Hindawi
Security and Communication Networks
Volume 2020, Article ID 8840645, 15 pages
https://doi.org/10.1155/2020/8840645

Research Article

A Secure Communication Scheme Based on Equivalent Interference Channel Assisted by Physical Layer Secret Keys

Xiaoyan Hu,[1] **Liang Jin**,[1,2] **Kaizhi Huang**,[1,2] **Keming Ma**,[1,2] **Changcheng Song**,[2] **and Shuaifang Xiao**[1,2]

[1]*PLA Strategic Support Force Information Engineering University, Zhengzhou 450001, China*
[2]*Purple Mountain Laboratories: Networking, Communications and Security, Nanjing 211111, China*

Correspondence should be addressed to Liang Jin; liangjin@263.net

Received 17 July 2020; Revised 3 September 2020; Accepted 18 September 2020; Published 21 October 2020

Academic Editor: Savio Sciancalepore

Due to the channel estimation error, most of the physical layer secret key generation schemes need information reconciliation to correct error key bits, resulting in reduced efficiency. To solve the problem, this work proposes a novel secure communication scheme based on a equivalent interference channel. Different keys generated from imperfect channel state information are directly applied to signal scrambling and descrambling, which is equivalent to the process of a signal passing through an interference channel. Legitimate communication parties can reduce interference with the help of similar keys and channel coding without sending additional signals, while the eavesdropper channel is deteriorated due to the spatial decorrelation. For this kind of schemes, we first establish a discrete memoryless broadcast channel model to derive the expressions of bit error rate (BER), channel capacity, and security capacity for performance analysis. Simulation results verify the derivations that the proposed scheme achieves secure communication with a correlated eavesdropping channel and has a higher upper bound of transmission rate. Furthermore, we design a new metric to evaluate the efficiency and the result shows that the proposed scheme has superior performance on error reconciliation efficiency, despite its slight increase in BER.

1. Introduction

With the rapid popularization of the 5th generation wireless systems (5G), the confidentiality of wireless communications is also receiving extensive attention. The mainstream approach to information protection is the modern cryptography based on preagreed key [1]. Most of the cryptographic protocols are implemented in two ways: public-key encryption [2] and symmetric-key encryption (e.g., AES [3]). The theoretical basis of both works on the same implicit assumption that eavesdroppers have insufficient computational capabilities of solving a certain mathematical problem in feasible time. However, quantum computers may break this principle because of their powerful computing capabilities. On the other hand, complex key distribution protocols may be limited by the hardware conditions of the low-power terminals, such as wireless sensors [4, 5]. To address the above challenges, physical layer secure transmission (ST) [6] and physical layer secret key generation (SKG, also called secret key distribution) [7] emerge and have caused a wide concern. Based on information theoretic security, the two methods can ensure unconditional security even if the eavesdropper has unlimited computational power [8]. Thus, they can be examined as an alternative complement to traditional cryptography for wireless communication security.

1.1. Related Works. The realization of information theoretic security, i.e., one-time-pad encryption, was first proposed by Shannon in [8], which requires that the information rate cannot exceed the secret key rate. On this basis, Wyner proposed a secure transmission approach based on wiretap channel model on the condition that the channel capacity of the legal channel must be larger than that of the eavesdropping channel [9]. After that seminal work, many studies

focused on how to create the above-mentioned favourable conditions for achieving information theoretic security. The source model based SKG exploits inherent characteristics of wireless channels (i.e., reciprocity, spatial decorrelation, and temporal variation) to provide security solutions [10]. The statistics of channel state information (CSI), such as Received Signal Strength (RSS) [11], Channel Impulse Response (CIR) [12], and Channel Frequency Response (CFR) [13], can be utilized as common random source to extract secret keys. In those studies, the two legal parties simultaneously measure the same noise channel to obtain highly correlated but not completely consistent CSI samples and then quantize them into secret bits. Due to the asymmetric noise and the evaluated error in half-duplex mode, legal parties have to correct the disagreement bits through the information reconciliation process [14] and then eliminate the influence of key leakage caused by sending reconciliation signals through privacy amplification [15].

Although research on physical layer security has been conducted for several years, there are still few applications because most schemes cannot meet the requirement of low-cost implementation. As proved in [16, 17], ST have strict requirements for the number of antennas to inject artificial interference while transmitting confidential information, which inevitably increases energy consumption. As for SKG, interactively sending reconciliation signal is necessary for both legal parties to reduce the negative impact of imperfect CSI and correct error key bits, which also results in large overhead [18]. The authors in [19, 20] try to reduce the estimation error of random sources by common signal processing techniques, such as PCA or Kalman filter. But these algorithms have higher requirements on computational ability of the communication devices. The authors in [13, 21] improved the quantization algorithm to reduce the key bit mismatch rate (BMR) with lower complexity, but they must send additional signals to transmit the quantization information. Moreover, sending additional reconciliation signals not only consumes resources originally used for normal wireless communication but also may leak some key information.

1.2. Motivation and Contributions. To address this challenge, we focus on developing more efficient physical layer security solutions. Our previous work [22] first proposed the notion of equivalent channel for authentication and key distribution. The equivalent channel is built by asymmetric physical layer secret keys generated from CSI. It is a cascade channel composed of encryption, decryption, and noiseless public channel. The scheme in [22] guarantees a secure and reliable transmission of private information without information or artificial noise, but it still needs to send additional hash signals to verify the message, and the assumption of noiseless channel is too ideal. Recent studies have applied similar ideas to physical layer authentication in [23, 24] and to ST in [25, 26]. But they still need to send additional signals for secret key quantization or verification, thus increasing overhead. In addition, although research studies such as [10, 27] have done a lot of work in key generation and secure channel capacity, the analysis of these new solutions that directly scramble signals by asymmetric secret keys is still rare, which makes it difficult to evaluate or optimize system performance. Furthermore, the impact of correlated eavesdropping channel on the security capacity is not considered.

Based on the previous work, this paper proposes a novel secure communication scheme based on equivalent interference channel (EIC). Specifically, legal parties first generate physical layer secret keys and then scramble encoded signals according to the keys to establish the equivalent scrambling channel. The legal receiver can generate similar keys to reduce the interference due to channel reciprocity. However, because of the spatial decorrelation of the wireless channel, the bit mismatch rate (BMR) of the keys of illegal eavesdropper in different location is much higher than that of the legal parties, so that the interference cannot be eliminated.

The main contributions of this paper are as follows:

(i) The physical layer keys in proposed scheme are used to scramble the encoded signal instead of encrypting original confidential information, and the error bits in received signals can be corrected by channel coding. Therefore, we save the overhead of sending additional signals for quantization, information reconciliation, or key verification.

(ii) We first establish a discrete memoryless broadcast channel (DMBC) model for this kind of schemes to evaluate the performance. The entire process of scrambling, descrambling, and noisy public channel is equivalent to an equivalent interference channel, and the expressions of BER, channel capacity, and security capacity are derived. Based on the deductions, we jointly design the SKG and secure communication method to optimize the channel capacity. The numerical and simulation results verify our theoretical analysis that the proposed scheme has a higher upper bound of transmission rate.

(iii) A new metric is proposed for defining and evaluating the efficiency of different schemes. The simulation results show that the efficiency of this scheme is higher than existing SKG and encrypted transmission schemes.

1.3. Organization and Notation. The rest of this paper is organized as follows. Section 2 describes the typical wireless channel model of SKG scheme. Section 3 outlines the existing schemes and the proposed scheme. The detailed description of the program flow is in Section 4. Section 5 presents the performance evaluation and optimization of the scheme. Section 6 presents the numerical and simulation results. The concluding remarks of this paper are given in Section 7. The corresponding proofs are deferred to the Appendix. The notations used in this paper are shown in Table 1.

Table 1: Glossary of symbols.

Symbol	Definition
h_{AB}, h_{AE}	Channel complex gains of Alice-Bob and Alice-Eve
ρ	Correlation coefficient between h_{AB} and h_{AE}
M	Confidential information
X	Encoded information of Alice
X_s	Signal after scrambling of Alice
Y_s	Received signal of Bob
Y	Signal after descrambling of Bob
Z_s	Received signal of Eve
Z	Signal after descrambling of Eve
$\mathbf{K}_A, \mathbf{K}_B, \mathbf{K}_E$	Secret key sequences of Alice, Bob, and Eve
$\mathbf{H}_A, \mathbf{H}_B, \mathbf{H}_E$	Common random source of Alice, Bob, and Eve
q	Quantization precision
t_s	Acquisition time of estimated channel gain
P_{AB}, P_{AE}	BMR between Alice and Bob keys and between Alice and Eve keys
P_{xy}, P_{xz}	BER of Bob and Eve in equivalent interference channel
$\Pr(\cdot)$	Traditional probability
ζ	Error reconciliation efficiency

2. Wireless Channel Model

Figure 1 shows the correlated eavesdropping channel model of SKG. The wireless channel between Alice and Bob is assumed to be an insecure Rayleigh fading channel with an eavesdropper denoted by Eve. All of them are equipped with a single antenna and work in time-division duplex (TDD) mode. Channel gains h_{AB}, h_{BA}, and h_{AE} are identically distributed random variables that satisfy $h \sim \mathcal{CN}(0, \sigma_h^2)$. We consider two types of eavesdroppers: the uncorrelated eavesdropper is far away from Alice or Bob but can receive signals from them; the correlated eavesdropper not only can receive all signals but also attempts to approach Bob in order to eavesdrop more information. As shown in Figure 1, the channel between Alice and Eve (or Alice-Eve channel for short) is correlated with the Alice-Bob channel, and ρ is the correlation coefficient between the channel gains h_{AB} and h_{AE}. In Rayleigh fading channel, ρ can be calculated in Jakes model as

$$\rho = \frac{E\left[h_{AB}^{\dagger} h_{AE}\right]}{\sigma_h^2} = J_0\left(2\pi \frac{d}{\lambda}\right), \tag{1}$$

where $J_0(\cdot)$ is a zeroth-order Bessel function of the first kind; d is the distance between Eve and Bob; and λ is the length of waveform. For an uncorrelated eavesdropper, $\rho = 0$.

