-based SKG scheme strongly depends on channel estimation accuracy. We assume wireless channel reciprocity and all time-frequency resources can be used for probing, i.e., ignore the interpolation error, then we formulate the probing errors in this section.

A. Half-duplex Probing

Alice and Bob send orthogonal probing signals $\mathbf{X}_{A}^{HD}[k] \in \mathbb{C}^{N_A\times\frac{T}{2}}$ and $\mathbf{X}_{B}^{HD}[k] \in \mathbb{C}^{N_B\times\frac{T}{2}}$, $\forall k \in [1,K]$ during the first and last $\frac{T}{2}$ OFDM symbols (i.e., τ_1 and τ_2), respectively. Let $\mathbf{H}_{BA}^{(\tau_1)}[k]$ denote the wireless channel from Alice to Bob over the period of the first $\frac{T}{2}$ OFDM symbols duration and $\mathbf{H}_{AB}^{(\tau_2)}[k]$ denote the wireless channel from Bob to Alice over the period of the last $\frac{T}{2}$ OFDM symbols duration. The signals received by Alice and Bob are denoted as

$$\begin{aligned}\mathbf{Y}_{A}^{HD}[k] &= \mathbf{H}_{AB}^{(\tau_2)}[k]\left(\mathbf{X}_{B}^{HD}[k] + \mathbf{\Phi}_{B}^{HD}[k]\right) \\ &\quad + \mathbf{W}_{A}^{HD}[k] + \mathbf{\Psi}_{A}^{HD}[k] \\ &= \mathbf{H}_{AB}^{(\tau_2)}[k]\mathbf{X}_{B}^{HD}[k] + \mathbf{N}_{A}^{HD}[k],\end{aligned} \tag{7}$$

$$\begin{aligned}\mathbf{Y}_{B}^{HD}[k] &= \mathbf{H}_{BA}^{(\tau_1)}[k]\left(\mathbf{X}_{A}^{HD}[k] + \mathbf{\Phi}_{A}^{HD}[k]\right) \\ &\quad + \mathbf{W}_{B}^{HD}[k] + \mathbf{\Psi}_{B}^{HD}[k] \\ &= \mathbf{H}_{BA}^{(\tau_1)}[k]\mathbf{X}_{A}^{HD}[k] + \mathbf{N}_{B}^{HD}[k],\end{aligned} \tag{8}$$

where $\mathbf{N}_{A}^{HD}[k] = \mathbf{H}_{AB}^{(\tau_2)}[k]\mathbf{\Phi}_{B}^{HD}[k] + \mathbf{W}_{A}^{HD}[k] + \mathbf{\Psi}_{A}^{HD}[k]$ and $\mathbf{N}_{B}^{HD}[k] = \mathbf{H}_{BA}^{(\tau_1)}[k]\mathbf{\Phi}_{A}^{HD}[k] + \mathbf{W}_{B}^{HD}[k] + \mathbf{\Psi}_{B}^{HD}[k]$ denote the noise for channel estimation during HD probing. The noise matrix has i.i.d zero-mean complex Gaussian elements with variance of $\sigma_{n,i}^2 = (\sigma_r^2 + \sigma_t^2 + \sigma_r^2\sigma_t^2)P_j\varrho_{ij} + \sigma_{w,i}^2$. With the known transmitted probing signals, Alice and Bob can acquire the estimate of the wireless channel as Equations (9) and (10), where $\mathbf{R}_{HH,\tau_1} = \mathbb{E}\left\{\left(\mathbf{H}_{BA}^{(\tau_1)}[k]\right)^{\dagger}\mathbf{H}_{BA}^{(\tau_1)}[k]\right\}$ and $\mathbf{R}_{HH,\tau_2} = \mathbb{E}\left\{\left(\mathbf{H}_{AB}^{(\tau_2)}[k]\right)^{\dagger}\mathbf{H}_{AB}^{(\tau_2)}[k]\right\}$; $\mathbf{\Delta}_{AB}^{HD}[k]$ has i.i.d zero-mean complex Gaussian elements with variance of $\sigma_{\Delta,A}^2 = \frac{\sigma_{n,A}^2}{\frac{TP_B}{2N_B} + \frac{\sigma_{n,A}^2}{\varrho_{AB}}}$; $\mathbf{\Delta}_{BA}^{HD}[k]$ has i.i.d zero-mean complex Gaussian elements with variance of $\sigma_{\Delta,B}^2 = \frac{\sigma_{n,B}^2}{\frac{TP_A}{2N_A} + \frac{\sigma_{n,B}^2}{\varrho_{AB}}}$. To have an appropriate estimation, we should have

$$\frac{T}{2} \geqslant \max\{N_A, N_B\}. \tag{11}$$

Due to the temporal changes of the environment during the transmission interval in HD mode [3], the wireless channel may not be identical during the probing period τ_1 and τ_2, i.e., $\mathbf{H}_{AB}^{(\tau_1)}$ and $\mathbf{H}_{AB}^{(\tau_2)}$ are not identical but highly correlated, where $\mathbf{H}_{AB}^{(\tau_1)}[k]$ denotes the wireless channel from Bob to Alice during period τ_1. $\mathbf{H}_{AB}^{(\tau_1)}[k]$ is reciprocal to $\mathbf{H}_{BA}^{(\tau_1)}[k]$ such that $\mathbf{H}_{BA}^{(\tau_1)}[k] = \left(\mathbf{H}_{AB}^{(\tau_1)}[k]\right)^{T}$ due to the wireless channel reciprocity, so Equation (10) can be written as

$$\hat{\mathbf{H}}_{BA}^{HD}[k] = \left(\mathbf{H}_{AB}^{(\tau_1)}[k]\right)^{T} + \mathbf{\Delta}_{BA}^{HD}[k]. \tag{12}$$

B. In-band Full-duplex Probing

During the IBFD probing phase, Alice and Bob simultaneously send orthogonal probing signals $\mathbf{X}_{A}^{FD,1}[k] \in \mathbb{C}^{N_A\times(1-\alpha)T}$ and $\mathbf{X}_{B}^{FD,1}[k] \in \mathbb{C}^{N_B\times(1-\alpha)T}$, $\forall k \in [1,K]$ within the last $(1-\alpha)T$ OFDM symbols. With the estimate of the effective SI channel $\hat{\mathbf{G}}_i[k]$ obtained from the SIC overheads, legitimate users are able to generate $\hat{\mathbf{G}}_i[k]\mathbf{X}_{i}^{FD,1}[k]$ to cancel out the received RSI, which is given as $\tilde{\mathbf{G}}_i[k]\left(\mathbf{X}_{i}^{FD,1}[k] + \mathbf{\Phi}_{i}^{FD,1}[k]\right) + \mathbf{D}_{i}^{FD,1}[k]$. Due to the imperfect estimate of effective SI channel and additional noise from RF cancellers, there will be residual effects of SI after digital cancellation denoted as

$$\mathbf{\Omega}_{i}^{FD,1}[k] = \tilde{\mathbf{G}}_i[k]\mathbf{\Phi}_{i}^{FD,1}[k] + \mathbf{\Delta}_i\mathbf{X}_{i}^{FD,1}[k] + \mathbf{D}_{i}^{FD,1}[k]. \tag{13}$$

The entries of $\mathbf{\Omega}_{i}^{FD,1}[k]$ are i.i.d. to complex Gaussian distribution with zero mean and variance of $\sigma_{s,i,0}^2 = \sigma_t^2P_i\eta_i\varrho_i + \sigma_{\Delta,i,0}^2P_i + \sigma_{d,i}^2$. With SIC applied, the received signals at legitimate users during the IBFD probing phase can be denoted as (the superscript for the time period of the channel matrix is omitted here since legitimate users send the probing signals simultaneously)

$$\begin{aligned}\mathbf{Y}_{i}^{FD,1}[k] &= \mathbf{H}_{ij}[k]\left(\mathbf{X}_{j}^{FD,1}[k] + \mathbf{\Phi}_{j}^{FD,1}[k]\right) \\ &\quad + \mathbf{\Omega}_{i}^{FD,1}[k] + \mathbf{W}_{i}^{FD,1}[k] + \mathbf{\Psi}_{i}^{FD,1}[k] \\ &= \mathbf{H}_{ij}[k]\mathbf{X}_{j}^{FD,1}[k] + \mathbf{N}_{i}^{FD,1}[k],\end{aligned} \tag{14}$$

where $\mathbf{N}_{i}^{FD,1}[k] = \mathbf{H}_{ij}[k]\mathbf{\Phi}_{j}^{FD,1}[k] + \mathbf{\Omega}_{i}^{FD,1}[k] + \mathbf{W}_{i}^{FD,1}[k] + \mathbf{\Psi}_{i}^{FD,1}[k]$ denotes the noise for channel estimation during the IBFD probing and it has i.i.d zero-mean complex Gaussian elements with variance of $\sigma_{n,i,1}^2 = (1+\sigma_r^2)\left(\sigma_t^2P_j\varrho_{ij} + \sigma_{s,i,0}^2\right) + \sigma_r^2P_j\varrho_{ij} + \sigma_{w,i}^2$. With the known transmitted probing signals, Alice and Bob can estimate the channel similarly to Equations (9) and (10), yielding the estimates with errors as

$$\hat{\mathbf{H}}_{AB}^{FD}[k] = \mathbf{H}_{AB}[k] + \mathbf{\Delta}_{AB}^{FD}[k], \tag{15}$$

$$\hat{\mathbf{H}}_{BA}^{FD}[k] = \mathbf{H}_{BA}[k] + \mathbf{\Delta}_{BA}^{FD}[k], \tag{16}$$

where the entries of $\mathbf{\Delta}_{AB}^{FD}[k]$ and $\mathbf{\Delta}_{BA}^{FD}[k]$ are i.i.d to complex Gaussian distribution with zero mean and variance of $\sigma_{\Delta,A,1}^2 = \frac{\sigma_{n,A,1}^2}{\frac{(1-\alpha)TP_B}{N_B} + \frac{\sigma_{n,A,1}^2}{\varrho_{AB}}}$ and $\sigma_{\Delta,B,1}^2 = \frac{\sigma_{n,B,1}^2}{\frac{(1-\alpha)TP_A}{N_A} + \frac{\sigma_{n,B,1}^2}{\varrho_{AB}}}$,

respectively. To have an appropriate estimation, we should have

$$(1-\alpha)T \geqslant \max\{N_A, N_B\}. \tag{17}$$

For IBFD probing, we have $\mathbf{H}_{AB}[k] = (\mathbf{H}_{BA}[k])^T$ due to the reciprocity, so Equation (16) can be written as

$$\hat{\mathbf{H}}_{BA}^{FD}[k] = (\mathbf{H}_{AB}[k])^T + \mathbf{\Delta}_{BA}^{FD}[k]. \tag{18}$$

