Research Article

Scramble-Based Secret Key Generation Algorithm in Physical Layer Security

Dan Wang, Feng Chen, Yongtai Chen, Mingjie Zheng, and Jingui Zheng

College of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Correspondence should be addressed to Feng Chen; s200131084@stu.cqupt.edu.cn

Received 28 April 2022; Revised 15 August 2022; Accepted 10 September 2022; Published 3 October 2022

Academic Editor: Jose M. Barcelo-Ordinas

Copyright © 2022 Dan Wang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

As a new way to enhance wireless communication security, secret key generation based on physical layer channel characteristics has emerged. In this paper, we propose a novel secret key generation algorithm based on wireless channel characteristics for orthogonal frequency division multiplexing (OFDM) communication systems. The mean quantization algorithm is applied to quantize the real part and imaginary part of OFDM subcarriers, respectively, which can significantly increase the length of the generated secret key in the OFDM system. To reduce the consistency between the secret keys generated by the eavesdropper and the legitimate communication nodes, a processing method by taking the subcarrier phase as initialization of a scrambling code and scrambling the quantized result is proposed. The simulation and test results show that compared with the existing research, the proposed algorithm can improve the key generation rate (KGR), reduce the key mismatch rate (KMR) and complexity, maintain high randomness, and disturb the eavesdroppers.

1. Introduction

Secret key generation technology is becoming increasingly popular in wireless communication devices, especially smartphones and other smart devices. It plays an increasingly important role in people’s daily lives. To ensure the confidentiality and security of wireless communication, classical encryption-based techniques are used in the upper layers [1]. Unlike traditional upper-layer keys, physical layer secret key generation techniques do not require complicated hash calculations or any infrastructure for distribution or management [2]. This technique can be used in wireless communication devices with limited computing power, or even by eavesdroppers with unlimited computing power. Furthermore, in a multipath scattering environment, if the distance between the eavesdropper (Eve) and the legitimate node (Alice/Bob) is greater than half a wavelength, they will experience uncorrelated channels [3]. As a result, the eavesdropper (Eve) is unable to obtain the same as the one obtained by the legitimate node (Alice/Bob). As well as the above-given advantages, physical layer secret key generation has been gaining attention as a lightweight security tool, especially in applications such as V2X, IoT, and smart homes. The physical layer secret key generation techniques based on the randomness and reciprocity of wireless channels are gradually becoming more effective as a complement to upper layer encryption methods.

Numerous physical layer secret key generation schemes have been proposed for orthogonal frequency division multiplexing (OFDM)-based systems. These schemes generally used channel impulse responses (CIR), phase, or amplitude of the received signal to generate secret keys [4]. The authors of [5] proposed an OFDM subcarrier index selection (OFDM-SIS) which maximized the signal-to-noise ratio at legitimate receivers and an adaptive subcarrier interleaving scheme that reduced the correlations among subcarriers. The authors of [6] proposed channel status information (CSI) based key generation for OFDM indoor and outdoor systems. In [7], signal space diversity is used to separate the in-phase and orthogonal components of complex modulated symbols to increase diversity gain over Eve, thereby improving the confidentiality of OFDM...
systems. The authors of [8] studied key generation for OFDM systems with the phase variation of channel frequency response based on time-varying channels. The legitimate communication nodes in the above schemes mainly use CIR, index, or received signal strength (RSS) to generate the same random secret key. However, all these methods have some limitations [9]. For example, a faster channel probing rate will produce a higher key generation rate but may reduce temporal redundancy and randomness, while a higher quantization level will produce a higher key generation rate but a higher key mismatch rate, especially in a low signal-to-noise environment it could become more obvious. On the other hand, some of the above-mentioned literature can take into consideration the key generation rate and key mismatch rate, but the computational complexity increases as a result. On the other hand, while pursuing high performance in key generation rate and key mismatch rate, the randomness of secret keys cannot be compromised and must be maintained at a high level.