3. Overview of Existing and Proposed Schemes

In the above wireless channel model, the process of existing physical layer secret key generation and encrypted transmission scheme is shown in Figure 2. First, Alice and Bob send pilot signals to estimate CSI to generate secret keys $\mathbf{K}_A$ and $\mathbf{K}_B$, where $\psi_q(\cdot)$ denotes the generation algorithm. Due to channel estimation errors, $\mathbf{K}_A$ and $\mathbf{K}_B$ are not consistent. Therefore, Alice and Bob need information reconciliation to correct wrong bits. Without loss of generality, we consider that Alice calculates the reconciliation signal $\mathbf{V}_A$ according to the preagreed generation matrix of linear block code and its own key $\mathbf{K}_A$, where $\phi(\cdot)$ is the calculation function of reconciliation information. Then, Alice sends $\mathbf{V}_A$ to Bob through the public channel. Based on $\mathbf{K}_B$ and $\mathbf{V}_A$, Bob decodes the reconciliation signal to get $\mathbf{K}_A$. Finally, Alice and Bob encrypt and decrypt the original confidential information M by a pair of identical keys. For most existing schemes, sending reconciliation information to obtain a consistent key is an essential step. However, this method has the following adverse effects: (i) sending additional quantization and reconciliation signals $\mathbf{V}_A$ will increase the overhead; (ii) the extra coding and decoding process will also increase the calculation cost; (iii) since coding method is overt, transmitting $\mathbf{V}_A$ on a public channel may reveal some key information. These shortcomings motivate us to develop a new secret key generation and application method.

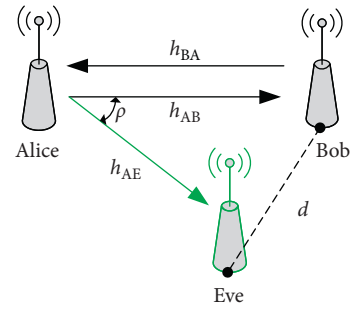

Figure 1: Wireless channel model.

The secure communication process of this scheme is shown in Figure 3. The main difference is that we directly use different keys to scramble the encoded signal instead of encrypting M with the same key. We perform channel decoding after descrambling to correct all wrong bits caused by different keys and noise. Instead of sending hash information, we verify the message with CRC check bits. Furthermore, apart from adding the key generation and scrambling module, we do not change the existing communication process. The specific steps of the scheme are detailed in Section 4.

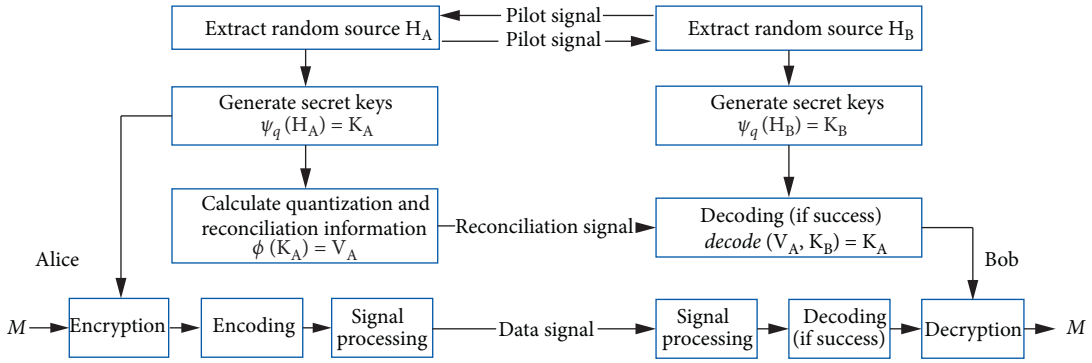

Figure 2: Process of the existing physical layer secret key generation and encrypted transmission scheme.

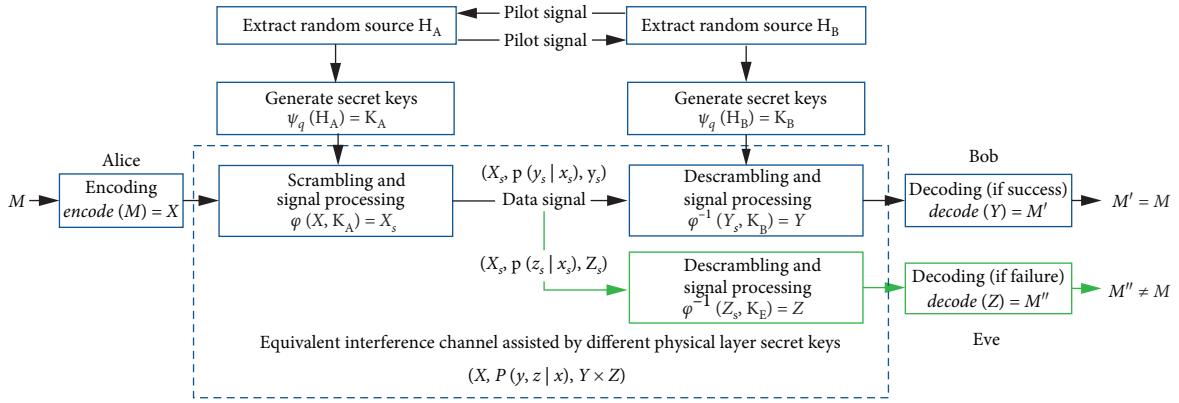

Figure 3: Process of secure communication scheme based on equivalent interference channel.

Based on this scheme, an equivalent interference channel model is established to derive performance evaluation functions. As shown in the black-dashed frame in Figure 3, we refer to the entire process between scrambling and descrambling as an equivalent interference channel, which is a DMBC denoted by $(\mathsf{X}, p(y, z \mid x), \mathsf{Y} \times \mathsf{Z})$, where $p(y, z \mid x)$ denotes channel transition probability, $x \in \mathsf{X}$ denotes encoded message of Alice, and $y \in \mathsf{Y}$ and $z \in \mathsf{Z}$ denote the received codewords of Bob and Eve, respectively, after descrambling. The data transmission channels of Alice-Bob and Alice-Eve are discrete memoryless channels (DMC) denoted by $(\mathsf{X}_s, p(y_s \mid x_s), \mathsf{Y}_s)$ and $(\mathsf{X}_s, p(z_s \mid x_s), \mathsf{Z}_s)$, where $x_s \in \mathsf{X}_s$ denotes the data signals sent by Alice after scrambling and $y_s \in \mathsf{Y}_s$ and $z_s \in \mathsf{Z}_s$ denote the received signals of Bob and Eve, respectively. Note that we estimate CSI in Rayleigh channel and evaluate the system in DMC model. The derivation results guide the design and optimization of the scheme, so there is no need to transmit signals for quantization or information verification like [22, 26]. The details of the performance analysis are presented in Section 5.

4. Process of the Proposed Scheme

4.1. Secret Key Generation. For TDD wireless system, there are two mainstream approaches for legal partners to obtain relevant common random source to generate secret key. One is to estimate the CSI by the received pilot signal; the other is sending random signals to mix the random signals and the channel gains [28]. The former is selected in this scheme.

4.1.1. Extraction of Common Random Source. As shown in Figure 3, Alice and Bob send pilot signals to each other for estimating CSI. Similarly, Eve obtains the CSI without sending pilot. When they measure the channel gain of the i-th received pilot signal with zero forcing (ZF) algorithm, the results can be expressed as follows:

$$\begin{cases} \widehat{h}_{\mathrm{A},i} = h_{\mathrm{BA},i} + n_{\mathrm{A},i}, \\ \widehat{h}_{\mathrm{B},i} = h_{\mathrm{AB},i} + n_{\mathrm{B},i}, \\ \widehat{h}_{\mathrm{E},i} = h_{\mathrm{AE},i} + n_{\mathrm{E},i}, \end{cases} \tag{2}$$

where $n_{\mathrm{A},i}$, $n_{\mathrm{B},i}$, and $n_{\mathrm{E},i}$ are the estimated errors of ZF algorithm. They are independent and identically distributed (i.i.d.) complex Gaussian random variables. Let σ_a^2 and σ_b^2 denote the pilot signal powers of Alice and Bob, respectively, and let σ_n^2 denote the noise power. Then, according to the channel estimation error model in [29, 30], the probability distributions of $n_{\mathrm{B},i}$ and $n_{\mathrm{E},i}$ are $\mathcal{CN}(0, \sigma_n^2/(\sigma_a^2\sigma_p^2))$ and $n_{A,i} \sim \mathcal{CN}(0, \sigma_n^2/(\sigma_b^2\sigma_p^2))$. For a correlated eavesdropper, $h_{\mathrm{AE},i}$ can be rewritten as

$$h_{\mathrm{AE},i} = \rho h_{\mathrm{AB},i} + \sqrt{1-\rho^2}\, n_{h,i}, \tag{3}$$

where $n_{h,i}$ is independent of $h_{AB,i}$, which satisfies $n_{h,i} \sim \mathcal{CN}(0, \sigma_h^2)$. To ensure the maximum independence of random sources, Alice and Bob send pilot signals to each other only once in each coherent time. Assume that the Alice-Bob channel in the same coherent time remains unchanged because of the reciprocity. Then it can be inferred that $h_{AB,i} = h_{BA,i}$. After N coherent times, Alice, Bob, and Eve hold N channel estimation results as samples of common random source, i.e., $\mathbf{H}_B = \{\widehat{h}_{B,i},\ 1 \le i \le N\}$ and $\mathbf{H}_E = \{\widehat{h}_{E,i},\ 1 \le i \le N\}$.

4.1.2. Quantization. In general, the purpose of quantization algorithm for Alice and Bob is to quantize the common random source into more secret key bits, while the probability of keeping key mismatch between them and the probability of key being successfully predicted by Eve are both low. Since different key bits can be corrected in the next channel decoding process, we pay more attention to increasing the obstacle of the key being predicted by the eavesdropper. This is different from the traditional quantization algorithm in SKG, which focuses more on key consistency. Therefore, we select q-bit equal-probability quantization algorithm to generate secret keys, where q represents quantization precision. Assume that the secret keys of Alice, Bob, or Eve are denoted by $\mathbf{K}_u$, where u = A, B or E. As for the shared random source with complex Gaussian distribution, let $F(s)$ be the probability distribution function, and let $F^{-1}(z), z \in [0, 1]$ be its inverse function. To obtain more keys, the real part and the imaginary part of the channel gains are quantized, respectively. The quantization algorithm is shown in Table 2.

After converting the quantized key into binary gray code, the length of the output secret keys is Nq bits. To evaluate the BMR of the secret keys $\mathbf{K}_A$, $\mathbf{K}_B$, and $\mathbf{K}_E$, we take 1-bit quantization as an example to deduce the following theorem.