V. Secret Key Capacity

Secret key capacity (SKC) is the maximum key generation rate at which the secret key can be generated reliably, securely, and uniformly [11]. As stated in the attacker model, we consider an eavesdropper with high-quality hardware and powerful computation ability. Thus, we assume Eve acquires the eavesdropping channel with trivial errors that can be ignored. Since Eve can be located anywhere, there are two cases: 1) Eve is very close to the legitimate user (we assume it is Bob) so that the eavesdropping and legitimate channels are correlated; 2) Eve is far away from any of the legitimate users and experiences independent fading. We will derive the SKC for both cases in this section.

A. Correlated Eavesdropping Channel

When Eve is very close to Bob, she will experience correlated fading as Bob. We do not consider how Eve processes her observations since this is not our concern, while we assume Eve can extract a channel matrix correlated with $\mathbf{H}_{BA}^{\epsilon}$ from the correlated observations, which can be modeled as [7]

$$\hat{\mathbf{H}}_{EA}^{\epsilon} = \rho' \mathbf{H}_{BA}^{\epsilon} + \mathbf{\Lambda}_{BA}^{\epsilon}, \tag{19}$$

where $[\mathbf{\Lambda}_{BA}^{\epsilon}]_{k,l} \sim \mathcal{CN}\left(0, (1-\rho'^2)\varrho_{AB}\right) \quad \forall \quad k,l;\ \epsilon \in \{HD, FD\}$ denotes the probing mode. The SKC is determined by the conditional mutual information given the column-wise vectorization of the measured CFRs (i.e., $\mathbf{h}_i^{\epsilon} = \text{vec}\left(\hat{\mathbf{H}}_{ij}^{\epsilon}[k]\right)$), expressed as

$$C_k^{\epsilon} = I\left(\mathbf{h}_A^{\epsilon}; \mathbf{h}_B^{\epsilon} | \mathbf{h}_E^{\epsilon}\right). \tag{20}$$

Lemma 1. *The closed-form expressions of SKC for HD and IBFD probing are given as Equations* (24) *and* (25) *on the top of next page, where* $\varpi_i^{HD} = \varrho_{AB} + \sigma_{\Delta,i}^2$ *and* $\varpi_i^{FD} = \varrho_{AB} + \sigma_{\Delta,i,1}^2$.

Proof. See Appendix C. □

The expressions clearly illustrate the gain of MIMO systems that both the Tx and Rx antenna arrays can increase the SKC proportionally. The SKC is subjected to the probing errors ($\sigma_{\Delta,i}^2$ or $\sigma_{\Delta,i,1}^2$), the correlation between consecutive CFRs (ρ), and the correlation between the eavesdropping and legitimate channels (ρ'). In addition, the SIC overheads (α), probing duration (T), transmit power (P_A and P_B), noise and distortions, and antenna array size (N_A and N_b) will affect the SKC by affecting the probing errors.

B. Independent Eavesdropping Channel

Eve will experience independent fading from legitimate users if she is located half a wavelength away from them, which is known as the spatial independence assumption. This assumption is stated and considered in many related studies, such as in [5], [18]. Let $\mathbf{Y}_E^{\epsilon}[k]$ denote Eve's observation, which is expressed as

$$\begin{aligned}\mathbf{Y}_E^{\epsilon}[k] = {} & \phi_{EA}\mathbf{H}_{EA}[k]\left(\mathbf{X}_A^{\epsilon}[k] + \mathbf{\Phi}_A^{\epsilon}[k]\right) \\ & + \phi_{EB}\mathbf{H}_{EB}[k]\left(\mathbf{X}_B^{\epsilon}[k] + \mathbf{\Phi}_B^{\epsilon}[k]\right) \\ & + \mathbf{W}_E^{\epsilon}[k] + \mathbf{\Psi}_E^{\epsilon}[k],\end{aligned} \tag{21}$$

where $\phi_{EA}, \phi_{EB} \in \{0,1\}$ depends on the probing mode and phase, e.g., $\phi_{EA} = 1$ and $\phi_{EB} = 1$ during the IBFD probing phase. Based on the spatial independence assumption that the $\mathbf{H}_{EA}$ and $\mathbf{H}_{EB}$ are independent of $\mathbf{H}_{AB}$ and $\mathbf{H}_{BA}$), Eve cannot extract a correlated CFR from her observations since none of the terms in (21) is correlated with the legitimate channel. In this case, the SKC is given as the mutual information given estimated legitimate CFRs.

Lemma 2. *The closed-form expressions of SKC for HD and IBFD probing under spatial independence assumption are given as Equations* (22) *and* (23)*, which are equivalent to substituting* $\rho' = 0$ *to Equations* (24) *and* (25)*.*

$$\begin{aligned}C_k^{HD} &= I\left(\mathbf{h}_A^{HD}; \mathbf{h}_B^{HD}\right) \\ &= N_A N_B \log_2\left(\frac{\varpi_A^{HD}\varpi_B^{HD}}{\varpi_A^{HD}\varpi_B^{HD} - \rho^2\varrho_{AB}^2}\right),\end{aligned} \tag{22}$$

$$\begin{aligned}C_k^{FD} &= I\left(\mathbf{h}_A^{FD}; \mathbf{h}_B^{FD}\right) \\ &= N_A N_B \log_2\left(\frac{\varpi_A^{FD}\varpi_B^{FD}}{\varpi_A^{FD}\varpi_B^{FD} - \varrho_{AB}^2}\right).\end{aligned} \tag{23}$$

Proof. See Appendix D. □

The expressions suggest that the SKC is mainly limited by the probing error (i.e., $\sigma_{\Delta,i}^2$ for HD and $\sigma_{\Delta,i,1}^2$ for IBFD) and the correlation coefficient (i.e., ρ) in this case. The SKC decreases with increasing probing errors and decreasing correction coefficients. The correlation coefficient is an inherent property of the wireless channel, which depends on the user's moving speed. The probing errors will be affected by many system parameters, as their expressions suggest.

C. Asymptotic Behavior Analysis

To investigate the fundamental limits on the performance of PHY-SKG, we derive the asymptotic SKC in the high-SNR regime, which can be obtained by tending the transmit power in Equations (22) and (23) to infinity. We only consider the case under the spatial independence assumption since we want to focus on its intrinsic limits rather than the eavesdropper's effect. The asymptotic SKC for HD probing is given as

$$C_k^{HD,asym} = N_A N_B \log_2\left(\frac{\bar{\varpi}_A^{HD}\bar{\varpi}_B^{HD}}{\bar{\varpi}_A^{HD}\bar{\varpi}_B^{HD} - \rho^2\varrho_{AB}^2}\right), \tag{26}$$

where $\bar{\varpi}_i^{HD} = \varrho_{ij} + \bar{\sigma}_{\Delta,i}^2$ with

$$\bar{\sigma}_{\Delta,i}^2 = \lim_{P_i \to \infty} \sigma_{\Delta,i}^2 = \varrho_{ij}\frac{1}{\frac{T\varrho_{ij}}{2N_j\Sigma_\sigma} + 1}, \tag{27}$$

$$C_k^{HD} = I\left(\mathbf{h}_A^{HD}; \mathbf{h}_B^{HD} \mid \mathbf{h}_E^{HD}\right) = N_A N_B \log_2\left(\frac{\varpi_A^{HD}\varpi_B^{HD} - \left(\varpi_A^{HD} + \varpi_B^{HD}\rho^2\right)\rho'^2\varrho_{AB} + \rho'^4\rho^2\varrho_{AB}^2}{\varpi_A^{HD}\varpi_B^{HD} - \left(\varpi_A^{HD} + \varpi_B^{HD}\rho^2\right)\rho'^2\varrho_{AB} + \left(2\rho'^2 - 1\right)\rho^2\varrho_{AB}^2}\right). \tag{24}$$

$$C_k^{FD} = I\left(\mathbf{h}_A^{FD}; \mathbf{h}_B^{FD} \mid \mathbf{h}_E^{FD}\right) = N_A N_B \log_2\left(\frac{\varpi_A^{FD}\varpi_B^{FD} - (\varpi_A^{FD} + \varpi_B^{FD})\rho'^2\varrho_{AB} + \rho'^4\varrho_{AB}^2}{\varpi_A^{FD}\varpi_B^{FD} - (\varpi_A^{FD} + \varpi_B^{FD})\rho'^2\varrho_{AB} + (2\rho'^2 - 1)\varrho_{AB}^2}\right). \tag{25}$$

where $\Sigma_\sigma = \sigma_t^2 + \sigma_r^2 + \sigma_t^2\sigma_r^2$. Similarly, we can derive the asymptotic SKC for IBFD probing. We first investigate the IBFD probing error in the high-SNR regime as

$$\begin{aligned}\bar{\sigma}_{\Delta,i,1}^2 &= \lim_{P_i,P_j\to\infty} \frac{\sigma_{n,i,1}^2}{\frac{(1-\alpha)TP_j}{N_j} + \frac{\sigma_{n,i,1}^2}{\varrho_{ij}}} \\ &= \lim_{P_i=P_j=P\to\infty} \frac{\frac{\partial\sigma_{n,i,1}^2}{\partial P}}{\frac{(1-\alpha)T}{N_j} + \frac{1}{\varrho_{ij}}\frac{\partial\sigma_{n,i,1}^2}{\partial P}},\end{aligned} \tag{28}$$

where $\sigma_{n,i,1}^2$ is detailed in Equation (35) on the top of next page. Thus, we will have

$$\begin{aligned}n_{FD}^{asym} &= \lim_{P\to\infty} \frac{\partial\sigma_{n,i,1}^2}{\partial P} \\ &= \Sigma_\sigma\varrho_{ij} + (1+\sigma_r^2)\left(\sigma_t^2\eta_i\varrho_i + \frac{2N_i\eta_i\varrho_i\Sigma_\sigma}{\alpha T + 2N_i\Sigma_\sigma}\right),\end{aligned} \tag{29}$$