In general, most of the current secret key generation techniques are based on received signal strength (RSS) and channel state information (CSI), where channel impulse response (CIR) is one of the most commonly used CSI. The RSS is a coarse-grained channel information indicator, where only one RSS value can be obtained per packet, which imposes a limitation on the KGR. The CIR is a fine-grained channel parameter that provides detailed channel information, CSI-based systems are able to provide high KGR, and CIR has been shown to be ideal for a key generation [10]. In addition, RSS is vulnerable to predictable channel attacks in some cases, but there is experimental evidence that CSI is immune to predictable channel attacks [11]. To further improve the key generation rate of the secret key generation method as well as to reduce the key mismatch rate while maintaining the key randomness. We choose to use the real and imaginary parts of CIR to generate secret keys. In addition, in order to enhance the confidentiality of the key, the phase is used to quantize the initial value of the scrambled code and to facilitate subsequent quantization. In this paper, a novel key generation algorithm for the OFDM system is proposed. The work in this paper is summarized as follows:

(1) Generates initial secret keys by comparing the imaginary and real parts of each subcarrier with the mean of the real and imaginary parts of the entire OFDM block, respectively. It can increase the key generation rate by a large amount compared with it based on the magnitude of CIR.

(2) After the initial secret key generation, the entire OFDM block is divided into multiple subblocks. The mean phase of the subcarriers within each subblock is used as an initial value and a scrambling sequence is generated with it. Then, the secret key is scrambled with that sequence, which can effectively reduce the key leakage at the eavesdropper and improve the confidentiality of the key.

(3) We analyze the proposed algorithm’s reliability and security by using results derived from information-theoretic security theory. Simulation results show that the algorithm can significantly improve the key generation rate, further reduce key mismatch rate both in high and low SNR environments, also it passes the NIST randomness test. Finally, its computational complexity is analyzed and compared with existing algorithms.

1.1. Notations. The transpose is represented by $(·)^T$.

2. System Model and the Proposed Algorithm

2.1. System Model. As shown in Figure 1, the channel model is assumed to be a Rayleigh fading channel with $N$ exponentially fading taps. The communication system model is assumed to be SISO-OFDM with time-division duplexing (TDD). The legitimate nodes are Alice and Bob who try to communicate securely with each other by using CIR to generate secret keys in the presence of a passive eavesdropper (Eve). In addition, the CIR between Alice and Bob is denoted as $h_{AB}(t_1) \in \mathbb{C}^{1 \times N}$, the CIR between Bob and Alice is denoted as $h_{BA}(t_2) \in \mathbb{C}^{1 \times N}$, and the CIR between Alice and Eve is denoted as $h_{AE}(t_3) \in \mathbb{C}^{1 \times N}$, when the interval time between $t_1$ and $t_2$ are shorter than the coherence time $\tau (|t_1 - t_2| < \tau)$, according to the characteristic of short-time reciprocity of wireless channels [12], the radio channels experienced by both are closely correlated between $h_{AB}(t_1)$ and $h_{BA}(t_2)$, i.e., $h_{AB}(t_1) \approx h_{BA}(t_2)$.

Furthermore, we consider an eavesdropper, who tracks the legitimate nodes involved in secret key extraction. It could eavesdrop on all open discussions in the key generation process and the secret key generation algorithm with the corresponding key generation parameters. Because of the
differences in location and environment, it is assumed that the distance between Alice/Bob and Eve is greater than or equal to half a wavelength. Hence the wireless channels experienced by both are uncorrelated in the multipath fading environment, resulting in independent observations at the legitimate nodes and the eavesdropper.

Taking Alice as the transmitter, the frequency domain OFDM symbols (pilots) can be expressed as $[a_1, a_2, ..., a_M]^T \in \mathbb{C}^{M \times 1}$, where $M$ denotes the number of the pilots. The pilots are processed first, then sent to Bob and Eve through the wireless channel. In the frequency domain, the received signal $y_i \in \mathbb{C}^{M \times 1}$ of Bob or Eve can be written as follows:

$$y_i = H_i^T a + Z_i^f,$$

where the subscripts $i = [b, e]$ denote the receiver’s parameters for Bob or Eve, and the vectors $Z_i^f$ denote the Fourier transform of the additive white Gaussian noise (AWGN) with mean 0 and variance of $\sigma^2$. Furthermore, $H_i^T \in \mathbb{C}^{M \times M}$ is the channel frequency response diagonal matrix.

2.2. Proposed Algorithms. In this section, we present the detailed steps of the proposed Real and Imaginary parts-based Scrambled Key Generation (RISKG) algorithm. Among them, we use the real and imaginary parts of CSI to generate the initial secret key, and it is proved that the real and imaginary parts always have better performance than the amplitude and phase in generating the secret key. In addition, we use the mean phase of the subblock for quantization as a scrambling code initialization in order to enhance the key confidentiality, since the phase has a higher amount of mutual information between the channel of Alice to Bob and Bob to Alice compared to the amplitude and is easier to quantize [10].