Theorem 1. *If we perform 1-bit equal-probability quantization algorithm on the complex Gaussian random vectors $\mathbf{H}_A$ and $\mathbf{H}_B$, the BMR between the outputs $\mathbf{K}_A$ and $\mathbf{K}_B$ denoted by $P_{AB}(\gamma_a, \gamma_b, q)$ is as follows:*

$$P_{\mathrm{AB}}(\gamma_a, \gamma_b, 1) = \frac{1}{2} - \frac{1}{\sqrt{2\pi}} \int_0^{\infty} \mathrm{erf}\left(\sqrt{\frac{\gamma_a s^2}{2}}\right) \mathrm{erf} \cdot \left(\sqrt{\frac{\gamma_b s^2}{2}}\right) \exp\left(\frac{-s^2}{2}\right) \mathrm{d}s, \tag{4}$$

where $\gamma_a = (\sigma_a^2 \sigma_h^2 / \sigma_n^2)$ and $\gamma_b = (\sigma_b^2 \sigma_h^2 / \sigma_n^2)$ are the normalized SNR of pilot signals of Alice and Bob, respectively. For the random sources of Alice and Eve, that is, $\mathbf{H}_A$ and $\mathbf{H}_E$, $P_{AE}(\gamma_a, \gamma_b, q, \rho)$ is as follows:

$$P_{\mathrm{AE}}(\gamma_a, \gamma_b, 1, \rho) = \frac{1}{2} - \frac{1}{\sqrt{2\pi}} \int_0^{\infty} \mathrm{erf}\left(\sqrt{\frac{\gamma_b s^2}{2}}\right) \times \mathrm{erf} \cdot \left(\sqrt{\frac{\gamma_a \rho^2 s^2}{2\left(\gamma_a - \rho^2 \gamma_a + 1\right)}}\right) \exp\left(\frac{-s^2}{2}\right) \mathrm{d}s. \tag{5}$$

The following relationship is satisfied:

$$P_{\mathrm{AE}}(\gamma_a, \gamma_b, 1, \rho) \ge P_{\mathrm{AB}}(\gamma_a, \gamma_b, q) = P_{\mathrm{AE}}(\gamma_a, \gamma_b, 1, 1). \tag{6}$$

Proof:. see Appendix A.

From (4), one can see that $P_{\mathrm{AB}}(\gamma_a, \gamma_b, 1)$ decreases with the increase of γ_a and γ_b, and this conclusion is still valid on multibit quantization [31]. This shows that we can obtain more consistent keys by increasing the power of the pilot signal, thereby improving the robustness of our scheme. From (5) and (1), it is clear that $P_{\mathrm{AE}}(\gamma_a, \gamma_b, 1, \rho)$ increases when Eve and Bob get farther. If we let $d \longrightarrow \infty$, then $\rho \approx 0$ and $P_{\mathrm{AE}}(\gamma_a, \gamma_b, 1, \rho) \approx 0.5$. This conclusion is consistent with most of the SKG experiments; that is, the channels of Alice-Bob and Alice-Eve can be considered approximately independent when $d > 0.5\lambda$ in a scattering-rich channel environment. Therefore, in most cases, spatial decorrelation of the wireless channel protects the legal party's secret key from being predicted by Eve. In practice, $P_{\mathrm{AB}}(\gamma_a, \gamma_b, q)$ and $P_{\mathrm{AE}}(\gamma_a, \gamma_b, q, \rho)$ can be solved by statistical counting. In Section 6, we get the statistical value of multibit quantization BER from the simulation result.

Assuming that the average acquisition time of each channel estimated sample is t_s and the processing delay is ignored, the secret key generation rate of the proposed scheme is

$$R_s = \frac{2q}{t_s}. \tag{7}$$

Note that the choice of q is crucial to BMR and secret key generation rate. In Section 5, we will introduce a method for dynamically selecting q according to SNR. □

4.2. Construction of the Equivalent Interference Channel. Unlike encrypting information with the same keys, scrambling and descrambling are performed to construct interference channel based on different keys. The interference can be injected in multiple steps of the signal processing, including spread spectrum, precoding, or changing constellation diagram in modulation like [32]. To facilitate hardware implementation, we XOR the key bits with the signal we want to scramble. As shown in Figure 3, the message M after encoding is denoted by X, and the codeword after scrambling is expressed as X_s. Then, Alice sends X_s via the Alice-Bob data channel. After that, Bob receives

Table 2: Equal-probability quantization algorithm.

Input	$\mathbf{H}_{\mathrm{u}}$,$F(s)$, and q
Output	Secret key $\mathbf{K}_{\mathrm{u}}$
Initialization	(1) Calculate $F^{-1}(z)$ and the variance of $\mathbf{H}_{\mathrm{u}}$ (2) Set 2^q quantization partitions, where the lth partition is expressed as $Q_l = (F^{-1}(l - 1/2^q), F^{-1}(l/2^q))$
Quantification	(3) If $s_{\mathrm{u},i} \in Q_l$, then $k_{\mathrm{u},i} = l$ (4) Convert quantized key $k_{\mathrm{u},i}$ into gray code $(k_{u,q(i-1)+1}', k_{u,q(i-1)+2}', \ldots, k_{u,qi}')$ with length q (5) Repeat steps 3 and 4 until $i = N$, and then output $\mathbf{K}_u = \{k_{u,i}, 1 \le i \le N\} = \{k_{u,j}', 1 \le j \le Nq\}$

Y_s and descrambles it by $\mathbf{K}_{\mathrm{B}}$. Finally, Bob performs decoding to recover M. The reception capabilities of Bob and Eve in EIC will be discussed in Section 5.

Note that the proposed scheme is similar to ST schemes based on artificial noise [33]. For the latter, the interference in the received signal arises because the artificial noise injected into the null space is not eliminated completely. For this scheme, the reason for the increase of BER is that estimation error of CSI cannot be eliminated completely. The commonality is to deteriorate the eavesdropping channel. Then, the legal party can use the advantage of signal-to-noise ratio and well-designed channel coding to transmit large amounts of information without leaking to eavesdroppers. Therefore, the careful design of channel coding is also necessary. It must fulfill the requirement that the error bits in Bob's received signal can be corrected while preventing Eve from effectively correcting them during the channel decoding. As shown in Figure 3, Alice first adds CRC check bits to the message M and then encodes it as $X = \mathrm{encode}(M)$. To prevent Eve from recovering M, Alice should encode M with the highest possible code rate on the premise of meeting the system BER requirements. We analyzed the BER of Bob and Eve after decoding in Section 6. After decoding and getting M', if Bob's CRC does not match M', the retransmission of M shall be carried out in accordance with ARQ protocol. Thus, the proposed scheme does not need to send verification information as [22].

5. Performance Evaluation

In this section, we evaluate the performance of the scheme based on the equivalent interference channel model by deriving BER, channel capacity, security capacity, and error reconciliation efficiency of the scheme. Such metrics are commonly used in the performance analysis of physical layer security technologies.

5.1. Channel Capacity. First, we take the Alice-Bob channel as an example to calculate the channel capacity C_{xy}, which characterizes the limit of transmission rate. Note that it incorporates the effect of modulation and signal processing methods. The equivalent interference channel of Alice-Bob denoted by $(\mathsf{X}, p(y \mid x), \mathsf{Y})$ with input X, output Y, and the transition probability matrix is as follows:

$$p(y \mid x) = \begin{matrix} \\ 0 \\ 1 \end{matrix} \begin{matrix} \begin{matrix} 0 & \quad 1 \end{matrix} \\ \begin{bmatrix} 1 - p_{xy}(\gamma_d, \gamma_a, \gamma_b, q) & p_{xy}(\gamma_d, \gamma_a, \gamma_b, q) \\ p_{xy}(\gamma_d, \gamma_a, \gamma_b, q) & 1 - p_{xy}(\gamma_d, \gamma_a, \gamma_b, q) \end{bmatrix} \end{matrix} \tag{8}$$

where $P_{xy}(\gamma_d, \gamma_a, \gamma_b, q)$ is the bit error rate of Y with respect to X and γ_d is the SNR of the received data signal. As shown in the dashed box in Figure 3, it contains the transmission channel of the data signal. Similarly, assume that the BER of transmission channel $(\mathsf{X}_s, p(y_s \mid x_s), \mathsf{Y}_s)$ is denoted by $P_d(\gamma_d)$. To deduce $P_{xy}(\gamma_d, \gamma_a, \gamma_b, q)$ and C_{xy}, the following theorem is stated.

Theorem 2. *For an equivalent interference channel $(\mathsf{X}, p(y \mid x), \mathsf{Y})$, it is equivalent to a cascade channel composed of $(\mathsf{X}_s, p(y_s \mid x_s), \mathsf{Y}_s)$ and a virtual binary symmetric channel with bit error rate $P_{AB}(\gamma_a, \gamma_b, q)$. $P_{xy}(\gamma_d, \gamma_a, \gamma_b, q)$ is given as*

$$\begin{aligned} P_{xy}(\gamma_d, \gamma_a, \gamma_b, q) = {} & P_d(\gamma_d) + P_{\mathrm{AB}}(\gamma_a, \gamma_b, q) \\ & - 2P_{\mathrm{AB}}(\gamma_a, \gamma_b, q) P_d(\gamma_d). \end{aligned} \tag{9}$$

When the input X satisfies $\Pr(x = 0) = \Pr(x = 1) = 0.5$, the channel capacity is as follows:

$$C_{xy} = 1 - H\left(P_{xy}(\gamma_d, \gamma_a, \gamma_b, q)\right) \text{ bit/channel use}, \tag{10}$$

where $H(\cdot)$ is the entropy function.

Proof:. see Appendix B.

C_{xy} defines the upper limit of the amount of information transmitted on the Alice-Bob channel each time. From (9) and (10), we can find an obvious relationship that the effects of $P_d(\gamma_d)$ and $P_{\mathrm{AB}}(\gamma_a, \gamma_b, q)$ are the same for C_{xy}, which inspires us to equate the processes of scrambling and descrambling with different keys to an equivalent interference channel. Obviously, the solution of capacity of Alice-Eve channel C_{xz} is the same as C_{xy}:

$$C_{xz} = 1 - H(P_{xz}(\gamma_d, \gamma_a, \gamma_b, q, \rho)) \text{ bit/channel use}, \tag{11}$$

where $P_{xz}(\gamma_d, \gamma_a, \gamma_b, q, \rho)$ is the bit error rate of Z with respect to X. □

5.2. Security Capacity. Security capacity represents the theoretical upper limit of secure transmission rate [9]. It indicates the advantage of the legal parties in channel capacity compared with Eve. For DMBC channel model, it is expressed as follows [34]:

$$C_s = \left[C_{xy} - C_{xz}\right]^+, \tag{12}$$

where $[\cdot]^+$ denotes $\max(0, \cdot)$. We derive security capacity in the following two different eavesdropping scenarios.