Then, the asymptotic SKC for IBFD probing can be written as

$$C_k^{FD,asym} = N_A N_B \log_2\left(\frac{\bar{\varpi}_A^{FD}\bar{\varpi}_B^{FD}}{\bar{\varpi_A}^{FD}\bar{\varpi}_B^{FD} - \varrho_{AB}^2}\right), \tag{30}$$

where $\bar{\varpi}_i^{FD} = \varrho_{ij} + \bar{\sigma}_{\Delta,i,1}^2$ with $\bar{\sigma}_{\Delta,i,1}^2 = \varrho_{ij}\frac{1}{\frac{(1-\alpha)T\varrho_{ij}}{N_j n_{FD}^{asym}} + 1}$. The asymptotic results illustrate that there is an upper bound of the SKC, which is imposed by transceiver HWIs in HD systems. In IBFD systems, the limits are also imposed by the ASIC depth (which is reflected by η_i and ϱ_i) and SIC overheads (α) in addition to the transceiver HWIs.

D. Conditions for IBFD to Gain Benefits

To get practical insights, we explore the conditions under which IBFD probing can provide gains over its HD counterpart based on asymptotic behavior. We assume Alice and Bob have identical settings (i.e., identical hardware conditions, transmit power, etc.) for simplicity so that they will have identical probing errors. Let $P_A = P_B = P$, $N_A = N_B = N$, we can denote the probing errors for legitimate users in HD and IBFD mode as

$$\bar{\sigma}_{HD}^2 = \bar{\sigma}_{\Delta,i}^2 = \varrho_{AB}\frac{1}{\frac{T\varrho_{AB}}{2N\Sigma_\sigma} + 1}\ \forall\, i, \tag{31}$$

$$\bar{\sigma}_{FD}^2 = \bar{\sigma}_{\Delta,i}^2 = \varrho_{AB}\frac{1}{\frac{T\varrho_{AB}}{2Nn_{FD}^{asym}} + 1}\ \forall\, i. \tag{32}$$

By deriving from $C_k^{FD,asym} > C_k^{HD,asym}$, we will have the condition for IBFD to gain benefits over HD as

$$\rho\bar{\sigma}_{FD}^2 < h(1-\rho) + \bar{\sigma}_{HD}^2. \tag{33}$$

This suggests that IBFD could have a larger probing error but still achieve higher SKC than HD with $\rho < 1$. Consider the scenario that $\rho \to 1$, we will have this condition to be

$$n_{FD}^{asym} < 2(1-\alpha)\Sigma_\sigma, \tag{34}$$

which can be satisfied with appropriate SIC overheads (α) and ASIC depth (which is reflected by η_i and ϱ_i). It reveals that an appropriate SIC scheme (with sufficient ASIC depth and small SIC overheads) is the basis for IBFD to gain benefits. The minimum ASIC depth or the range of SIC overhead that IBFD outperforms HD can be easily calculated by Equation (34) under specific conditions.

VI. Secret Key Generation Scheme

For the CFR-based SKG scheme, one round of channel probing is performed within a coherence time period to guarantee the randomness of the generated key bits and the KGR. Within the n^{th} coherence time period, a set of measurements can be obtained at legitimate users, which consist of estimated CFR matrices over all subcarriers as $\mathcal{H}_{i,n}^{\epsilon} = \left\{\hat{\mathbf{H}}_{ij,n}^{\epsilon}[k]\right\}_{k=1}^{K}$. Then, these measurements are appropriately converted into bit sequences independently by Alice and Bob.

A. Pre-processing

The measured channel matrices on consecutive subcarriers are highly correlated, so directly quantizing the entries of these matrices will decrease the randomness of the generated bit sequences. Therefore, the measurements are pre-processed to enhance the key performance. A feasible solution is intermittently selecting the measured channel matrices for quantization with fixed subcarrier intervals. To fully utilize the channel information on each subcarrier, we alternatively average the measurements within the same subband, which can reduce the effects of estimation errors if the errors are independent on each subcarrier [2], [14]. Assume all the K measurements are divided into M blocks, and the $\lfloor\frac{K}{M}\rfloor$ measurements within the m^{th} block are averaged to obtain a single sample for quantization as (we assume $\frac{K}{M}$ is an integer for simplicity)

$$\hat{\mathbf{H}}_{ij,n,m}^{\epsilon} = \frac{K}{M}\sum_{k=1}^{\frac{K}{M}} \hat{\mathbf{H}}_{ij,n}^{\epsilon}[\frac{K(m-1)}{M} + k]. \tag{36}$$

$$\sigma_{n,i,1}^2 = (1+\sigma_r^2)\left(\sigma_t^2 P_j \varrho_{ij} + \sigma_t^2 P_i \eta_i \varrho_i + \frac{\sigma_t^2 P_i \eta_i \varrho_i + \sigma_{d,i}^2 + \sigma_{w,i}^2 + \sigma_r^2[(1+\sigma_t^2)P_i\eta_i\varrho_i + \sigma_{d,i}^2]}{\frac{\alpha T P_i}{2N_i} + \frac{\sigma_t^2 P_i \eta_i \varrho_i + \sigma_{d,i}^2 + \sigma_{w,i}^2 + \sigma_r^2[(1+\sigma_t^2)P_i\eta_i\varrho_i + \sigma_{d,i}^2]}{\eta_i \varrho_i}} P_i + \sigma_{d,i}^2\right) + \sigma_r^2 P_j \varrho_{ij} + \sigma_{w,i}^2 \tag{35}$$

To fully utilize these samples and maximize the KGR, we quantize both the real and imaginary parts of the complex entries of these matrices. Therefore, $\hat{\mathbf{H}}_{ij,n,m}^{\epsilon} \in \mathbb{C}^{N_i \times N_j}$ is converted into a vector $\mathbf{s}_{i,n,m} \in \mathbb{R}^{2N_A N_B \times 1}$ as

$$\mathbf{s}_{i,n,m} = \begin{bmatrix} \mathcal{R}\left\{\text{vec}\left(\hat{\mathbf{H}}_{ij,n,m}^{\epsilon}\right)\right\} \\ \mathcal{I}\left\{\text{vec}\left(\hat{\mathbf{H}}_{ij,n,m}^{\epsilon}\right)\right\} \end{bmatrix}. \tag{37}$$

At the end of the n^{th} coherence time period, a total of $L_s = 2MN_AN_B$ of real numbers are collected by Alice and Bob as

$$\mathcal{S}_i = \{\mathbf{s}_{i,n,m}\}_{m=1}^{M}. \tag{38}$$

The power of the CFR is identical on all subcarriers in an uncorrelated scattering environment [29], which means the samples are within the same range. Thus, it is not necessary to adjust the range of these samples to generate a uniformly-distributed key. The samples can be normalized by the pathloss ϱ_{AB}, and the scaling does not affect the distribution of samples nor the mutual information between the sample sets collected by legitimate users. Fig. 3 shows the distribution of processed samples to be quantized at Alice and Bob, which indicates that the samples are subjected to a zero-mean Gaussian distribution.

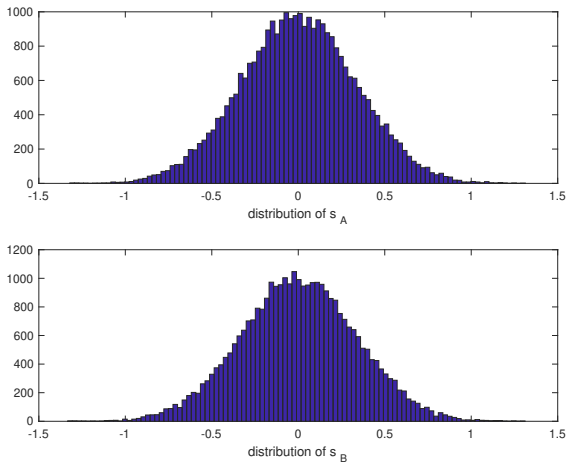


Fig. 3. Distribution of the collected samples.