The specific steps of the algorithm are as follows:

1. During the coherence time $T$ of the channel, Alice and Bob send the pilots $a = [a_1, a_2, ..., a_M]^T \in \mathbb{C}^{M \times 1}$ and $b = [b_1, b_2, ..., b_M]^T \in \mathbb{C}^{M \times 1}$ to each other for channel estimation. Taking the example of Alice sending pilots $a$ to Bob, the channel estimate at Bob/Eve can be expressed in the frequency domain as $H_i^T \in \mathbb{C}^{M \times M}$.
2. The diagonal matrix $H_i^T$ obtained at Bob/Eve is converted into a row vector $h_i$, and the procedure can be described as $h_i = [\text{diag}(H_i^T)]^T \in \mathbb{C}^{1 \times M}$.
3. After that, the vector $h_i$ is evenly divided into $s$ subblocks, i.e., $h_i = [h_i^1, h_i^2, ..., h_i^s]$, where $j = [1, 2, ..., s]$. Each subblock contains $l$ elements that $= M/s$, $h_i^j = [h_i^{1,j}, h_i^{2,j}, ..., h_i^{l,j}]$, where $k = [1, 2, ..., l]$.
4. Next, compute its real and imaginary part values for each element $h_i^{j,k}$ in each subblock $h_i^j$, which can be indicated by $R(h_i^{j,k})$ and $I(h_i^{j,k})$ respectively.

Calculate the real part mean and the imaginary part mean of all elements in the vector $h_i$:

$$\text{meanR} = \frac{\sum_{j=1}^{s} \sum_{k=1}^{l} R(h_i^{j,k})}{M},$$

$$\text{meanI} = \frac{\sum_{j=1}^{s} \sum_{k=1}^{l} I(h_i^{j,k})}{M}.$$

5. Extract the mean phase $\theta_i$ for each subblock $h_i^j$:

$$\theta_i = \frac{\sum_{j=1}^{s} \theta_i^{j,k}}{l},$$

where $\theta_i^{j,k}$ is the phase of each element $h_i^{j,k}$.
6. The initial secret key generation rule corresponding to each element $h_i^{j,k}$ within each subblock $h_i^j$ is shown as follows:

$$\text{KeyR}_{i,j,k} = \begin{cases} 0, \text{meanR} > R(h_i^{j,k}), \\ 1, \text{meanR} \leq R(h_i^{j,k}), \end{cases}$$

$$\text{KeyI}_{i,j,k} = \begin{cases} 0, \text{meanI} > I(h_i^{j,k}), \\ 1, \text{meanI} \leq I(h_i^{j,k}). \end{cases}$$

For each subblock $h_i^j$, the real part key and imaginary part key are respectively generated by $\text{KeyR}_i = \{\text{KeyR}_{i,j,k}^1, \text{KeyR}_{i,j,k}^2, ..., \text{KeyR}_{i,j,k}^{31}\}$ and $\text{KeyI}_i = \{\text{KeyI}_{i,j,k}^1, \text{KeyI}_{i,j,k}^2, ..., \text{KeyI}_{i,j,k}^{31}\}$. The initial secret key of the real part and the imaginary part of the whole vector $h_i$ can be expressed as $\text{KeyR}_i = \{\text{KeyR}_1, \text{KeyR}_2, ..., \text{KeyR}_M\}$ and $\text{KeyI}_i = \{\text{KeyI}_1, \text{KeyI}_2, ..., \text{KeyI}_M\}$.

7. The acquired phase $\theta_i$ is quantized as follows:

$$C_{1,j} = \begin{cases} 0, \pi > \theta_j \geq 0, \\ 1, 2\pi > \theta_j \geq \pi, \end{cases}$$

where $C_1$ denotes the mean phase quantization of all the elements within each subblock, $C_1 = [C_{1,1}, ..., C_{1,j}, ..., C_{1,s}]$.
8. For the sequence $C_1 = [C_{1,1}, ..., C_{1,j}, ..., C_{1,s}]$, To obtain a 31-length scrambling initialization sequence $C_2$, only the first 31 bits are remain when $s \geq 31$; or $31 - s$ bits of 0 are added to $C_1$ when $s < 31$. The generation process of the scramble initialization sequence $C_2 = [C_{2,1}, ..., C_{2,j}, ..., C_{2,31}] \in \mathbb{C}^{1 \times 31}$ can be expressed as follows:

$$C_2 = \begin{cases} [C_{1,1}, ..., C_{1,j}, ..., C_{1,s}] \in \mathbb{C}^{1 \times 31}, s \geq 31, \\ [C_{1,1}, ..., C_{1,j}, ..., C_{1,0}, ..., 0] \in \mathbb{C}^{1 \times 31}, s < 31. \end{cases}$$