5.2.1. Uncorrelated Eavesdropping Scenario. In an uncorrelated eavesdropping scenario, Eve is far away from Alice and Bob. Based on previous analysis, this makes ρ approach zero and makes $P_{\mathrm{AE}}(\gamma_a, \gamma_b, q, \rho)$ approach 0.5. Therefore, Eve randomly generates $\mathbf{K}_{\mathrm{E}}$ to reduce interference in the Alice-Eve channel without any prior knowledge about common random source. Let $\mathbf{P}_{\mathrm{u}} = [P_{u,0}, P_{u,1}, \ldots, P_{u,q}]$ denote the probability distribution of the random variables $k_{\mathrm{u}} \in (0, 1, \ldots, q)$, which are shown in Table 2. Then we give Corollary 1 to illustrate the probability of Eve successfully predicting Alice key.

Corollary 1. *For two independent and identically distributed sequences of N random variables samples $\mathbf{K}_A = \{k_{A,i},\ 1 \le i \le N\}$ and $\mathbf{K}_E = \{k_{E,i},\ 1 \le i \le N\}$ generated by the quantization algorithm shown in Table 2, the probability distribution of each quantized output k_u is $\mathbf{P}_u = [P_{u,0}, P_{u,1}, \ldots, P_{u,q}]$. Then, the following inequality holds:*

$$\Pr(\mathbf{K}_{\mathrm{A}} = \mathbf{K}_{\mathrm{E}}) \ge \left[2^{-H(k_{\mathrm{u}})}\right]^N. \tag{13}$$

And if and only if $P_{u,0} = P_{u,1} = \cdots = P_{u,q}$, the equal sign holds.

Proof:. see Appendix C.

From (13), it can be inferred that when $P_{u,0} = P_{u,1} = \cdots = P_{u,q}$ and $H(k_u) = q$, we can minimize the possibility of Eve successfully predicting $\mathbf{K}_{\mathrm{A}}$. It is our motivation for choosing equal q-bit equal-probability quantization algorithm. After converting k_{u} into gray code k_u' of length Nq, (13) can be rewritten as

$$\Pr(\mathbf{K}_{\mathrm{A}} = \mathbf{K}_{\mathrm{E}}) = \left[2^{-q}\right]^N = \left[\Pr(k_{\mathrm{A}}' = k_{\mathrm{E}}')\right]^{Nq}, \tag{14}$$

and the bit error rate is given by $\Pr(k_{\mathrm{A}}' = k_{\mathrm{E}}') = 0.5$. Therefore, the capacity of Alice-Eve equivalent interference channel is given by $C_{xz} = 0$ according to (11), and the security capacity is given by $C_s = [C_{xy}]^+$. □

5.2.2. Correlated Eavesdropping Scenario. In a more dangerous scenario with an correlated eavesdropper, Eve increases the correlation between h_{AB} and h_{AE} by approaching Bob. In this way, Eve may obtain random source samples similar to the legal parties and generate $\mathbf{K}_{\mathrm{E}}$ as consistent as possible with $\mathbf{K}_{\mathrm{A}}$. According to Theorem 2 and (12), C_s can be rewritten as

$$\begin{aligned} C_s &= \left[C_{xy} - C_{xz}\right]^+ = \left[H(P_{xz}(\gamma_d, \gamma_a, \gamma_b, q, \rho))\right. \\ &\quad \left. - H\left(P_{xy}(\gamma_d, \gamma_a, \gamma_b, q)\right)\right]^+ \ge 0. \end{aligned} \tag{15}$$

Due to the fact that the entropy function $H(\cdot)$ is a rigid monotony increasing convex function at $(0, 0.5)$, we can infer that $C_s > 0$ when $P_{\mathrm{AE}}(\gamma_a, \gamma_b, q, \rho) > P_{\mathrm{AB}}(\gamma_a, \gamma_b, q)$. Benefiting from the spatial decorrelation, the inequality $P_{\mathrm{AE}}(\gamma_a, \gamma_b, q, \rho) > P_{\mathrm{AB}}(\gamma_a, \gamma_b, q)$ holds in most environments with multipath scattering even if Eve is extremely close to Bob [7]. Therefore, our scheme can obtain a positive upper bound of secure transmission rate with correlated eavesdropping channel.

5.3. Optimization of the Proposed Scheme. Note that the unit in (10) and (11) is bit per channel use, and the utilization frequency (i.e., the scrambling rate) of the equivalent scrambling channel is determined by the scrambling method. The same as one-time-pad encryption, we have $H(X) = H(\mathbf{K}_{\mathrm{U}})$. Assuming that the newly generated key is immediately used to scramble X, the utilization frequency denoted by R_f is equal to the bit rate of X, which can be given as

$$R_f = \frac{H(X)}{Nt_s} = \frac{H(\mathbf{K}_{\mathrm{u}})}{Nt_s} \overset{(a)}{=} \frac{2NH(k_u)}{Nt_s} = R_s, \tag{16}$$

where (a) holds due to the equal probability quantization and $H(k_u) = q$. Then, according to (7), (10) and (11) can be rewritten in bits per second as

$$C_{\mathrm{AB}} = R_f C_{xy} = \frac{2q}{t_s}\left[1 - H\left(P_{xy}(\gamma_d, \gamma_a, \gamma_b, q)\right)\right]\mathrm{bit/s}, \tag{17}$$

$$C_{\mathrm{AE}} = R_f C_{xz} = \frac{2q}{t_s}\left[1 - H(P_{xz}(\gamma_d, \gamma_a, \gamma_b, q, \rho))\right]\mathrm{bit/s}. \tag{18}$$

Obviously, in order to maximize security capacity, q should be adjusted dynamically according to current γ_a, γ_b, and γ_d of Alice, Bob, and Eve. However, knowing Eve's SNR, BER or decoding method may not be easy. Thus, in this paper, we only discuss the optimization of C_{AB}. For given γ_d, γ_a, γ_b, and t_s, this problem can be described as

$$q^* = \arg\max_{q \in N_+} C_{\mathrm{AB}} = \arg\max_{q \in N_+} \frac{2q}{t_s}\left[1 - H\left(P_{xy}(\gamma_d, \gamma_a, \gamma_b, q)\right)\right]. \tag{19}$$

Equation (19) provides a reference for the design of signal power and quantization precision of the scheme. From the simulation results in the next section, we find that the optimal value usually satisfies $q^* \le 5$ in an actual environment (e.g., $\gamma_d \le 10$ dB and $\gamma_a = \gamma_b \le 30$ dB). Therefore, (19) is solved by one-dimensional search.

5.4. Error Reconciliation Efficiency. Channel coding is a common technique for correcting error bits in different schemes, although it reduces efficiency. However, the comparison of the efficiency in different schemes was rarely discussed in previous works, which inspires us to measure it with a new and unified metric. The error reconciliation efficiency denoted by $\zeta \in [0, 1]$ is expressed as follows:

$$\zeta = \frac{L_M}{L}, \tag{20}$$

where L_M is the length of initial information M transmitted by Alice; L is the total number of bits sent by both legal parties for the purpose of transmitting M safely and correctly. For ease of analysis, it is assumed that the channel for

transmitting confidential data or reconciliation signals is noiseless, while the pilot channel is noisy. The schemes in Figures 2 and 3 use the same linear block code (n_s, k_s), and $\eta = (k_s/n_s)$ denotes the code rate.

For our proposed scheme, the error bits in received signal will be corrected in the process of channel decoding. Therefore, L is the length of codeword after encoding, and the error reconciliation efficiency is equal to the code rate; i.e., $\zeta_{\mathrm{EIC}} = \eta$.

For existing schemes in Figure 2, information reconciliation is a necessary step to obtain the same keys. The mainstream is to use channel coding in two different ways. One is described in [35–37]. Assume that Alice calculates parity check bits based on the generator matrix of systematic linear block code and its keys of length k_s. Then, Alice sends them to Bob through the public channel. Since the generator matrix is well known, it divulges $(n_s - k_s)$ bits secret keys [17], so the length of available secret keys $L_{\mathrm{key}\,1}$ after information reconciliation is

$$\begin{cases} L_{\mathrm{key}\,1} = k_s - (n_s - k_s), & \text{for } \eta \in (0.5, 1), \\ L_{\mathrm{key}\,1} = 0, & \text{for } \eta \in (0, 0.5]. \end{cases} \tag{21}$$

Under the condition of one-time-pad encryption, we have $L_M = L_{\mathrm{key}\,1}$, and the error reconciliation efficiency is

$$\zeta_{k1} = \frac{L_{\mathrm{key}\,1}}{(n_s - k_s) + L_{\mathrm{key}\,1}} = \min\left(2 - \frac{1}{\eta}, 0\right). \tag{22}$$

The other method is described in [38–40]. Supposing that Alice creates the check information by XOR a series of encoded random number with its keys of length n_s and sends them to Bob, the length of available secret keys is $L_{\mathrm{key}\,2} = k_s$. Therefore, we have

$$\zeta_{k2} = \frac{k_s}{n_s + k_s}. \tag{23}$$

According to (20)–(23), it can then be inferred that the error reconciliation efficiency of the above three methods satisfies

$$\begin{cases} \zeta_{\mathrm{EIC}} > \zeta_{k1} > \zeta_{k2}, & \text{for } \eta \in \left(\dfrac{\sqrt{5}-1}{2}, 1\right), \\ \zeta_{\mathrm{EIC}} > \zeta_{k2} > \zeta_{k1}, & \text{for } \eta \in \left(0, \dfrac{\sqrt{5}-1}{2}\right]. \end{cases} \tag{24}$$

6. Numerical and Simulation Results

This section shows our Monte Carlo simulation results and theoretical results. The experiment was repeated 5,000 times in each simulation; and, for each experiment, 10,000 channel gain and noise samples are randomly generated. To simplify the analysis, we omit other processes except modulation and take BPSK for an instance to calculate $P_d(\gamma_d)$, which is only affected by the SNR of the received data signal γ_d. For the Rayleigh data channel with $h \sim \mathcal{CN}(0, 1)$, $P_d(\gamma_d)$ can be calculated by the following formula:

$$P_d(\gamma_d) = \frac{1}{2}\left(1 - \sqrt{\frac{\gamma_d}{1 + \gamma_d}}\right). \tag{25}$$

6.1. Security and Reliability Verification. In this subsection, we prove the security and reliability of the scheme by calculating and simulating BER, channel capacity, and security capacity. Figure 4 shows that the BER of Bob's received signal is affected by quantization precision q, the SNR of the received pilot signal γ_a and γ_b, and the SNR of the received data signal γ_d. One can see that BER decreases with the increase of γ_a, γ_b, and γ_d. This phenomenon proves the inference based on Theorem 2 that the equivalent interference and the noise in data transmission channel have similar effects on reception capability. It also confirms that γ_a and γ_b described have the same effect on $P_{\mathrm{AB}}(\gamma_a, \gamma_b, q)$, which implies that increasing either of them will reduce the BER of the received signal. Therefore, for ease of observation, in the following simulations, we let $\gamma_p = \gamma_a = \gamma_b$ and $\gamma_d = 10\,\mathrm{dB}$.