B. Segmental Quantization

Quantization is employed to convert the processed samples $\mathcal{S}_A$ and $\mathcal{S}_B$ into binary bit sequences. The quantization schemes can be classified into lossy quantizers and lossless quantizers. Lossless quantizers utilize every sample to maximize the KGR, while lossy quantizers set guard strips to strike a tradeoff between the KGR and KDR. The readers are referred to [20] for more information about the quantizer design. We consider a single-bit lossy quantizer to minimize the KDR. To improve the randomness of the generated key bit sequence, we propose segmental quantization to remove the effects of large-scale fading and only quantize the small-scale fading. This is realized by dividing the sample sequence into multiple segments to be independently quantized. The thresholds are calculated according to the samples within different segments. Let $\mathbf{s}_{i,z}$ denote the z^{th} segments consisting of L_b samples at user i, it can be quantized to a binary bit sequence as

$$\mathbf{b}_{i,z} = \begin{cases} 1, \text{ if } \mathbf{s}_{i,z} > q_{+,i,z} \\ 0, \text{ if } \mathbf{s}_{i,z} < q_{-,i,z} \end{cases} \tag{39}$$

where $q_{+,i,z} = \mu_{i,z} + \gamma\sigma_{i,z}$ and $q_{-,i,z} = \mu_{i,z} - \gamma\sigma_{i,z}$ with $0 \leq \gamma \leq 1$ denote the upper and lower thresholds; $\mu_{i,z}$ and $\sigma_{i,z}^2$ are the mean and variance of the samples in $\mathbf{s}_{i,z}$. The range of $[q_{-,i,z}, q_{+,i,z}]$ is the guard strip that samples fall into the strip will be discarded with their indices recorded into $\mathcal{M}_i$. The key bit sequence can be obtained as $\mathcal{K}_i = \{\mathbf{b}_{i,1}, \mathbf{b}_{i,2}, \ldots, \mathbf{b}_{i,L_{k,i}}\}$. It is guaranteed to generate a uniformly-distributed key sequence due to the symmetry of the thresholds and the probability distribution function of Gaussian distribution as Fig. 3 shows.

C. Information Reconciliation and Privacy Amplification

The latter two steps serve as the complement and depend highly on the performance of the initial bit sequence. Off-the-shelf reconciliation and privacy amplification techniques can be employed to achieve a secure key agreement, so we do not pay particular attention to them. The readers are referred to [6], [30], [31] and references therein for a detailed description of the processing.

VII. Simulation Results

Our simulations follow 3GPP specifications. We consider an OFDM system with 15kHz of subcarrier spacing and normal cyclic prefix. $T = 14$ OFDM symbols (i.e., a subframe of 1ms) are utilized for probing, and the probing interval is 25ms if not specified. 4QAM is applied for the baseband modulation. A total of 4.5MHz bandwidth centered at 2.5GHz is utilized. The thermal noise density is -174dBm/Hz, and the noise figure is 9dB. The noise of RF cancellers is set to be identical to the thermal noise if not specified. 3GPP tapped delay line (TDL) models are utilized to construct the wireless MIMO channels based on a Matlab implementation. The "TDL-C" model is employed to construct the channel between legitimate users, and the "TDL-E" model with a K-factor of 22dB is used to construct the SI channel. The delay and power profile of these

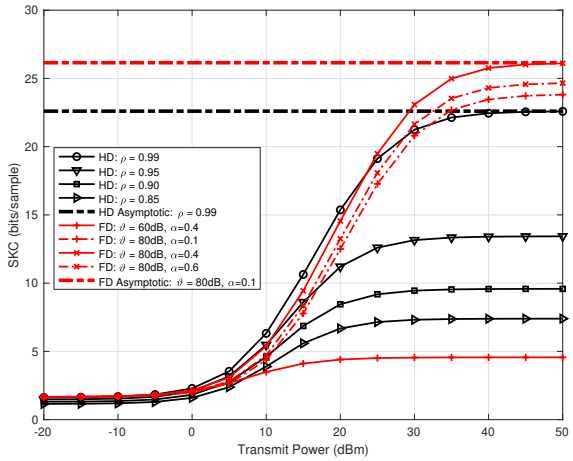


Fig. 4. SKC versus transmit power under various conditions for HD and IBFD probing.

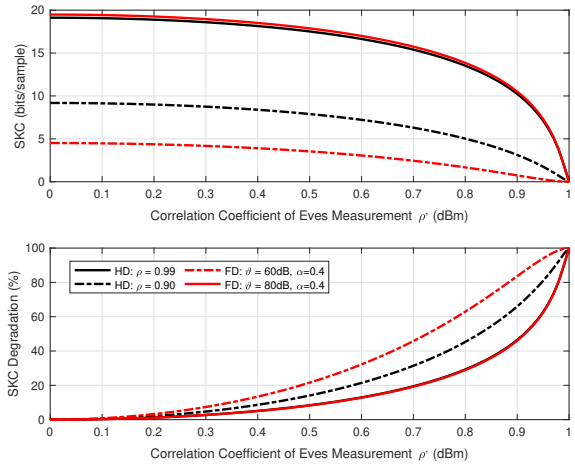


Fig. 5. SKC degradation due to correlated eavesdropping channel.

channels are given in Tables 7.7.2-3 and 7.7.2-5 in [32]. The MIMO correlation is set to be low to be consistent with the theoretical derivation. The pathloss of the SI channel is set to be 0dB, and the pathloss of the legitimate channel is calculated from the formulas given in Table 7.4.1-1 in [32]. Urban-macro (UMa) scenarios are considered for a typical open space and office environment, and the root-mean-square delay spread of 50ns is utilized for simulations [2]. The distance between legitimate users is 100m if not specified.

A. Secret Key Capacity

In this section, we explore the limits and affecting factors of the SKC based on the derivations. We set $\sigma_r^2 = \sigma_t^2 = -50$dB for the simulations in this section. Fig. 4 compares the SKC of HD and IBFD probing under an independent eavesdropper ($\rho' = 0$) with varying transmit power and different channel conditions. The results illustrate that the reduced correlation between continuous channels (ρ) is the limiting factor for HD probing, which makes it inferior to IBFD probing. The SKC decreases significantly with decreasing ρ for HD probing. IBFD probing with different correlation coefficients ρ is not compared since it does not impose an effect in this mode. For IBFD probing, the most critical factor limiting the key capacity is the ASIC depth. The SI has to be efficiently suppressed in the analog domain to guarantee the effectiveness of digital cancellation [25]. In addition to the SIC depth, another affecting factor is the SIC overheads, which is related to α. SIC overheads reduce the available resources for legitimate channel estimation, increasing the estimation error and reducing the SKC. For $\alpha < 0.5$, more OFDM symbols are available for legitimate channel estimation in IBFD mode than its HD counterpart, benefitting the SKC by reducing the estimation errors. However, α has to satisfy the condition that $T \cdot \min\left\{\frac{\alpha}{2}, 1-\alpha\right\} \geqslant \max\{N_A, N_B\}$; otherwise, it will decrease the SKC due to inappropriate digital cancellation, e.g., $\alpha = 0.1$. Too long SIC overheads (e.g., $\alpha = 0.6$) will also decrease the SKC of IBFD probing. In the high-SNR regime, IBFD can achieve a higher SKC than HD with effective ASIC depth and appropriate SIC overheads.

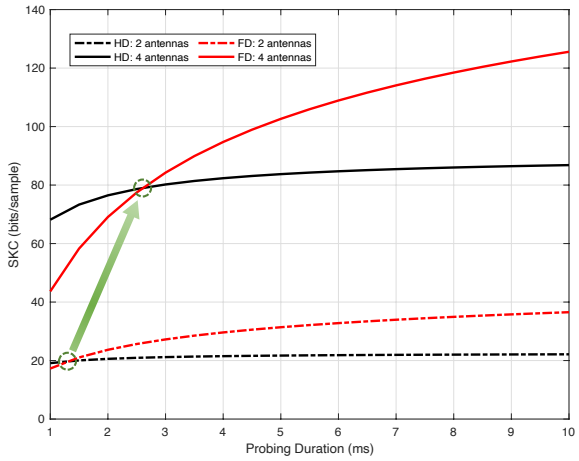
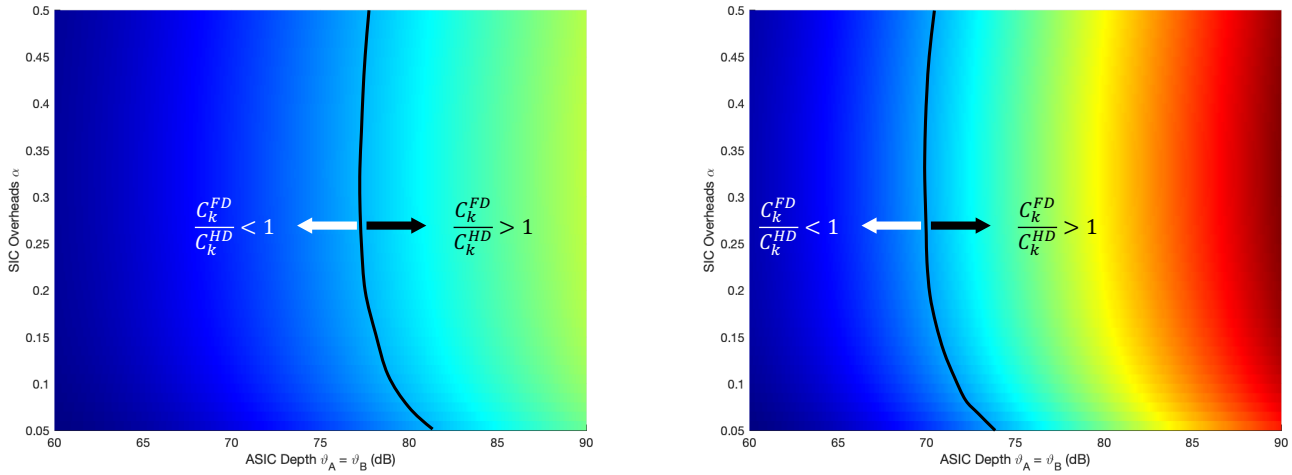


Fig. 6. SKC versus probing duration with different antenna array sizes.

Fig. 5 illustrates the SKC degradation due to the presence of a close eavesdropper, who can acquire a CFR correlated with the legitimate channel. The results show that if Eve cannot obtain a highly-correlated channel observation, it will not significantly reduce the SKC. The SKC degradation increases with decreasing ρ for HD and poor ASIC configurations (i.e., decreasing ϑ) for IBFD. In addition, IBFD could reduce the SKC degradation with effective ASIC for moving users, which have a low correlation coefficient ρ of continuous channels due to the Doppler shifts, compared to its HD counterpart. However, the SKC degradation for HD and IBFD probing is similar for relatively stationary users.