9. Referring to the scrambling generation in 3GPP physical layer standard [13]. Generating a Gold sequence $C_3$ of length $M$. The first $m$-sequence $p$ shall be initialized with $p(1) = 1, p(n) = 0, n = 2, 3, ..., 31$. The initialization of the second $m$-sequence $q$ is
denoted by \( q(n') = C2(n') \), where \( n' = 1, 2, ..., 31 \).
When the length of the \( m \)-sequence is greater than 31, the calculation is performed as follows:
\[
p(n + 31) = (p(n + 3) + p(n)) \bmod 2, 
q(n + 31) = (q(n + 3) + q(n + 2) + q(n + 1) + q(n)) \bmod 2. 
\]

The Gold sequence \( C3 \) of length \( M \) is generated as a scrambled sequence as follows:
\[
C3(n) = (p(n + Nc) + q(n + Nc)) \bmod 2, 
\]
where \( Nc = 1600 \).
The Gold sequence \( C3 \) is used to scramble the real initial key \( Key_i \) and the imaginary initial key \( Key_i \) of the entire vector \( h_i \). The final real part key \( KR_i \) and imaginary part key \( KL_i \) can be expressed as \( KR_i = [KR^1_i, KR^2_i, ..., KR^s_i] \) and \( KL_i = [KL^1_i, KL^2_i, ..., KL^s_i] \).

The generated final real part key \( KR_i \) and the final real part key \( KL_i \) of each subblock \( h_i \) are arranged in Figure 2 to generate the final secret key \( K \).

The final secret key \( K \) can be given by \( K = [KR^1_i, KL^1_i, ..., KR^s_i, KL^s_i] \).

### 3. Security Analysis

In this section, we analyze quantitative measurements of security. The metric of security is usually based on information theory, in which one of the metrics is the amount of mutual information between the key generated at the legitimate node and eavesdropper.

Since the distance between Eve and Bob is assumed to be smaller than the distance between Eve and Alice, only the mutual information between Alice to Bob and the mutual information between Alice to Eve is taken into consideration. Equation (13) can be used to calculate the Pearson correlation coefficient of the channel fading coefficient at two locations separated by \( d \).

\[
\rho = J_0(kd) \bigg/ \bigg/ J_0(kd) \bigg/ \bigg/ J_0(kd) \bigg/ \bigg/ J_0(kd) \bigg/ \bigg/ J_0(kd) \bigg/ \bigg/ J_0(kd) \\
\rho = [J_0(kd)]^2 
\]

where \( J_0(\cdot) \) is the first kind of Bessel function, \( k \) is the wavenumber. As shown in Figure 3 that is the image of the function.

At the \( p \)-th subcarrier, the fading coefficients of the Alice to Bob and Alice to Eve channels are determined as \( h_{bp} \) and \( h_{ep} \). In addition, the correlation coefficient between \( h_{bp} \) and \( h_{ep} \) is shown in equation (13) that is \( \rho \). The amount of mutual information between \( h_{bp} \) and \( h_{ep} \) is minded to be expressed as \( I(h_{bp}; h_{ep}) \).

\[
h_{bp} = h_{bp,R} + ih_{bp,I}, 
\]
\[
h_{ep} = h_{ep,R} + ih_{ep,I}. 
\]

Both \( h_{bp,R} \) and \( h_{bp,I} \) are independent identical distributions and obey \( \mathcal{N}(0, \sigma^2_{h_{bp}}/2) \). As well, \( h_{ep,R} \) and \( h_{ep,I} \) are independent identical distributions and obey \( \mathcal{N}(0, \sigma^2_{h_{ep}}/2) \). \( I(h_{bp}; h_{ep}) \) can be calculated by the following equation (16):

\[
\begin{align*}
 KL_i & \mid KR_i, KL_i, KR_i, KL_i, KL_i, KR_i, KL_i \mid
\end{align*}
\]