In Figure 5, we analyze the BER of Eve. The trend of curves with respect to SNR is similar to that of the former. Note that, with the increase of d, the deterioration of Eve's BER performance is highly significant. Especially when $d = 0.4\lambda$, Eve's received signal is almost all wrong. As a common channel environment in 2.4 GHz band, we can infer that $d = 0.4\lambda = (0.4 \times 3 \times 10^8/(2.4 \times 10^9)) = 5\,\mathrm{cm}$, and it is impractical for Eve to hide itself at such a close distance in our scheme. In Figures 4 and 5, the black-dashed lines represent the numerical results calculated by (4) and (5). As can be observed from the figures, the simulation and numerical results match very well.

Figures 6 and 7 show the channel capacity of equivalent interference channel of Alice-Bob and Alice-Eve, where C_{AB} and C_{AE} are calculated according to (17) and (18). According to Figure 6, one can see that the increase in γ_p significantly improves C_{AB}, and, for different γ_p, q is different when C_{AB} is the maximum. Therefore, to maximize C_{AB}, q should be dynamically adjusted according to current γ_p and γ_d. Figure 7 is similar to Figure 5, where C_{AE} is mainly affected by d. It can be inferred that the channel correlation of Alice-Bob and Alice-Eve is reduced due to larger d, which leads to a higher BER and a lower channel capacity of Eve. When $d = 0.4\lambda$, the keys are almost completely different and more interference is added to the equivalent interference channel of Eve, which results in Eve not receiving any useful information from Alice. In addition, we can also find that even if Bob is in an extremely harsh environment, such as $d = 0.1\lambda$, C_{AB} is still larger than C_{AE}.

6.2. Performance Comparison. In this subsection, we compare the performance difference between the proposed scheme and the existing schemes through simulation. First, we compare the security capacity of the proposed method with the fixed quantization precision method in [22–26] in Figure 8. We assume that Eve fully knows the SNR of Alice and Bob and uses the same strategy to adjust or fix q. As shown in Figure 8, the

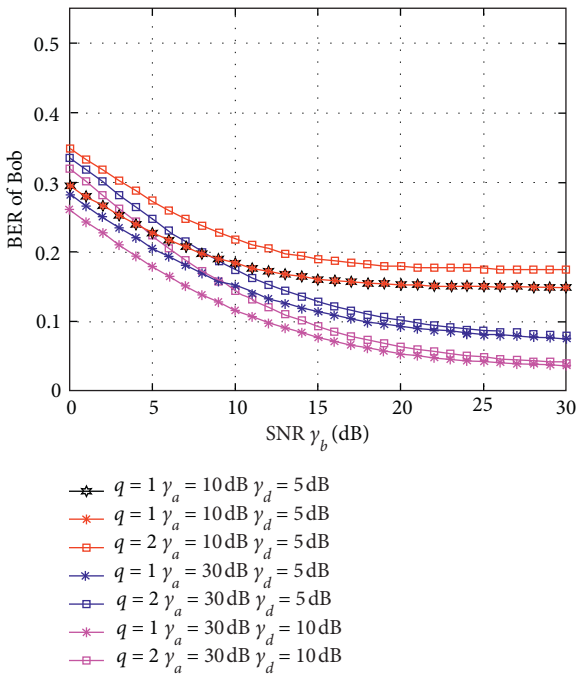

Figure 4: BER of Bob's received signal.

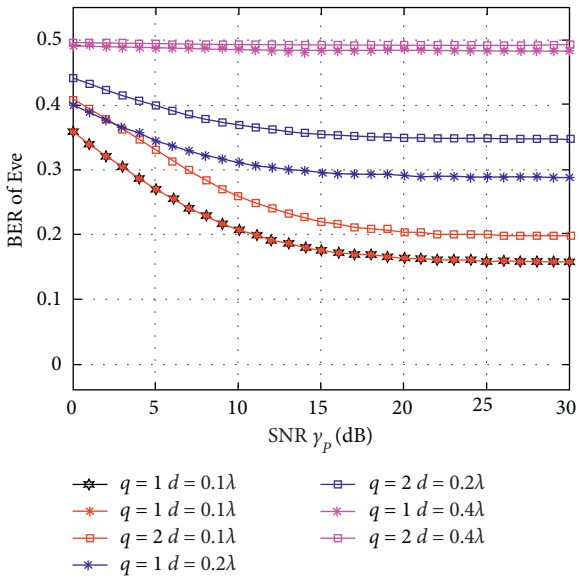

Figure 5: BER of Eve's received signal with y_d = 10 dB.

dynamic q selection method according to (19) can obtain the largest C_s in the entire γ_p interval, while the existing methods can only obtain the maximum C_s within a certain SNR interval. This result means that even if our strategy is copied by Eve, it can still reach a higher upper for secure transmission rate because it is more adaptable to a real-time changing channel environment. In addition, although the decrease of Eve-Bob distance will slightly reduce C_s, it does not have a significant impact on our optimization method of C_{AB}.

Then, we take polar code as an example to simulate the BER performance loss of the scheme in Figure 9. The

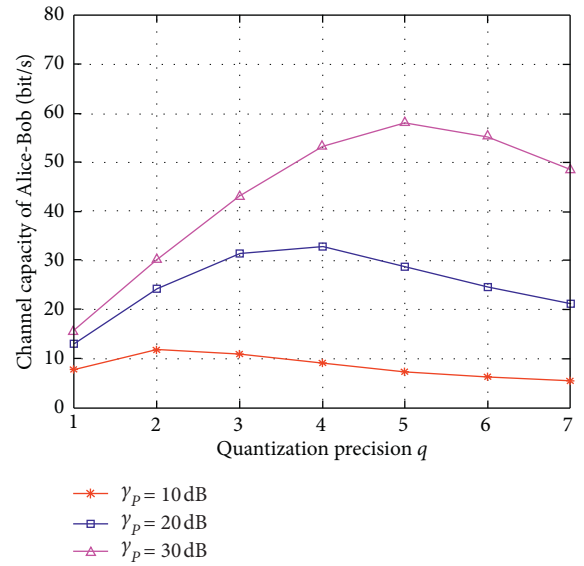

Figure 6: Channel capacity of Alice-Bob with y_d = 10 dB and t_s = 0.1 s.

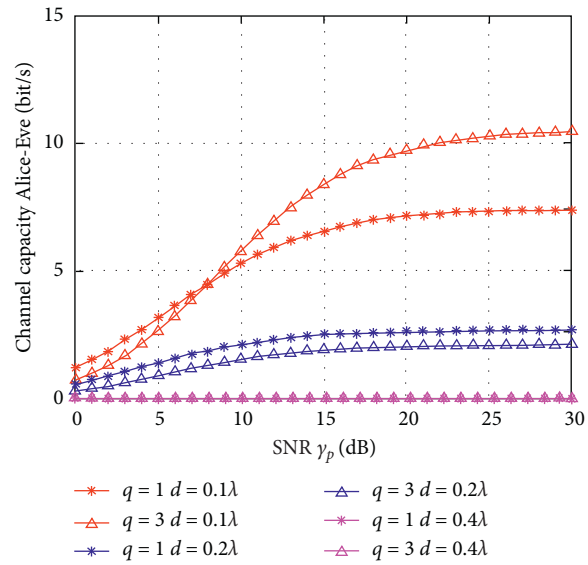

Figure 7: Channel capacity of Alice-Eve with γ_d = 10 dB and t_s = 0.1 s.

relevant codes refer to the application in MATLAB 5G Toolbox. In this simulation, $L_m = 100$ and $\eta = 0.33$. For comparison, we also simulate the decoded BER of Bob without applying the scrambling method. If we take decoded BER $\leq 10^{-6}$ as the reference standard, one can see that, in the case of γ_p = 30 dB, the decoding BER performance deteriorates by less than one dB. In the case of γ_p = 20 dB, the decoding BER performance deteriorates by less than 3 dB. Overall, this kind of BER performance loss is acceptable for Bob. For Eve, the BER cannot be reduced by decoding because the initial receiving BER is too large to correct error bits.

For comparison, we analyze the error reconciliation efficiency. Figures 10(a) and 10(b) show the trend of ζ versus various γ_p and η. As can be observed, the scheme based on

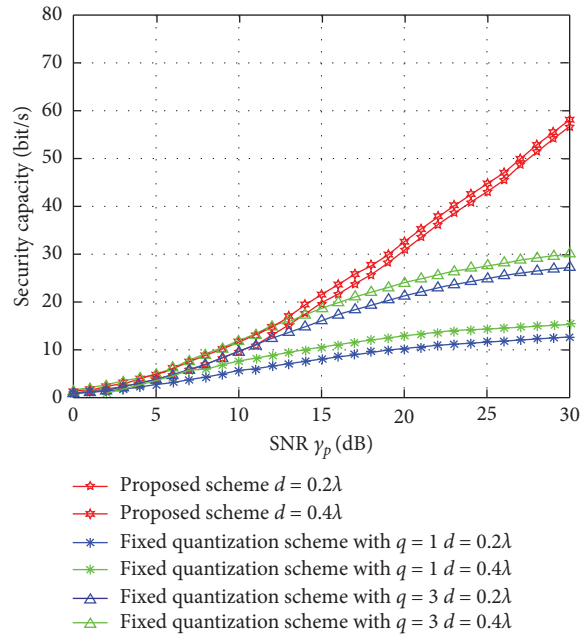

Figure 8: Security capacity with $\gamma_d = 10$ dB and $t_s = 0.1$ s.