Fig. 6 shows the SKC variation with increasing probing duration and enlarged antenna arrays. It can be seen that a larger antenna array can significantly improve the SKC, illustrating the MIMO gain. However, a longer probing duration is required for IBFD to achieve a higher SKC than HD. The reason is that SIC requires longer overheads with enlarging



(a) $\rho = 0.99$ (b) $\rho = 0.95$

Fig. 7. Gain of IBFD probing over HD probing on secret key capacity (i.e., C_k^{FD}/C_k^{HD}) with varying SIC overheads and ASIC depth.

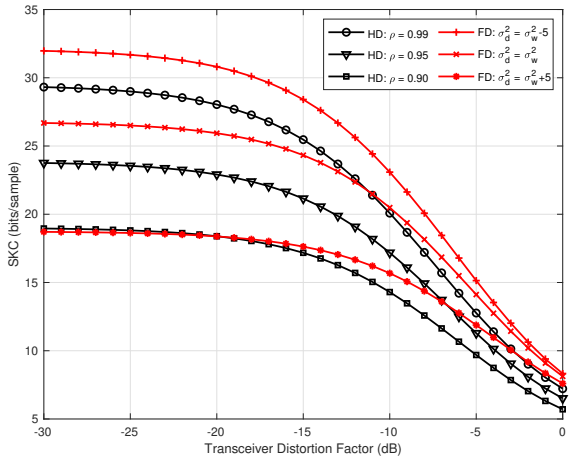


Fig. 8. Secret key capacity variation against increasing transceiver HWIs under various conditions ($N_A = N_B = 2$, $P_A = P_B = 25$dBm).

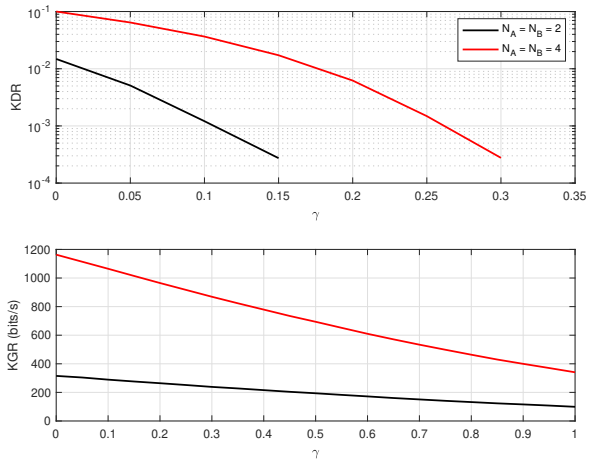


Fig. 9. KDR and KGR variation with widening guard stripes of the lossy quantizers (IBFD probing, $T = 14$).

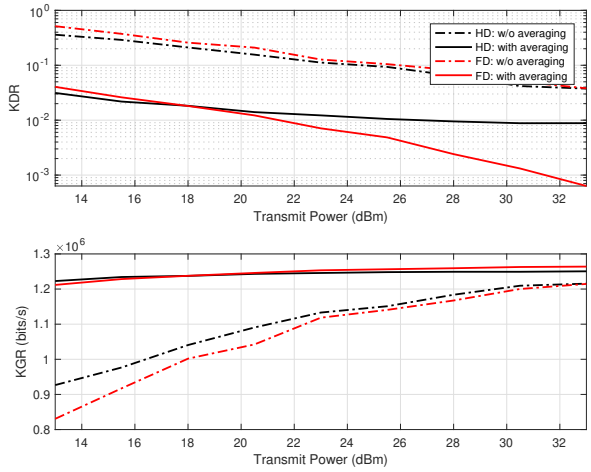
antenna arrays; otherwise, the RSI is increased, increasing the probing errors and reducing the SKC.

As analyzed above, the condition for IBFD to gain benefits over HD depends on the SIC overheads and ASIC depth for a fixed transceiver and channel condition. Thus, we explore the IBFD gain (C_k^{FD}/C_k^{HD}) with varying α and ϑ_A (ϑ_B), as Figure 7 shows. The results show that sufficient ASIC is the basis for IBFD to gain benefits, and appropriate SIC overheads can maximize the gain. With rapidly-varying channels (or fast-moving users), i.e., low ρ, IBFD probing has less requirement on the ASIC depth to outperform its HD counterpart.

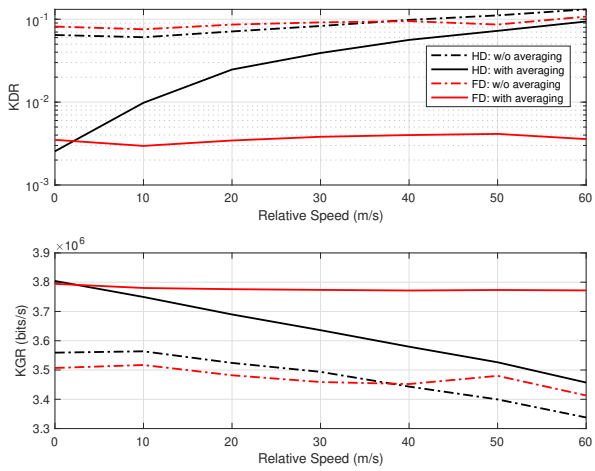
Fig. 8 shows the effects of transceiver HWIs, which are revealed as a fundamental limit of the SKC for both HD and IBFD probing. The results show that large transceiver distortions will reduce the SKC since they increase the inconsistencies between the measurements. For IBFD probing, the additional noise introduced by imperfect hardware of RF cancellers significantly affects the SKC, which is different from its impact on the system capacity. For maximizing the system capacity, as long as the additional noise caused by cancellers is not greater than the thermal noise of receivers, the maximum IBFD gain can be obtained [22], [25]. But for the SKC, the additional noise needs to be much smaller than the thermal noise to maximize the IBFD gain. With large transceiver HWIs, IBFD probing has obvious advantages over HD probing. The reason is that the penalty of RSI for IBFD becomes trivial when transceiver HWIs are significant.

B. Secret Key Generation Protocol

In this section, we run Monte Carlo simulations to evaluate the performance of the proposed CFR-based SKG scheme in terms of KGR, KDR, and randomness. We set $\sigma_r^2 = \sigma_t^2 =$



(a) KDR and KGR versus transmit power (SNR).



(b) KDR and KGR versus relative speed between legitimate users.

Fig. 10. Key performance comparison in HD and FD with various transmit power and Doppler shift ($\Delta_\tau = 25$ms, $L_b = 40$).

TABLE I
NIST TEST RESULTS (P-VALUES)

	$\Delta_\tau = 5$ms, $L_b = L_k$	$\Delta_\tau = 5$ms, $L_b = 40$	$\Delta_\tau = 25$ms, $L_b = L_k$	$\Delta_\tau = 25$ms, $L_b = 40$
Monobit	0.877	0.6877	0.6496	**0.9692**
Block frequency	0.0	0.9968	0.0	**0.9999**
Runs	0.0002	0.0	0.0049	**0.2456**
Longest runs	0.1421	0.0	0.0312	**0.2689**
DFT (Spectral)	0.0	0.0	**0.9346**	0.8753
Non-overlapping template	0.9461	0.9996	0.9964	**0.9999**
Maurer's universal statistical	0.0	0.0	**0.2311**	0.0141
Linear complexity	0.0	0.0	0.0779	**0.7876**
Serial	0.0	0.0	0.0535	**0.3483**
Approximate entropy	0.0	0.0	0.0676	**0.3431**
Cumulative sums	0.0	0.3859	0.0	**0.6899**
Random excursion	0.0266	0.0045	**0.2782**	0.0444
Random excursion variant	0.3192	0.0449	**0.2787**	0.1088
Number of passed tests	5 (×)	4 (×)	10 (×)	13 (✓)

-70dB, $\alpha = 0.3$ and $T = 14$ for simulations, and we consider 60dB of ASIC depth, which could be realized by a combination of antenna isolation and RF cancellation [25]. The additional noise caused by RF cancellers is set to be identical to the receivers' thermal noise. Simulation results show that the KDR is decreased to 0 in most cases with the index-based reconciliation as in [1], [20], so we show the KDR before the reconciliation. It should be noted that this scheme does not guarantee key agreement but will not cause key information leakage since the shared public message is independent of the key itself. For a lossy quantizer, it is efficient to remove a large portion of error bits through the index-based reconciliation method.

Fig. 9 shows the KDR and KGR variation against the width of the guard stripe of the lossy quantizers. The samples are collected with IBFD probing. Larger γ yields a wider guard stripe, and the KDR is reduced at the cost of a slow KGR. It also illustrates the benefits of antenna arrays that more antennas benefit the SKG in terms of KGR. Although an enlarged antenna array increases the KDR, it can be reduced by a fairly wide guard strip. For instance, 4-antenna arrays at legitimate users can achieve a KGR of 869bps and KDR approximate to the order of 10^{-4} with $\gamma = 0.3$. In contrast, 2-antenna arrays at legitimate users achieve a KGR of 275bps and KDR approximate to the same order (10^{-4}) with $\gamma = 0.15$. Thus, an enlarged antenna array improves the key performance in general with appropriate guard stripe and reconciliation.