Figure 2: Key arrangement.

\[
I(h_{bp}; h_{ep}) = I(h_{bp,R}, h_{bp,I}, h_{ep,R}, h_{ep,I}), 
\]
\[
H_d(h_{bp,R}, h_{bp,I}) + H_d(h_{ep,R}, h_{ep,I}), 
\]
\[
-H_d(h_{bp,R}, h_{bp,I}, h_{ep,R}, h_{ep,I}), 
\]

where \( H_d(\cdot) \) is the entropy. The real and imaginary parts of the Alice to Bob and Alice to Eve channel coefficients are related to the parameter \( \rho \). Alternatively, the covariance matrix can be shown as follows:

\[
\begin{pmatrix}
\sigma^2_{h_{bp}}/2 & 0 \\
0 & \sigma^2_{h_{bp}}/2
\end{pmatrix}
\]

After introducing equation (12), equation (11) can be written as follows:

\[
\begin{align*}
I(h_{bp}; h_{ep}) & = H_d(h_{bp,R}, h_{bp,I}) + H_d(h_{ep,R}, h_{ep,I}), 
\end{align*}
\]

\[
= \frac{1}{2} \log \left( \text{det} \left( 2\pi e \frac{\Sigma}{3} \right) \right) + \frac{1}{2} \log \left( \text{det} \left( 2\pi e \frac{\Sigma}{3} \right) \right) 
\]

\[
= \log \left( \frac{\Sigma_{h_{bp}}}{2\pi e} \right) + \log \left( \frac{\Sigma_{h_{ep}}}{2\pi e} \right) 
\]

\[
= \log \left( \frac{\Sigma_{h_{bp}}}{2\pi e} \right) + \log \left( \frac{\Sigma_{h_{ep}}}{2\pi e} \right) 
\]

\[
= -\log \left( 1 - \rho^2 \right) 
\]
When $\rho$ approaches 0, the amount of mutual information $I(h_{bp}, h_{ep})$ approaches 0. In the worst-case situation, Eve and Bob are separated by half a wavelength. Half a wavelength is 5 cm when the frequency band is assumed to be 3 GHz.

$$\rho \approx \frac{1}{2} J_0 \left(\frac{2\pi}{\lambda} d\right)^2 = \frac{1}{2} J_0 \left(\frac{2\pi}{c f d}\right)^2,$$

where $c$ is the speed of light. As shown in Figure 4, at this time we can obtain the correlation coefficient $\rho \approx 0.09$ and the amount of mutual information $I(h_{bp}, h_{ep}) \approx 0.01$ (bit).

### 4. Simulation Performance Analysis

In this section, numerical results are given to illustrate the performance of the RISKG algorithm. The RISKG algorithm is compared with three algorithms including the conventional key generation (CKG) algorithm, index-based key generation (IKG) algorithm, and joint key generation (JKG) algorithm. The CKG algorithm generates the key by comparing each subcarrier amplitude with the mean of the subcarrier amplitudes within the entire OFDM block [6]; the IKG algorithm divides the whole OFDM block into subblocks, which generates the corresponding secret keys according to the index positions of the strongest and second strongest subcarriers within the subblocks; the JKG algorithm combines CKG and IKG to generate the corresponding secret keys [16].

We assume that there are $N = 9$ pathways in the Rayleigh fading channel between any two communication nodes, where the exponentially fading power delay distribution is taken into consideration [17]. To make a fair comparison with the other above-mentioned three algorithms, the parameters related to the simulation performance analysis of all algorithms are uniformly set (according to Table 1).

In addition, the effects of nonideal channel reciprocity and nonideal channel estimation due to noise, interference, and synchronization errors are considered [18]. Due to the influence of the channel estimation, the channel between Alice and Bob can be expressed as $\hat{H}_{ah/b} = H^i_{ah/b} + \Delta \hat{H}_{ah/b}$ and $\hat{H}_{bh/ah} = H^i_{bh/ah} + \Delta \hat{H}_{bh/ah}$. $\Delta \hat{H}_{ah/b}$ and $\Delta \hat{H}_{bh/ah}$ is modeled as an independent complex Gaussian noise with mean 0 and variance $\sigma^2_{ah/b} = e \times 10^{-SNR_{dB}/10}$, it should be emphasized that the error variance value of the estimated channel depends on the quality of the adopted estimator, which is highly affected by the length of the training sequence and its power. Thus, we use a similar scale $e \in \{0.01, 0.001, 0.0001\}$ referred to all secret key generation algorithms [19].