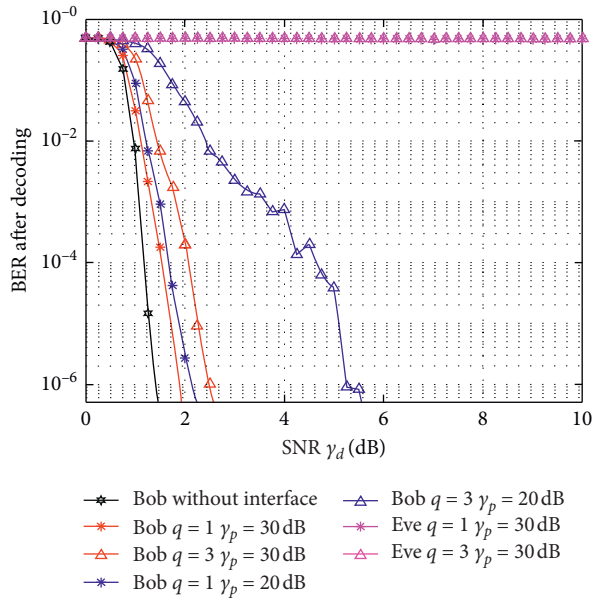

Figure 9: BER after decoding of Bob and Eve.

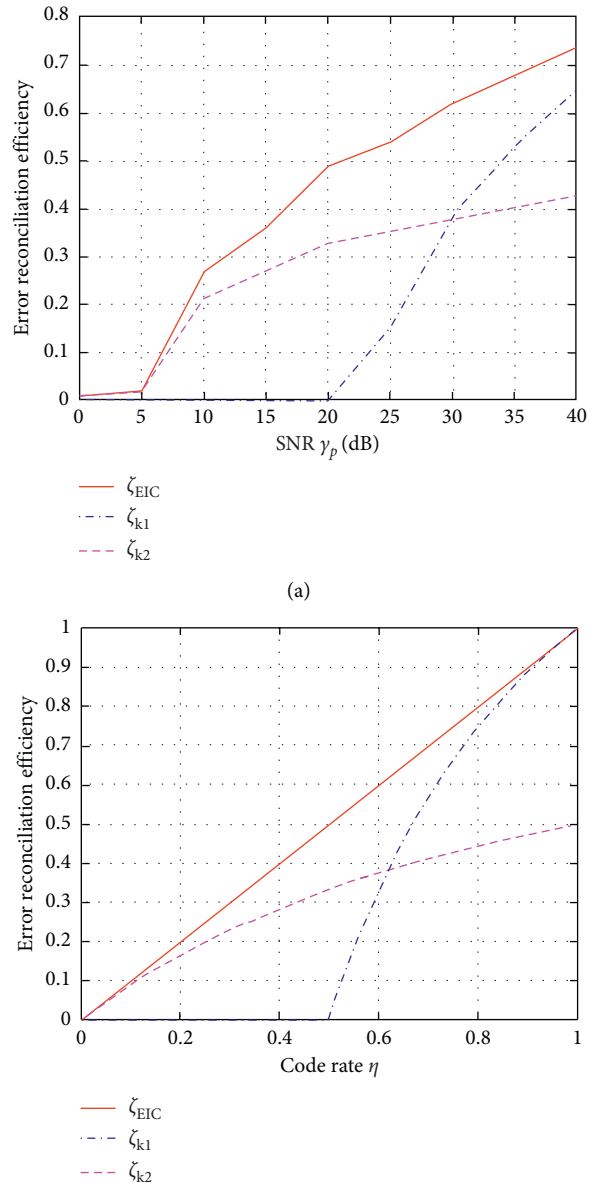

Figure 10: Comparison of error reconciliation efficiency. (a)ζ for various γ_p when polar code is used and the decoded is BER $\leq 10^{-6}$. (b)ζ for various η when linear block code is used

EIC has higher error reconciliation efficiency because it does not send any additional reconciliation signals. Note that when η is less than 0.5, we have $\zeta_{k1} = 0$. This is because, for a linear block code such as BCH, when $\eta \leq 0.5$, there is a one-to-one mapping relationship between the check bits and the key bits. Sending the check bits under this condition will leak all key bits to Eve [18]. Moreover, the fixed mapping relationship between the check bits and the information bits always exists even if other channel coding methods are used. When η is close to 1, ζ_{k1} is close to EIC-based scheme, but ζ_{k2} approaches 0.5. This is because the condition of $\eta = 1$ implies that no information reconciliation is needed to correct the key bits. At this time, sending a useless reconciliation signal of the same length as the confidential information will reduce the efficiency by half. Therefore, these results indicate that the scheme based on EIC is more cost-saving and has higher error reconciliation efficiency.

7. Conclusion and Future Work

This paper proposes a novel secure communication scheme based on equivalent interference channel assisted by physical layer secret keys to improve efficiency. The proposed scheme scrambles the encoded signal with asymmetric physical layer keys and uses channel coding to correct the error bits caused

by the different keys and the traditional noise, so there is no need to send additional signals for information reconciliation. The quantization precision is adjusted according to the expected channel capacity, and the correctness of the confidential information is verified by CRC, so there is no need to send signals for quantization or consistency check. The expressions of BER, channel capacity, and security capacity were deduced and the simulation results prove that even when Eve is very close to the legal parties, our scheme is still available. Finally, results for the performance comparison are shown, which indicate that the proposed scheme has superior performance on the security capacity and the error reconciliation efficiency, although BER slightly increases.

For future work, we will investigate the problem of maximizing the security capacity under limited transmission power and quantification precision. On the other hand, optimizing secure transmission rate under a certain channel coding condition can be considered. In addition, the single-antenna secure communication system in this paper can be extended to MIMO system.

Appendix

A. Proof of Theorem 1

As shown in Table 2, when performing 1-bit quantization of the channel gain of the i-th received pilot signal, the quantization threshold should be 0, and the real and imaginary parts of the shared random source will be quantized into key bits, respectively. Here, we first take the real part as an example and denote by $f_{\mathrm{Re}(h_{\mathrm{AB},i})}(s)$ the probability density function of $\mathrm{Re}(h_{\mathrm{AB},i})$; then $\Pr[\mathrm{Re}(\widehat{h}_{\mathrm{A},i})<0, \mathrm{Re}(\widehat{h}_{\mathrm{B},i})>0 \mid \mathrm{Re}(h_{\mathrm{AB},i})>0]$ can be calculated as (A.1), which is shown at the top of the next page, where (a) holds due to the fact that $n_{A,i}$ and $n_{B,i}$ are independent; (b) follows Gauss error function. Similarly, the BMR of Alice and Eve can be obtained as

$$\begin{aligned}
&\Pr\left[\mathrm{Re}\left(\widehat{h}_{A,i}\right)<0, \mathrm{Re}\left(\widehat{h}_{B,i}\right)>0 \,\middle|\, \mathrm{Re}\left(h_{AB,i}\right)>0\right] \\
&= \int_0^{\infty} \Pr\left[\mathrm{Re}\left(\widehat{h}_{A,i}\right)<0, \mathrm{Re}\left(\widehat{h}_{B,i}\right)>0 \,\middle|\, \mathrm{Re}\left(h_{AB,i}\right)=s\right] f_{\mathrm{Re}\left(h_{AB,i}\right)}(s)\mathrm{d}s \\
&\overset{(a)}{=} \int_0^{\infty} \Pr\left[\mathrm{Re}\left(n_{A,i}\right)<-s\right]\Pr\left[\mathrm{Re}\left(n_{B,i}\right)>-s\right] f_{\mathrm{Re}\left(h_{AB,i}\right)}(s)\mathrm{d}s \\
&\overset{(b)}{=} \int_0^{\infty}\left[\frac{1}{2}+\frac{1}{2}\mathrm{erf}\left(\sqrt{\frac{s^2\sigma_h^2\sigma_a^2}{2\sigma_n^2}}\right)\right]\left[\frac{1}{2}-\frac{1}{2}\mathrm{erf}\left(\sqrt{\frac{s^2\sigma_h^2\sigma_b^2}{2\sigma_n^2}}\right)\right]\frac{1}{\sqrt{2\pi\sigma_h^2}}\exp\left(\frac{-s^2}{2}\right)\mathrm{d}s \\
&= \frac{1}{8}-\frac{1}{4\sqrt{2\pi\sigma_h^2}}\int_0^{\infty}\mathrm{erf}\left(\sqrt{\frac{\gamma_a s^2}{2}}\right)\mathrm{erf}\left(\sqrt{\frac{\gamma_b s^2}{2}}\right)\exp\left(\frac{-s^2}{2}\right)\mathrm{d}s.
\end{aligned} \tag{A.1}$$

$$\begin{aligned}
&\Pr\left[\mathrm{Re}\left(\widehat{h}_{A,i}\right)<0, \mathrm{Re}\left(\widehat{h}_{E,i}\right)>0 \,\middle|\, \mathrm{Re}\left(h_{\mathrm{AB},i}\right)>0\right] \\
&= \frac{1}{8}-\frac{1}{4\sqrt{2\pi}}\int_0^{\infty}\mathrm{erf}\left(\sqrt{\frac{\gamma_b s^2}{2}}\right)\times\mathrm{erf}\left(\sqrt{\frac{\gamma_a\rho^2 s^2}{2\left(\gamma_a-\rho^2\gamma_a+1\right)}}\right)\exp\left(\frac{-s^2}{2}\right)\mathrm{d}s.
\end{aligned} \tag{A.2}$$