Fig. 10 compares the key performance of HD and IBFD probing with different SNR (i.e., transmit power) and the relative speed of legitimate users. The quantization segment length is set to 40, i.e., $L_b = 40$ to guarantee the randomness of the generated key. A lossy quantizer with a narrow guard stripe (i.e., $\gamma = 0.01$) is utilized here to compare the KDR of different schemes explicitly; otherwise, there will not be error bits due to limited samples. A fast relative speed of legitimate users results in a large Doppler shift of the legitimate channel, reducing the correlation between consecutive CFRs (i.e., ρ). It shows that IBFD probing achieves lower KDR and higher KGR than its HD counterpart with high transmit power and fast relative speed between legitimate users, which is consistent with the theoretical analysis. Furthermore, it

shows the advantages of the CFR averaging operation, which fully utilizes the CFRs within the same band to significantly improve the key performance in terms of both KDR and KGR.

Table I shows the NIST test results for the generated key with different probing rates and quantization segment lengths, where binary matrix rank test and overlapping template test are not performed due to the limited length of the generated key. The random excursion and random excursion variant tests are performed with $J = 35$ (see [23]) due to the limited length, which may not be reliable. The relative speed of legitimate users is set to be 10m/s, and the key is generated from IBFD probing samples. Results indicate that there is a tradeoff between the KGR and the randomness of the key. A faster probing rate (i.e., a shorter probing interval of $\Delta_\tau = 5$ms) can increase the KGR, but the generated key only passes 5 of the 13 tests. Thus, in some ways, the generated key cannot be considered random. In contrast, a low probing rate (i.e., longer probing interval of $\Delta_\tau = 25$ms) is necessary to guarantee the security of the SKG scheme. The probing rate strongly depends on the environment. In a dynamically changing environment, the probing rate should be tuned by a proportional-integral-derivative controller. The readers are referred to [33] for a detailed description of applying such a controller to tune the probing rate. Besides, it also demonstrates the necessity of segmental quantization. If the samples are not quantized in segments, large-scale fading will cause consecutive 0s or 1s in the generated bit sequence so that it will fail in some tests. With appropriate probing rate and sample segmentation, the generated key passes all 13 tests.

VIII. Conclusion

In this paper, we have studied the secret key capacity of a CFR-based SKG scheme with IBFD and HD probing in MIMO systems by formulating the difference and correlation between the measurements of legitimate users. Theoretical analysis reveals that the fundamental limits of SKC come from the transceiver HWIs, while the non-simultaneous measurements limit the SKC for HD systems and SIC schemes (i.e., ASIC depth and SIC overheads) limit the SKC for IBFD systems. In the high-SNR regime, IBFD could have a larger probing error but achieve a higher SKC than HD with moving users. For stationary users, IBFD probing requires effective ASIC depth to outperform its HD counterpart, while appropriate SIC overheads can maximize the gain. Besides, IBFD probing is more robust to large transceiver HWIs than HD, and it could reduce the SKC degradation due to the presence of a close eavesdropper. MIMO systems can significantly improve the KGR, but longer SIC overheads are required for appropriate SIC. Thus, a longer probing duration is required for IBFD to provide benefits on the SKC over HD. Then, 3GPP specification-based simulations verified the effectiveness of the proposed SKG processing scheme. The results are consistent with the analysis.

Acknowledgment

A research grant from Huawei Technologies Canada Co., Ltd partly supported the work. This work of T. Ratnarajah is supported by the U.K. Engineering and Physical Sciences Research Council (EPSRC) under Grant EP/T021063/1.

TABLE II
Important Symbols and Descriptions

Symbol	Description
σ_t^2, σ_r^2	transceiver HWIs factor
$\sigma_{w,i}^2$	power of AWGN
$\sigma_{d,i}^2$	power of canceller's noise
$\sigma_{n,i}^2$	power of noise and interference for HD probing
$\sigma_{n,i,0}^2$	power of noise and interference for digital canceller
$\sigma_{n,i,1}^2$	power of noise and interference for IBFD probing
$\sigma_{\Delta,i}^2$	power of HD probing errors
$\sigma_{\Delta,i,0}^2$	power of estimation errors for digital canceller
$\sigma_{\Delta,i,1}^2$	power of IBFD probing errors
$\sigma_{s,i,0}^2$	power of RSI after digital cancellation
$\bar{\sigma}_{\Delta,i}^2$	power of HD probing errors in the high-SNR regime
$\bar{\sigma}_{\Delta,i,1}^2$	power of IBFD probing errors in the high-SNR regime
$\mathbf{\Phi}_i$, $\mathbf{\Psi}_i$	transceiver HWIs matrix
$\mathbf{W}_i$	AWGN matrix
$\mathbf{D}_i$	canceller's noise and distortion matrix
$\mathbf{G}_i$	effective SI channel after RF cancellation
α	SIC overheads to probing duration ratio
T	number of probing symbols
N_i	number of Tx/Rx antennas
P_i	transmit power
ϱ_i	pathloss of SI channel
ϱ_{AB}	pathloss of the legitimate channel
ϑ_i	realized ASIC depth in dB
η_i	$= 10^{-\frac{\vartheta_i}{10}}$
ρ	correlation coefficient of continuous legitimate channels
ρ'	correlation between legitimate and eavesdropping channels
γ	guard stripe of the lossy quantizer
Δ_τ	probing duration
L_b	the segment length of the segmental quantizer
L_k	the length of the generated key

Appendix A
Table for Notations

In this appendix, we list important and similar symbols in Table II to help reading this paper.

Appendix B
MMSE Channel Estimator

Assume $\mathbf{Y} = \mathbf{HX} + \mathbf{W}$, where $\mathbf{Y} \in \mathbb{C}^{M\times T}$, $\mathbf{H} \in \mathbb{C}^{M\times N}$, $\mathbf{X} \in \mathbb{C}^{N\times T}$, and $\mathbf{W} \in \mathbb{C}^{M\times T}$. The entries of matrices $\mathbf{X}$ and $\mathbf{W}$ are i.i.d. to Gaussian distribution with zero mean and variance of $\frac{P}{N}$ and σ_w^2, respectively. The MMSE estimate of $\mathbf{H}$ is given as

$$\begin{aligned}\hat{\mathbf{H}} &= \mathbf{Y}\left(\mathbb{E}\left\{\mathbf{Y}^\dagger\mathbf{Y}\right\}\right)^{-1}\mathbb{E}\left\{\mathbf{Y}^\dagger\mathbf{H}\right\}\\ &= \mathbf{Y}\left(\mathbf{X}^\dagger\mathbf{R}_{HH}\mathbf{X} + M\sigma_w^2\mathbf{I}\right)^{-1}\mathbf{X}^\dagger\mathbf{R}_{HH}\\ &= \mathbf{YX}^\dagger\left(\mathbf{R}_{HH}\mathbf{XX}^\dagger + M\sigma_w^2\mathbf{I}\right)^{-1}\mathbf{R}_{HH},\end{aligned} \tag{40}$$

where $\mathbf{R}_{HH} = \mathbb{E}\left\{\mathbf{H}^\dagger\mathbf{H}\right\}$ and $\mathbb{E}\left\{\mathbf{W}^\dagger\mathbf{W}\right\} = M\sigma_w^2\mathbf{I}$. It should have $T \geqslant \max(M, N)$ for an appropriate estimation; otherwise, the matrix in the parentheses of the inverse operation could be rank deficient. The estimation error is given as

$$\mathbf{\Delta}_H = \mathbf{H} - \hat{\mathbf{H}}. \tag{41}$$

According to the orthogonality principle [34], we have

$$\begin{aligned}\mathbb{E}\left\{\boldsymbol{\Delta}_H^{\dagger}\boldsymbol{\Delta}_H\right\} &= \mathbb{E}\left\{\left(\mathbf{H}-\hat{\mathbf{H}}\right)^{\dagger}\left(\mathbf{H}-\hat{\mathbf{H}}\right)\right\} \\ &= \mathbf{R}_{HH}-\mathbf{R}_{HH}\mathbf{X}\left(\mathbf{X}^{\dagger}\mathbf{R}_{HH}\mathbf{X}+M\sigma_w^2\mathbf{I}\right)^{-1}\mathbf{X}^{\dagger}\mathbf{R}_{HH} \\ &= \mathbf{R}_{HH}\left[\mathbf{I}-\mathbf{X}\left(\mathbf{X}^{\dagger}\mathbf{R}_{HH}\mathbf{X}+M\sigma_w^2\mathbf{I}\right)^{-1}\mathbf{X}^{\dagger}\mathbf{R}_{HH}\right] \\ &= \mathbf{R}_{HH}\left[\mathbf{I}-\left(\mathbf{X}\mathbf{X}^{\dagger}\mathbf{R}_{HH}+M\sigma_w^2\mathbf{I}\right)^{-1}\mathbf{X}\mathbf{X}^{\dagger}\mathbf{R}_{HH}\right] \\ &= M\sigma_w^2\mathbf{R}_{HH}\left(\mathbf{X}\mathbf{X}^{\dagger}\mathbf{R}_{HH}+M\sigma_w^2\mathbf{I}\right)^{-1}.\end{aligned} \tag{42}$$

Assume each element of the error matrix is independent of each other, then we have $\mathbb{E}\left\{\boldsymbol{\Delta}_H\boldsymbol{\Delta}_H^{\dagger}\right\} = N\sigma_w^2\mathbf{R}_{HH}\left(\mathbf{X}\mathbf{X}^{\dagger}\mathbf{R}_{HH}+M\sigma_w^2\mathbf{I}\right)^{-1}$. In the case of uncorrelated MIMO channel, i.e., $\mathbf{H}$ has i.i.d zero-mean complex Gaussian elements with variance of ϱ_H such that $\mathbf{R}_{HH} = M\varrho_H\mathbf{I}$, we can rewrite (40) as

$$\hat{\mathbf{H}} = \mathbf{Y}\left(\mathbf{X}^{\dagger}\mathbf{X}+\frac{\sigma_w^2}{\varrho_H}\mathbf{I}\right)^{-1}\mathbf{X}^{\dagger}. \tag{43}$$

Besides, the estimation error can be described by the circular complex Gaussian model as

$$\boldsymbol{\Delta}_H \sim \mathcal{CN}\left(\mathbf{0}, N\frac{\sigma_w^2}{\frac{PT}{N}+\frac{\sigma_w^2}{\varrho_H}}\mathbf{I}_M\right), \tag{44}$$

where the entries of $\boldsymbol{\Delta}_H$ are i.i.d. to zero-mean complex Gaussian distribution with variance of $\frac{\sigma_w^2}{\frac{PT}{N}+\frac{\sigma_w^2}{\varrho_H}}$.