#### 4.1. Performance Metrics

The key generation rate (KGR) describes the ratio of the number of secret keys generated to the number of channel characteristics in each measurement, and a higher bit rate indicates that a long secret key can be generated in a shorter period. When the key generation rate is faster, the keys are updated more frequently and the communication system is more secure. When the probing speed is given, the key generation rate is calculated as follows:

$$KGR = \frac{L}{M} \text{ (bits/sample)},$$

where $L$ is the number of secret keys, $M$ is the number of channel characteristics.

The key mismatch rate (KMR) is mainly used to measure the mismatch between legitimate communication nodes, which is calculated as follows:

$$KMR = \frac{\sum_{i=1}^{L} |K_A(i) - K_B(i)|}{L},$$

where $K_A$ and $K_B$ denote the secret keys generated at Alice and Bob’s, respectively.

The key leakage rate (KLR) is used to measure the matching rate of keys between legitimate communication nodes and eavesdroppers, which is calculated as follows:
**Figure 4:** Correlation coefficient versus distance in the 3 GHz band.

**Figure 5:** KGR versus SNR performance under non-ideal channels and imperfect channel estimation for RISKG, CKG, IKG, JKG algorithms.

**Table 1: Simulation parameters set.**

| Item                                | Number          |
|------------------------------------|-----------------|
| Number of subcarriers of the OFDM block | $M = 128$      |
| Total number of sub blocks          | $s = 32$        |
| Number of subcarriers per sub block | $I = M/s = 4$   |
\[ KLR = \frac{1 - \sum_{i=1}^{L} |K_B(i) - K_E(i)|}{L}, \tag{17} \]

where \(K_B\) and \(K_E\) denote the secret keys generated at Bob and Eve, respectively. Lower KLG indicates less information has been leaked and better performance.

Randomness is a measure of the security strength of the secret keys generated by Alice and Bob that determines whether the key generation scheme is secure or not. At present, most of the tests for secret key randomness in physical layer secret key research use the randomness test standard issued by the National Institute of Standards and Technology (NIST). The test items include: frequency, block frequency, cumulative sums, runs, longest run, rank, discrete Fourier transform, nonperiodic template matchings, overlapping template matchings, universal statistical, approximate entropy, random excursions, random excursions variant, serial, linear complexity [20]. Due to the limitation of the final key length, the key sequence generated by the RISKG algorithm meets 7 of 15 test items, and only 7 of them are selected for testing.

4.2. Simulation Performance. Figure 5 shows KGR versus SNR for the RISKG, CKG, IKG, and JKG algorithms at Bob or Eve under the nonideal channel situation and imperfect channel estimation \((e \in \{0.01, 0.001, 0.0001\})\). It can be seen from the figure that as \(e\) decreases, the KGR of all algorithms increases to some extent. As the SNR rises, the KGR of all algorithms rises to some extent, gradually approaching the highest KGR in the ideal state at around 40 dB. The RISKG algorithm proposed in this paper greatly surpasses the other three algorithms in the performance of KGR, under the same SNR and \(e\). It can also be seen that Eve’s KGR for different SNR cases is smaller than that of any algorithm used on Bob with all algorithms.

Figure 6 shows KMR versus SNR performance under non-ideal channels and imperfect channel estimation for RISKG, CKG, IKG, JKG algorithms. It can be seen from the figure that the KMR of all algorithms decreases as \(e\) decreases. Simultaneously the KMR of all algorithms decreases as SNR increases. The proposed RISKG algorithm outperforms the other three algorithms. Due to the uncorrelation of the channel, there is a significant gap between the KMR on Eve and Bob compared to all cases on Bob, and it becomes more obvious as the SNR increases.