Due to the symmetry of the zero-mean Gaussian random variable, it can be inferred that (A.1) have the following relationship:

$$\begin{aligned}
&\Pr\left[\mathrm{Re}\left(\widehat{h}_{A,i}\right)<0, \mathrm{Re}\left(\widehat{h}_{B,i}\right)>0 \,\middle|\, \mathrm{Re}\left(h_{\mathrm{AB},i}\right)>0\right] \\
&= \Pr\left[\mathrm{Re}\left(\widehat{h}_{A,i}\right)>0, \mathrm{Re}\left(\widehat{h}_{B,i}\right)<0 \,\middle|\, \mathrm{Re}\left(h_{\mathrm{AB},i}\right)>0\right] \\
&= \Pr\left[\mathrm{Re}\left(\widehat{h}_{A,i}\right)<0, \mathrm{Re}\left(\widehat{h}_{B,i}\right)>0 \,\middle|\, \mathrm{Re}\left(h_{\mathrm{AB},i}\right)<0\right] \\
&= \Pr\left[\mathrm{Re}\left(\widehat{h}_{A,i}\right)>0, \mathrm{Re}\left(\widehat{h}_{B,i}\right)<0 \,\middle|\, \mathrm{Re}\left(h_{\mathrm{AB},i}\right)<0\right].
\end{aligned} \tag{A.3}$$

For the error probability of Alice and Eve, it can be inferred that (A.2) have the following relationship:

$$\begin{aligned}
&\Pr\left[\mathrm{Re}\left(\widehat{h}_{\mathrm{A},i}\right)<0, \mathrm{Re}\left(\widehat{h}_{\mathrm{E},i}\right)>0 \,\middle|\, \mathrm{Re}\left(h_{\mathrm{AB},i}\right)>0\right] \\
&\quad = \Pr\left[\mathrm{Re}\left(\widehat{h}_{\mathrm{A},i}\right)>0, \mathrm{Re}\left(\widehat{h}_{\mathrm{E},i}\right)<0 \,\middle|\, \mathrm{Re}\left(h_{\mathrm{AB},i}\right)>0\right], \\
&\Pr\left[\mathrm{Re}\left(\widehat{h}_{\mathrm{A},i}\right)<0, \mathrm{Re}\left(\widehat{h}_{\mathrm{E},i}\right)>0 \,\middle|\, \mathrm{Re}\left(h_{\mathrm{AB},i}\right)<0\right] \\
&\quad = \Pr\left[\mathrm{Re}\left(\widehat{h}_{\mathrm{A},i}\right)>0, \mathrm{Re}\left(\widehat{h}_{\mathrm{E},i}\right)<0 \,\middle|\, \mathrm{Re}\left(h_{\mathrm{AB},i}\right)<0\right].
\end{aligned} \tag{A.4}$$

Then $P_{\mathrm{AB}}(\gamma_a, \gamma_b, 1)$ and $P_{\mathrm{AE}}(\gamma_a, \gamma_b, 1, \rho)$ can be calculated as

$$\begin{aligned} P_{\mathrm{AB}}(\gamma_a, \gamma_b, 1) &= 4\Pr\left[\mathrm{Re}\left(\widehat{h}_{\mathrm{A},i}\right) < 0, \mathrm{Re}\left(\widehat{h}_{\mathrm{B},i}\right) > 0 | \mathrm{Re}\left(h_{\mathrm{AB},i}\right) > 0\right] \\ &= \frac{1}{2} - \frac{1}{\sqrt{2\pi}} \int_0^{\infty} \mathrm{erf}\left(\sqrt{\frac{\gamma_a s^2}{2}}\right) \mathrm{erf}\left(\sqrt{\frac{\gamma_b s^2}{2}}\right) \exp\left(\frac{-s^2}{2}\right) \mathrm{d}s, \\ P_{\mathrm{AE}}(\gamma_a, \gamma_b, 1, \rho) &= 2\Pr\left[\mathrm{Re}\left(\widehat{h}_{\mathrm{A},i}\right) < 0, \mathrm{Re}\left(\widehat{h}_{\mathrm{E},i}\right) > 0 | \mathrm{Re}\left(h_{\mathrm{AB},i}\right) > 0\right] \\ &\quad + 2\Pr\left[\mathrm{Re}\left(\widehat{h}_{\mathrm{A},i}\right) < 0, \mathrm{Re}\left(\widehat{h}_{\mathrm{E},i}\right) > 0 | \mathrm{Re}\left(h_{\mathrm{AB},i}\right) < 0\right] \\ &= \frac{1}{8} - \frac{1}{4\sqrt{2\pi}} \int_0^{\infty} \mathrm{erf}\left(\sqrt{\frac{\gamma_b s^2}{2}}\right) \times \mathrm{erf}\left(\sqrt{\frac{\gamma_a \rho^2 s^2}{2\left(\gamma_a - \rho^2 \gamma_a + 1\right)}}\right) \exp\left(\frac{-s^2}{2}\right) \mathrm{d}s \\ &\overset{(a)}{\geq} P_{\mathrm{AE}}(\gamma_a, \gamma_b, 1, 1) \overset{(b)}{=} P_{\mathrm{AB}}(\gamma_a, \gamma_b, 1). \end{aligned} \tag{A.5}$$

where (a) holds due to the fact that $p_{\mathrm{AE}}(\gamma_a, \gamma_b, 1, \rho)$ decreases with the increase of ρ; and (b) holds due to the fact that $h_{\mathrm{AB},i} = h_{\mathrm{AE},i}$, when $\rho = 1$.

So Theorem 1 is proved.

B. Proof of Theorem 2

For ease of analysis, we add a pair of symmetrical virtual scramblers at both ends of the equivalent interference channel. As shown in Figure 11, it is a simplified flow-process diagram of the scheme and the two virtual scramblers are, respectively, located before scrambling and after descrambling. They use the same secret key $\mathbf{K}_{\mathrm{B}}$ and the scrambling method is XOR, so channel $(\mathsf{X}_v, p(y_v \mid x_v), \mathsf{Y}_v)$ is also a DMC where the new input is $x_v \in \mathsf{X}_v$ and output is $y_v \in \mathsf{Y}_v$. Since there is no new noise or interference added, the channel transition probability is unchanged; that is, $p(y_v \mid x_v) = p(y \mid x)$. According to the principles over the binary field, it can be inferred that $Y_s = Y_v$ and $p(y_s \mid x_v) = p(y_v \mid x_v) = p(y \mid x)$. Let the input probability satisfy $p(x_v) = p(x)$; then the capacity of Alice-Bob C_{AB} is given by

$$\begin{aligned} C_{\mathrm{AB}} &= \max_{P(x)} I(X;Y) \\ &= \max_{P(x)} \left(\sum_{Y} P(y) \log \frac{1}{P(y)} - \sum_{X} P(x) \sum_{Y} p(y \mid x) \log \frac{1}{p(y \mid x)} \right) \\ &= \max_{P(x_v)} \left(\sum_{y_s} P(y_s) \log \frac{1}{p(y_s)} - \sum_{X_v} P(x_v) \sum_{Y_s} p\left(y_s \mid x_v\right) \log \frac{1}{p\left(y_s \mid x_v\right)} \right) \\ &= \max_{P(x_v)} I\left(X_v; Y_s\right). \end{aligned} \tag{B.1}$$

We have that $P(y_s) = \sum_{X_v} P(x_v) p(y_s \mid x_v)$ and log is a base-2 logarithm. In this case, the solution for the capacity of channel $(\mathsf{X}, p(y \mid x), \mathsf{Y})$ is converted to the channel $(\mathsf{X}_v, p(y_s \mid x_v), \mathsf{Y}_s)$, which can be equivalent to a virtual cascade channel that contains two parts. For the former $(\mathsf{X}_v, p(x_s \mid x_v), \mathsf{X}_s)$, we have

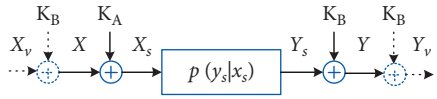

FIGURE 11: The simplified process of the proposed scheme with virtual scramblers attached.

$$\begin{aligned}
&\Pr\left(x_s = 1 \mid x_v = 1\right)\\
&= \Pr\left(k'_{\mathrm{B},j} \oplus x_v \oplus k'_{\mathrm{A},j} = 1 \mid x_v = 1\right)\\
&= \Pr\left(k'_{\mathrm{B},j} \oplus x_v \oplus k'_{\mathrm{A},j} = 1 \,\middle|\, k_{\mathrm{A},j}{}' \oplus x_v \oplus k'_{\mathrm{A},j} = 1\right)\\
&= \Pr\left(k'_{\mathrm{B},j} = 1 \,\middle|\, k'_{\mathrm{A},j} = 1\right)\\
&= 1 - P_{\mathrm{AB}}(\gamma_a, \gamma_b, q).
\end{aligned} \tag{B.2}$$

Similarly, $\Pr(x_s = 0 \mid x_v = 0) = 1 - P_{\mathrm{AB}}(\gamma_a, \gamma_b, q)$ and $\Pr(x_s = 1 \mid x_v = 0) = \Pr(x_s = 0 \mid x_v = 1) = P_{\mathrm{AB}}(\gamma_a, \gamma_b, q)$. So, the BER of $(\mathsf{X}_v, p(x_s \mid x_v), \mathsf{X}_s)$ is $P_{\mathrm{AB}}(\gamma_a, \gamma_b, q)$. For the latter of the cascade channel, that is, $(\mathsf{X}_s, p(y_s \mid x_s), \mathsf{Y}_s)$, the BER is $P_d(\gamma_d)$. Since $p(y_s \mid x_s)$ is only related to the noise in data signals and $p(x_s|x_v)$ is only related to the estimation error of pilot signals, Y_s is determined by X_s and $p(y_s \mid x_s)$. Thus, $X_v - X_s - Y_s$ is a Markov chain that satisfies

$$p\left(y_s \mid x_s x_v\right) = p\left(y_s \mid x_v\right) = \sum_{X_s} p\left(y_s \mid x_s\right) p\left(x_s \mid x_v\right). \tag{B.3}$$

The BER of channel $(\mathsf{X}, p(y \mid x), \mathsf{Y})$ (i.e., channel $(\mathsf{X}_v, p(y_s \mid x_v), \mathsf{Y}_s)$) is

$$\begin{aligned}
P_{xy}(\gamma_d, \gamma_a, \gamma_b, q) &= P_d(\gamma_d) + P_{\mathrm{AB}}(\gamma_a, \gamma_b, q)\\
&\quad - 2P_{\mathrm{AB}}(\gamma_a, \gamma_b, q) P_d(\gamma_d).
\end{aligned} \tag{B.4}$$

Assume that $\Pr(x_v = 0) = \omega = 1 - \overline{\omega}$ and $P_{xy}(\gamma_d, \gamma_a, \gamma_b, q) = \beta = 1 - \overline{\beta}$; then, combined with (B.2), (B.3), and (B.4), we can rewrite (B.1) as (B.6), which is shown at the bottom of the page, where $H(\cdot)$ is the entropy function of the (0, 1) region and it is convex with respect to ω. When $\omega = 0.5$, (B.6) has the maximum value as follows:

$$C_{\mathrm{AB}} = 1 - H\left(P_{xy}(\gamma_d, \gamma_a, \gamma_b, q)\right) \text{bits/channel use}. \tag{B.5}$$

Since the secret keys are equally distributing, $\omega = 0.5$ is equivalent to $\Pr(x = 0) = \Pr(x = 1) = 0.5$.