Appendix C
Proof of Lemma 1

The conditional mutual information is computed as [18]

$$I\left(\mathbf{h}_A^{\epsilon};\mathbf{h}_B^{\epsilon}\mid\mathbf{h}_E^{\epsilon}\right) = \log_2\frac{\left|\mathbf{C}_{AE}^{\epsilon}\right|\left|\mathbf{C}_{BE}^{\epsilon}\right|}{\left|\mathbf{R}_E^{\epsilon}\right|\left|\mathbf{C}_{ABE}^{\epsilon}\right|}, \tag{45}$$

where $\mathbf{C}_{i,j}^{\epsilon} = \mathbb{E}\left\{\mathbf{v}_{ij}\mathbf{v}_{ij}^{\dagger}\right\}$ with $\mathbf{v}_{ij} = \left[(\mathbf{h}_i^{\epsilon})^T,(\mathbf{h}_j^{\epsilon})^T\right]^T$, $i,j\in\{A,B,E\}$, $\mathbf{C}_{ABE}^{\epsilon} = \mathbb{E}\left\{\mathbf{v}_{ABE}\mathbf{v}_{ABE}^{\dagger}\right\}$ with $\mathbf{v}_{ABE} = \left[(\mathbf{h}_A^{\epsilon})^T,(\mathbf{h}_B^{\epsilon})^T,(\mathbf{h}_E^{\epsilon})^T\right]^T$. Thus, we have

$$\left|\mathbf{C}_{AE}^{\epsilon}\right| = \begin{vmatrix}\mathbf{R}_A^{\epsilon} & \mathbf{R}_{AE}^{\epsilon}\\ \mathbf{R}_{EA}^{\epsilon} & \mathbf{R}_E^{\epsilon}\end{vmatrix} = \mathbf{R}_A^{\epsilon}\mathbf{R}_E^{\epsilon}-\mathbf{R}_{AE}^{\epsilon}\mathbf{R}_{EA}^{\epsilon}, \tag{46}$$

$$\left|\mathbf{C}_{BE}^{\epsilon}\right| = \begin{vmatrix}\mathbf{R}_B^{\epsilon} & \mathbf{R}_{BE}^{\epsilon}\\ \mathbf{R}_{EB}^{\epsilon} & \mathbf{R}_E^{\epsilon}\end{vmatrix} = \mathbf{R}_B^{\epsilon}\mathbf{R}_E^{\epsilon}-\mathbf{R}_{BE}^{\epsilon}\mathbf{R}_{EB}^{\epsilon}, \tag{47}$$

$$\begin{aligned}\left|\mathbf{C}_{ABE}^{\epsilon}\right| &= \begin{vmatrix}\mathbf{R}_A^{\epsilon} & \mathbf{R}_{AB}^{\epsilon} & \mathbf{R}_{AE}^{\epsilon}\\ \mathbf{R}_{BA}^{\epsilon} & \mathbf{R}_B^{\epsilon} & \mathbf{R}_{BE}^{\epsilon}\\ \mathbf{R}_{EA}^{\epsilon} & \mathbf{R}_{EB}^{\epsilon} & \mathbf{R}_E^{\epsilon}\end{vmatrix} \\ &= \mathbf{R}_A^{\epsilon}\mathbf{R}_B^{\epsilon}\mathbf{R}_E^{\epsilon}+\mathbf{R}_{AB}^{\epsilon}\mathbf{R}_{BE}^{\epsilon}\mathbf{R}_{EA}^{\epsilon}+\mathbf{R}_{AE}^{\epsilon}\mathbf{R}_{BA}^{\epsilon}\mathbf{R}_{EB}^{\epsilon} \\ &\quad -\mathbf{R}_B^{\epsilon}\mathbf{R}_{AE}^{\epsilon}\mathbf{R}_{EA}^{\epsilon}-\mathbf{R}_A^{\epsilon}\mathbf{R}_{BE}^{\epsilon}\mathbf{R}_{EB}^{\epsilon}-\mathbf{R}_E^{\epsilon}\mathbf{R}_{AB}^{\epsilon}\mathbf{R}_{BA}^{\epsilon}.\end{aligned} \tag{48}$$

The variance matrix of $\mathbf{h}_E^{\epsilon}\ \forall\,\epsilon$ is given as

$$\begin{aligned}\mathbf{R}_E^{\epsilon} = \mathbb{E}\left\{\mathbf{h}_E^{\epsilon}\left(\mathbf{h}_E^{\epsilon}\right)^{\dagger}\right\} &= \left(\rho'^2\varrho_{AB}+(1-\rho'^2)\varrho_{AB}\right)\mathbf{I}_{N_AN_B} \\ &= \varrho_{AB}\mathbf{I}_{N_AN_B}.\end{aligned} \tag{49}$$

Since the entries of $\mathbf{H}_{ij}^{\epsilon}$ and $\boldsymbol{\Delta}_{ij}^{\epsilon}$ are i.i.d. to zero-mean complex Gaussian distribution, and they are uncorrelated due to the orthogonality principle of MMSE estimators [34], it can be derived that $\mathbf{h}_i^{\epsilon}$ is distributed to zero-mean Gaussian distribution. The variance matrix of $\mathbf{h}_i^{\epsilon}$, $i\in\{A,B\}$ is different for different probing modes, which is given as

$$\mathbf{R}_i^{HD} = \mathbb{E}\left\{\mathbf{h}_i^{HD}\left(\mathbf{h}_i^{HD}\right)^{\dagger}\right\} = \left(\varrho_{AB}+\sigma_{\Delta,i}^2\right)\mathbf{I}_{N_AN_B}. \tag{50}$$

$$\mathbf{R}_i^{FD} = \mathbb{E}\left\{\mathbf{h}_i^{FD}\left(\mathbf{h}_i^{FD}\right)^{\dagger}\right\} = \left(\varrho_{AB}+\sigma_{\Delta,i,1}^2\right)\mathbf{I}_{N_AN_B}, \tag{51}$$

The covariance matrices for HD probing are given as

$$\begin{aligned}\mathbf{R}_{AB}^{HD} &= \mathbb{E}\left\{\mathrm{vec}\left(\mathbf{H}_{AB}^{(\tau_2)}\right)\left(\mathrm{vec}\left(\left(\mathbf{H}_{BA}^{(\tau_1)}\right)^T\right)\right)^{\dagger}\right\} \\ &= \mathbb{E}\left\{\mathrm{vec}\left(\mathbf{H}_{AB}^{(\tau_2)}\right)\left(\mathrm{vec}\left(\mathbf{H}_{AB}^{(\tau_1)}\right)\right)^{\dagger}\right\} \\ &= \rho\varrho_{AB}\mathbf{I}_{N_AN_B},\end{aligned} \tag{52}$$

$$\begin{aligned}\mathbf{R}_{AE}^{HD} &= \mathbb{E}\left\{\mathrm{vec}\left(\mathbf{H}_{AB}^{(\tau_2)}\right)\left(\mathrm{vec}\left(\left(\mathbf{H}_{EA}^{(\tau_1)}\right)^T\right)\right)^{\dagger}\right\} \\ &= \mathbb{E}\left\{\mathrm{vec}\left(\mathbf{H}_{AB}^{(\tau_2)}\right)\left(\mathrm{vec}\left(\left(\rho'\mathbf{H}_{BA}^{(\tau_1)}+\boldsymbol{\Lambda}_{BA}^{(\tau_1)}\right)^T\right)\right)^{\dagger}\right\} \\ &= \rho'\rho\varrho_{AB}\mathbf{I}_{N_AN_B},\end{aligned} \tag{53}$$

$$\begin{aligned}\mathbf{R}_{BE}^{HD} &= \mathbb{E}\left\{\mathrm{vec}\left(\mathbf{H}_{BA}^{(\tau_1)}\right)\left(\mathrm{vec}\left(\left(\mathbf{H}_{EA}^{(\tau_1)}\right)^T\right)\right)^{\dagger}\right\} \\ &= \mathbb{E}\left\{\mathrm{vec}\left(\mathbf{H}_{BA}^{(\tau_1)}\right)\left(\mathrm{vec}\left(\left(\rho'\mathbf{H}_{BA}^{(\tau_1)}+\boldsymbol{\Lambda}_{BA}^{(\tau_1)}\right)^T\right)\right)^{\dagger}\right\} \\ &= \rho'\varrho_{AB}\mathbf{I}_{N_AN_B},\end{aligned} \tag{54}$$

where ρ is the correlation coefficients of consecutive CFRs due to temporal changes within different probing slots τ_1 and τ_2 in HD such that [4]

$$\rho = \frac{Cov\left(\mathrm{vec}\left(\mathbf{H}_{AB}^{(\tau_1)}\right),\mathrm{vec}\left(\mathbf{H}_{AB}^{(\tau_2)}\right)\right)}{\sqrt{Var\left(\mathrm{vec}\left(\mathbf{H}_{AB}^{(\tau_1)}\right)\right)}\sqrt{Var\left(\mathrm{vec}\left(\mathbf{H}_{AB}^{(\tau_2)}\right)\right)}}. \tag{55}$$

The covariance matrices for IBFD probing can similarly be given as

$$\mathbf{R}_{AB}^{FD} = \varrho_{AB}\mathbf{I}_{N_AN_B}, \tag{56}$$

$$\mathbf{R}_{AE}^{FD} = \rho'\varrho_{AB}\mathbf{I}_{N_AN_B}, \tag{57}$$

$$\mathbf{R}_{BE}^{FD} = \rho'\varrho_{AB}\mathbf{I}_{N_AN_B}. \tag{58}$$

We will have $\mathbf{R}_{ji}^{\epsilon} = \left(\mathbf{R}_{ij}^{\epsilon}\right)^{\dagger} = \mathbf{R}_{ij}^{\epsilon}\ \forall\ i,j\in\{A,B,E\}$ since its a real-number identity matrix. Insert these covariance matrices into Equation (45), we can obtain the SKC of HD and IBFD modes as Equations (24) and (25) with $\varpi_i^{HD} = \varrho_{AB}+\sigma_{\Delta,i}^2$ and $\varpi_i^{FD} = \varrho_{AB}+\sigma_{\Delta,i,1}^2$.