In addition, Figure 7 shows the KLG vs. SNR of keys generated at Eve using the RISKG algorithm, the IKG algorithm, and the RISKG algorithm without scrambling for \(e = 0.001\). From the three sets of data in Figure 7, the KLR is reduced by scrambling, which makes Eve steal less useful information. And RISKG algorithm also reduces the KLG at Eve compared to the IKG algorithm, which improves the security of the communication system.
The randomness test results of the keys generated by the RISKG algorithm are shown in Table 2. The generated final secret key sequence is checked for randomness using the NIST statistical test suite in this paper. The NIST statistical test suite consists of 15 different test items, each test is given a \( P \)-value \((P\)-value is a probability value between 0 and 1). If the \( P \)-value of each test is more than 0.01, the randomness tests are regarded to be passed. The 7 test items are randomly picked secret keys generated by the RISKG algorithm when the SNR is 10 dB, which tested under \( e \in \{0.01, 0.001, 0.0001\} \) respectively are shown in Table 2.

### 4.3. Computational Complexity

To fairly compare the complexity of the three algorithms, we uniformly assume that the key generation is performed for the diagonal matrix \( \mathbf{H} \in \mathbb{C}^{M \times M} \) in the coherent time \( \tau \) and the size of the subblock is uniformly assumed to be \( l \). For the RISKG algorithm, a total of \((3 - 1/l)M - 2\) addition calculations, \( M/l + 2 \) multiplication calculations, \( 7M + 3200 \) bitwise exclusive-OR calculations and \( 3M \) comparisons are performed. Taken together, the RISKG algorithm has complexity \( O(M) \), which implies that the proposed algorithm has linear complexity with respect to the length of key generation. For the IKG algorithm, because of its multiplication by the interleaving matrix \( \mathbf{R} \in \mathbb{C}^{M \times M} \), it performs \( M^2 \) multiplication calculations, \((M - 1)^3\) addition calculations, and \((1 + (\log l)/l - 2/l)M\) comparison calculations. The JKG algorithm performs more \((1 - 1/l)M\) addition calculations and \( M/l \) times multiplication on the base of the IKG algorithm, so the complexity of both the IKG and JKG algorithms is \( O(M^3) \) and greater than the proposed RISKG algorithm. The computational complexity of the three algorithms is shown in Table 3.

| Test items     | \( P \)-values (RISKG) |
|----------------|------------------------|
|                | \( \epsilon = 0.01 \)  | \( \epsilon = 0.001 \) | \( \epsilon = 0.0001 \) |
| Frequency      | 0.5838                 | 0.3115                 | 0.2549                 |
| Block frequency| 0.9952                 | 0.0338                 | 0.2888                 |
| Cumulative sums| 0.5446                 | 0.5620                 | 0.2915                 |
| Runs           | 0.6580                 | 0.7519                 | 0.0248                 |
| Longest run    | 0.3174                 | 0.5442                 | 0.3696                 |
| Approximate entropy | 0.9825                | 0.9732                 | 0.9814                 |
| Serial         | 0.4989                 | 0.4989                 | 0.1529                 |

### Table 3: Computational complexity.

| Algorithm | Complexity |
|-----------|------------|
| RISKG     | \( O(M) \) |
| IKG       | \( O(M^3) \) |
| JKG       | \( O(M^3) \) |

The JKG algorithm performs more \((1 - 1/l)M\) addition calculations and \( M/l \) times multiplication on the base of the IKG algorithm, so the complexity of both the IKG and JKG algorithms is \( O(M^3) \) and greater than the proposed RISKG algorithm. The computational complexity of the three algorithms is shown in Table 3.
5. Conclusions

Taking the short-time reciprocity of the time-division duplex communication, this paper proposes a novel key generation algorithm under the OFDM system and Rayleigh fading channel by using the CIR of the wireless channel and gives the specific implementation steps of the algorithm. The algorithm first obtains the CIR of the wireless channel at the legitimate communicate node by the pilots. Moreover, the keys for the real and imaginary parts of each subcarrier are generated independently and arranged in front-to-back order to enhance the key generation rate, with the initial key being generated by comparing the mean value when generating the key for the corresponding subcarrier. Finally, to make it more difficult for Eve to obtain the secret key based on the CIR trend and improve secret key confidentiality, the mean phase of subcarriers within each subblock is used as the scrambling initialization to scramble the generated initial secret key that enhances security and lowers the KLR at Eve.

In the security analysis section, the security is analyzed by information theory, and the results show that the proposed algorithm has high security in theory. In terms of simulation performance, compared with the CKG algorithm, IKG algorithm, and JKG algorithm, the RISKG algorithm significantly improves the performance in both KGR and KMR. Unlike the JKG algorithm, which enhances KGR by sacrificing a specific performance of KMR, the RISKG algorithm improves KGR without worsen KMR. Advanced the NIST statistical test suite is used to evaluate the randomness of the final key generated. The computational complexity of the algorithm is also analyzed. In summary, the secret key generated by the proposed algorithm can be used to encrypt and secure wireless communications.