So Theorem 2 is proved:

$$\begin{aligned}
C_{\mathrm{AB}} &= \max_{P(x_v)} \left\{ \left[(\omega\overline{\beta} + \overline{\omega}\beta) \log \frac{1}{(\omega\overline{\beta} + \overline{\omega}\beta)} + (\omega\beta + \overline{\omega}\overline{\beta}) \log \frac{1}{(\omega\beta + \overline{\omega}\overline{\beta})} \right] - \left[\beta \log \frac{1}{\beta} + \overline{\beta} \log \frac{1}{\overline{\beta}} \right] \right\}\\
&= \max_{P(x_v)} \left[H\left(\omega P_{xy}(\gamma_d, \gamma_a, \gamma_b, q) + \overline{\omega}\left(1 - p_{xy}(\gamma_d, \gamma_a, \gamma_b, q)\right)\right) - H\left(P_{xy}(\gamma_d, \gamma_a, \gamma_b, q)\right) \right].
\end{aligned} \tag{B.6}$$

C. Proof of Corollary 1

(13) can be rewritten as

$$\begin{aligned}
\Pr(\mathbf{K}_{\mathrm{A}} = \mathbf{K}_{\mathrm{E}}) &= \prod_i^N \Pr\left(k_{\mathrm{A},i} = k_{\mathrm{E},i}\right)\\
&= \prod_i^N \sum_j^q P_{u,j}^2 = \prod_i^N \sum_j^q P_{u,j} 2^{\log P_{u,j}}\\
&\overset{(a)}{\geq} \prod_i^N 2^{\sum_j^q P_{u,j} \log P_{u,j}} = \prod_i^N 2^{-H(k_{u,i})} \overset{(b)}{=} \left[2^{-H(k_u)}\right]^N,
\end{aligned} \tag{C.1}$$

where (a) is due to Jensen's inequality; (b) is because key quantization is an independent and repeated experiment process and $k_{\mathrm{u},i}$ are i.i.d. random variables.

So Corollary 1 is proved.

Data Availability

All data and results are generated by MATLAB, and they have been stored in the supplementary information files. Additional information can be obtained from the corresponding author upon request via email.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the National Key Research and Development Program of China under Grant 2017YFB0801903, in part by the National Natural Science Foundation of China under Grants 61701538, 61601514, 61501516, and 61521003, in part by Doctoral Fund of Ministry of Education of China (2019M663994), and in part by the National Defense Science and Technology Innovation Special Zone of China.

References

[1] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.

[2] P. Jilna and D. P. Pattathil, "A key management technique based on elliptic curves for static wireless sensor networks," *Security and Communication Networks*, vol. 8, no. 18, pp. 3726–3738, 2015.

[3] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," in *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 357–370, Cambridge, MA, USA, 2004.

[4] W. Chen, S. Jian, L. Qi, Y. Ren, and T. Li, "A novel security scheme based on instant encrypted transmission for internet of things," *Security and Communication Networks*, vol. 2018, Article ID 3680851, 7 pages, 2018.

[5] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott, "Security and privacy in device-to-device (D2D) communication: a review," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1054–1079, 2017.

[6] G. Oliveira, E. Fernández, S. Mafra, S. Montejo-Sánchez, and C. Azurdia-Meza, "Optimal improper Gaussian signaling for physical layer security in cognitive radio networks," *Security and Communication Networks*, vol. 2018, Article ID 9065856, 13 pages, 2018.

[7] Y. E. H. Shehadeh and D. Hogrefe, "A survey on secret key generation mechanisms on the physical layer in wireless networks," *Security and Communication Networks*, vol. 8, no. 2, pp. 332–341, 2015.

[8] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[9] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[10] M. Waqas, M. Ahmed, Y. Li, D. Jin, and S. Chen, "Social-aware secret key generation for secure device-to-device communication via trusted and non-trusted relays," *IEEE Transactions on Wireless Communications*, vol. 17, no. 6, pp. 3918–3930, 2013.

[11] J. Huang and T. Jiang, "Secret key generation exploiting ultra-wideband indoor wireless channel characteristics," *Security and Communication Networks*, vol. 8, no. 13, pp. 2329–2337, 2015.

[12] Y. Peng, P. Wang, W. Xiang, and Y. Li, "Secret key generation based on estimated channel state information for TDD-OFDM systems over fading channels," *IEEE Transactions on Wireless Communications*, vol. 16, no. 8, pp. 5176–5186, 2017.

[13] L. Cheng, W. Li, D. Ma, J. Wei, and X. Liu, "Moving window scheme for extracting secret keys in stationary environments," *IET Communications*, vol. 10, no. 16, pp. 2206–2214, 2016.

[14] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Proceedings of the Theory and Application of Cryptographic Techniques*, pp. 410–423, Lofthus, Norway, May 1994.

[15] J. Zhang, T. Q. Duong, A. Marshall et al., "Key generation from wireless channels: a review," *IEEE Access*, vol. 4, pp. 2206–2214, 2016.

[16] J. Qiao, H. Zhang, F. Zhao, and D. Yuan, "Secure transmission and self-energy recycling with partial eavesdropper CSI," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 7, pp. 1531–1543, 2018.

[17] M. Waqas, M. Ahmed, J. Zhang, and Y. Li, "Confidential information ensurance through physical layer security in device-to-device communication," in *Proceedings of the Global Communications Conference*, pp. 1–7, Abu Dhabi, UAE, December 2018.

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

[19] 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 Transactions on Communications*, vol. 66, no. 7, pp. 3022–3034, 2018.

[20] M. Yuliana, W. Wirawan, and S. Suwadi, "Performance analysis of loss multilevel quantization on the secret key generation scheme in indoor wireless environment," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 9, no. 1, pp. 100–108, 2019.

[21] H. Jin, K. Huang, S. Xiao, Y. Lou, X. Xu, and Y. Chen, "A two-layer secure quantization algorithm for secret key generation with correlated eavesdropping channel," *IEEE Access*, vol. 7, pp. 26480–26487, 2019.

[22] Q. Dai, K. Huang, L. Jin, and H. Song, "Physical-layer authentication and key distribution mechanism based on equivalent channel," *Scientia Sinica Informationis*, vol. 44, no. 12, pp. 1580–1592, 2014.

[23] J. Choi, "A coding approach with key-channel randomization for physical-layer authentication," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 175–185, 2019.

[24] H. Taha and E. Alsusa, "Secret key exchange and authentication via randomized spatial modulation and phase shifting," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 3, pp. 2165–2177, 2018.

[25] L. Peng, G. Li, J. Zhang, and A. Hu, "Securing M2M transmissions using nonreconciled secret keys generated from wireless channels," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, Abu Dhabi, UAE, December 2018.

[26] X. Hu, L. Jin, and Z. Zhong, "A scrambling scheme based on random wireless channel characteristics for secure transmission," in *Proceedings of the 12th International Conference on Communication Software and Networks (ICCSN)*, pp. 29–38, Chongqing, China, June 2020.

[27] M. Ahmed, H. Shi, X. Chen, Y. Li, M. Waqas, and D. Jin, "Socially aware secrecy-ensured resource allocation in D2D underlay communication: an overlapping coalitional game scheme," *IEEE Transactions on Wireless Communications*, vol. 17, no. 6, pp. 4118–4133, 2018.

[28] L. Jin, S. Zhang, Y. Lou, X. Xu, and Z. Zhong, "Secret key generation with cross multiplication of two-way random signals," *IEEE Access*, vol. 7, pp. 113065–113080, 2019.

[29] D. S. Michalopoulos, H. A. Suraweera, G. K. Karagiannidis, and R. Schober, "Amplify-and-forward relay selection with outdated channel estimates," *IEEE Transactions on Communications*, vol. 60, no. 5, pp. 1278–1290, 2012.

[30] A. Assalini, E. Dall'Anese, and S. Pupolin, "Linear MMSE MIMO channel estimation with imperfect channel covariance information," in *Proceedings of the IEEE International Conference on Communications (ICC)*, pp. 1–5, Dresden, Germany, June 2009.

[31] O. A. Topal, G. K. Kurt, and B. Özbek, "Key error rates in physical layer key generation: theoretical analysis and measurement-based verification," *IEEE Wireless Communications Letters*, vol. 6, no. 6, pp. 766–769, 2017.

[32] B. Chen, C. Zhu, W. Li, J. Wei, V. C. M. Leung, and L. T. Yang, "Original symbol phase rotated secure transmission against powerful massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 3016–3025, 2016.

[33] L. Hu, X. Zheng, and C. Chen, "Physical layer security in nonorthogonal multiple access wireless network with jammer selection," *Security and Communication Networks*, vol. 2019, Article ID 7869317, 9 pages, 2019.

[34] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[35] N. Islam, O. Graur, A. Filip, and W. Henkel, "LDPC code design aspects for physical layer key reconciliation," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM)*, pp. 1–7, San Diego, CA, USA, December 2015.

[36] D. Chen, Z. Qin, X. Mao, P. Yang, Z. Qin, and R. Wang, "SmokeGrenade: an efficient key generation protocol with artificial interference," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1731–1745, 2013.

[37] Z. Feng and L. Jingling, "Performance of an improved one-way error reconciliation protocol based on key redistribution," *China Communications*, vol. 11, no. 6, pp. 63–70, 2014.

[38] 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.

[39] S. Zhang, L. Jin, S. Zhu, K. Huang, and Z. Zhong, "Information reconciliation based on systematic secure polar code for secret key generation," in *Proceedings of the 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, pp. 1–6, Chicago, IL, USA, August 2018.

[40] J. Zhang, A. Marshall, and L. Hanzo, "Channel-envelope differencing eliminates secret key correlation: LoRa-based key generation in low power wide area networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 12462–12466, 2018.