APPENDIX D
PROOF OF LEMMA 2

The mutual information of $\mathbf{h}_A^\epsilon$ and $\mathbf{h}_B^\epsilon$ is given as

$$\begin{aligned} I\left(\mathbf{h}_A^\epsilon;\mathbf{h}_B^\epsilon\right) &= H\left(\mathbf{h}_A^\epsilon\right)+H\left(\mathbf{h}_B^\epsilon\right)-H\left(\mathbf{h}_A^\epsilon,\mathbf{h}_B^\epsilon\right) \\ &= \log_2\frac{\left|\mathbf{R}_A^\epsilon\right|\left|\mathbf{R}_B^\epsilon\right|}{\left|\mathbf{C}_{AB}^\epsilon\right|} \\ &= \log_2\frac{\left|\mathbf{R}_A^\epsilon\right|\left|\mathbf{R}_B^\epsilon\right|}{\left|\mathbf{R}_A^\epsilon\right|\left|\mathbf{R}_B^\epsilon-\mathbf{R}_{AB}^\epsilon\left(\mathbf{R}_A^\epsilon\right)^{-1}\mathbf{R}_{AB}^\epsilon\right|}. \end{aligned} \tag{59}$$

Insert Equations (50) and (52) into Equation (59), we can obtain the secret key capacity for HD probing under the spatial independence assumption as Equation (22). Similarly, insert Equations (51) and (56) into Equation (59), we can obtain the secret key capacity for IBFD probing under the spatial independence assumption as Equation (23).

REFERENCES

[1] Z. Zhuang, S. Jiang, Y. Xu, X. Luo, and X. Cheng, "A physical layer key generation scheme based on full-duplex mode in wireless networks without fixed infrastructure," *In Proc. Int. Conf. Inf. Commun. Syst.*, pp. 1-5, Aug. 2019.

[2] D. Guo, K. Cao, J. Xiong, D. Ma, and H. Zhao, "A Lightweight Key Generation Scheme for the Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 15, pp. 12137-12149, 2021.

[3] A. Sadeghi, M. Zorzi, and F. Lahouti, "Analysis of key generation rate from wireless channel in in-band full-duplex communications," *In Proc. IEEE Int. Conf. Commun. workshops*, pp. 104-109, May 2016.

[4] G. Li, A. Hu, J. Zhang, L. Peng, C. Sun, and D. Cao, "High-agreement uncorrelated secret key generation based on principal component analysis preprocessing," *IEEE Trans. Commun.*, vol. 66, no. 7, pp. 3022-3034, 2018.

[5] X. Wei, and D. Saha, "KNEW: Key Generation using NEural Networks from Wireless Channels," *In Proc. ACM Workshop on Wireless Security and Machine Learning*, pp. 45-50, May 2022.

[6] Z. Ji, Y. Zhang, Z. He, P.L. Yeoh, B. Li, H. Yin, Y. Li, and B. Vucetic, "Wireless secret key generation for distributed antenna systems: A joint space-time-frequency perspective," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 633-647, 2021.

[7] F. Rottenberg, T.H. Nguyen, J.M. Dricot, F. Horlin, and J. Louveaux, "CSI-based versus RSS-based secret-key generation under correlated eavesdropping," *IEEE Trans. Commun.*, vol. 69, no. 3, pp. 1868-1881, 2020.

[8] K. Lin, Z. Ji, Y. Zhang, G. Chen, P.L. Yeoh, and Z. He, "Secret Key Generation Based on 3D Spatial Angles for UAV Communications," *In Proc. IEEE Wireless Commun. Netw. Conf.*, pp. 1-6, Mar. 2021.

[9] M. Letafati, H. Behroozi, B.H. Khalaj, and E.A. Jorswieck, "Hardware-impaired PHY secret key generation with man-in-the-middle adversaries," *IEEE Wireless Commun. Lett.*, vol. 11, no. 4, pp. 856-860, 2022.

[10] A.K. Junejo, F. Benkhelifa, B. Wong, and J.A. McCann, "LoRa-LiSK: a lightweight shared secret key generation scheme for LoRA networks," *IEEE Internet Things J.*, vol. 9, no. 6, pp. 4110-4124, 2021.

[11] H. Vogt, Z.H. Awan, and A. Sezgin, "Secret-key generation: Full-duplex versus half-duplex probing," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 639-652, 2019.

[12] N. Aldaghri, and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2692-2705, 2020.

[13] K.P. Anjana, and R. Ramanathan, "Impact of Channel Estimation Errors on Secret Key Capacity in MIMO-OFDM Systems," *In Proc. Int. Conf. Commun. Inf. Comput. Technol.*, pp. 1-6, Jun. 2021.

[14] C.Y. Wu, P.C. Lan, P.C. Yeh, C.H. Lee, and C.M.Cheng, "Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1687-1700, 2013.

[15] G. Li, C. Sun, E.A. Jorswieck, J. Zhang, A. Hu, and Y. Chen, "Sum secret key rate maximization for TDD multi-user massive MIMO wireless networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 968-982, 2020.

[16] C. Chen, and M.A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 205-215, 2010.

[17] J. Zhang, X. Liu, and D. Xu, "Physical Layer Security Based on Full-Duplex Under the Impact of Channel Convergence," *In Proc. IEEE Int. Conf. Commun. Technol.*, pp. 259-262, Oct. 2021.

[18] G. Li, C. Sun, W. Xu, M. Di Renzo, and A. Hu, "On maximizing the sum secret key rate for reconfigurable intelligent surface-assisted multiuser systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 211-225, 2021.

[19] M. Wang, F. Gao, S. Jin, and H. Lin, "An overview of enhanced massive MIMO with array signal processing techniques," *IEEE J. Sel. Topics Signal Process.*, vol. 13, no. 5, pp. 886-901, 2019.

[20] M. Adil, S. Wyne, and S.J. Nawaz, "On quantization for secret key generation from wireless channel samples," *IEEE Access*, vol. 9, pp. 21653-21668, 2021.

[21] B. P. Day, A. R. Margetts, D. W. Bliss, and P. Schniter, "Full-Duplex MIMO Relaying: Achievable Rates Under Limited Dynamic Range," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 8, pp. 1541-1553, Sep. 2012.

[22] J. Zhang, H. Luo, N. Garg, A. Bishnu, M. Holm, and T. Ratnarajah, "Design and Analysis of Wideband In-Band-Full- Duplex FR2-IAB Networks," *IEEE Trans. Wireless Commun.*, vol. 21, no. 6, pp. 4183-4196, Jun. 2022.

[23] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, Special Publication 800-22, Rev.1a, Apr. 2010.

[24] K.E. Kolodziej, B.T. Perry, and J.S. Herd, "In-band full-duplex technology: Techniques and systems survey," *IEEE Trans. Microw. Theory Techn.*, vol. 67, no. 7, pp. 3025-3041, 2019.

[25] H. Luo, A. Bishnu, and T. Ratnarajah, "Design and Analysis of In-Band Full-Duplex Private 5G Networks Using FR2 Band," *IEEE Access*, vol. 9, pp. 166886-166905, Dec. 2021.

[26] P. Aquilina, A.C. Cirik, and T. Ratnarajah, "Weighted sum rate maximization in full-duplex multi-user multi-cell MIMO networks," *IEEE Trans. Commun.*, vol. 65, no. 4, pp. 1590-1608, 2017.

[27] D.Korpi, M.Heino, C.Icheln, K.Haneda, and M.Valkama, "Compact Inband Full-Duplex Relays With Beyond 100 dB Self-Interference Suppression: Enabling Techniques and Field Measurements," *IEEE Trans. Antennas Propag.*, vol. 65, no. 2, pp. 960-965, 2017.

[28] H. Luo, M. Holm, and T. Ratnarajah, "On the performance of active analog self-interference cancellation techniques for beyond 5G systems," *China Commun.*, vol. 18, no. 10, pp. 158-168, 2021.

[29] Y. Liu, S.C. Draper, and A.M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, pp. 1484-1497, 2012.

[30] K. Moara-Nkwe, Q. Shi, G.M. Lee, and M.H. Eiza, "A novel physical layer secure key generation and refreshment scheme for wireless sensor networks," *IEEE Access*, vol. 6, pp. 11374-11387, 2018.

[31] G. Li, Z. Zhang, Y. Yu, and A. Hu, "A hybrid information reconciliation method for physical layer key generation," *Entropy*, vol. 21, no. 7, pp. 688, 2019.

[32] *5G; Study on channel model for frequencies from 0.5 to 100 GHz (Release 16)*, document TR 38.901, 3rd Generation Partnership Project, Sophia Antipolis Cedex, France, 3GPP, 2020.

[33] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation based on PID controller," *IEEE Trans. Mobile Comput.*, vol. 12, no. 9, pp. 1842-1852, 2012.

[34] S.M. Kay, "Fundamentals of statistical signal processing: estimation theory," *Prentice-Hall, Inc.*, 1993.