Data Availability

The numerical simulation data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This work was supported by the Natural Science Foundation of Chongqing under Grant no. cstc2021jcyj-msxmX0454.

References

[1] R. Sharma, R. Sharma, and H. Singh, “Classical encryption techniques,” International Journal of Computers & Technology, vol. 3, no. 1, pp. 84–90, 2012.
[2] L. Jiao, N. Wang, P. Wang, A. Alipour-Fanid, J. Tang, and K. Zeng, “Physical layer key generation in 5G wireless networks,” IEEE Wireless Communications, vol. 26, no. 5, pp. 48–54, 2019.
[3] A. Goldsmith, Wireless Communications, Cambridge University Press, United Kingdom, 2005.
[4] K. Zeng, “Physical layer key generation in wireless networks: challenges and opportunities,” IEEE Communications Magazine, vol. 53, no. 6, pp. 33–39, 2015.
[5] J. M. Hamamreh, E. B. Asar, and H. Arslan, “OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services,” IEEE Access, vol. 5, pp. 25863–25875, 2017.
[6] H. Liu, W. Yang, and Y. Jie, “Fast and practical secret key extraction by exploiting channel response,” Proceedings of the 2013 IEEE INFOCOM, 14-19 April 2013, Turin, Italy, 2013.
[7] M. Yusuf and H. Arslan, “Enhancing physical-layer security in wireless communications using signal space diversity,” Proceedings of the MILCOM 2016 - 2016 IEEE Military Communications Conference (MILCOM), 01-03 November 2016, Baltimore, MD, USA, 2016.
[8] Q. Wang, H. Su, and K. Ren, “Fast and scalable secret key generation exploiting channel phase randomness in wireless networks,” Proceedings of the IEEE Infocom. IEEE, 10–15 April 2011, Shanghai, China, 2011.
[9] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, “Key generation from wireless channels: a review,” IEEE Access, vol. 4, no. 3, pp. 614–626, 2016.
[10] Y. Liu, S. C. Draper, and A. M. Sayeed, “Exploiting channel diversity in secret key generation from multipath fading randomness,” IEEE Transactions on Information Forensics and Security, vol. 7, no. 5, pp. 1484–1497, 2012.
[11] J. Zhang, R. Woods, and A. Marshall, “An effective key generation system using improved channel reciprocity,” Proceedings of the 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 1727–1731, IEEE, 19-24 April 2015, South Brisbane, QLD, Australia, 2015.
[12] H. Liu, Y. Wang, J. Yang, and Y. Chen, “Fast and practical secret key extraction by exploiting channel response,” Proceedings of the 32nd IEEE Int. Conf. Comput. Commun. (INFOCOM), pp. 3048–3056, 14-19 April 2013, Turin, Italy, 2013.
[13] F. Lu, “5G Evolved Universal terrestrial radio access (E-UTRA); physical channels and modulation,” Tobacco Situation, vol. 36, p. 211, 2011.
[14] N. Aldaghi and H. Mahdavifar, “Physical layer secret key generation in static environments,” IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2692–2705, 2019.
[15] C. Chan and M. A. Jensen, “Secret key establishment using temporally and spatially correlated wireless channel coefficients,” IEEE Transactions on Mobile Computing, vol. 10, no. 2, pp. 205–215, 2011.
[16] H. M. Furqan, J. M. Hamamreh, and H. Arslan, “New physical layer key generation dimensions: subcarrier indices/positions-based key generation,” IEEE Communications Letters, vol. 99, p. 1, 2020.
[17] Y. S. Cho, J. Kim, and W. Y. Yang, MIMO-OFDM Wireless Communications with MATLAB, John Wiley & Sons, New York, 2010.
[18] J. M. Hamamreh and H. Arslan, “Secure orthogonal transform division multiplexing (OTDM) waveform for 5G and beyond,” IEEE Communications Letters, vol. 21, no. 5, pp. 1191–1194, 2017.
[19] H. M. Furqan, “Physical layer security techniques for future wireless communication systems against eavesdropping,” Beyond, vol. 546, p. 31256, 2020.