SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

January 2024, Vol. 67, Iss. 1, 112303:1–112303:19
https://doi.org/10.1007/s11432-022-3768-8

Modulated symbol-based one-time pad secure transmission scheme using physical layer keys

Xiaoyan HU[1], Zheng WAN[1], Kaizhi HUANG[1,2*], Liang JIN[1,2], Mengyao YAN[1], Yajun CHEN[1] & Jinmei YANG[2]

[1]*Information Engineering University, Zhengzhou* 450001*, China;*
[2]*Purple Mountain Laboratories for Network and Communication Security, Nanjing* 211111*, China*

Received 13 November 2022/Revised 24 February 2023/Accepted 15 May 2023/Published online 27 December 2023

Abstract This paper proposes a novel modulated symbols-based one-time pad (SOTP) secure transmission scheme using physical layer keys. Unlike classical physical layer key generation and exclusive OR (XOR) encryption in the discrete binary space, we design a framework for modulated symbols-based one-time pad (OTP) encryption, where the cryptographic primitive and mathematical model of SOTP is given to build a practical cryptographic protocol. Compared with existing physical layer encryption (PLE) schemes, we provide rigorous proof that the framework can meet perfect secrecy and correctness requirements. In addition, we provide a specific scheme of physical layer OTP secure transmission for quadrature amplitude modulation (QAM) and phase-shift keying (PSK) symbols based on physical layer keys. This scheme realizes the unification of bit encryption and symbol encryption, which can adaptively select the quantization level according to the signal-to-noise ratio (SNR) to minimize the symbol error rate (SER). Further, we analyze the performance quantitatively and derive the closed-form expressions of SER, which indicates that the proposed scheme has a lower SER. Finally, simulation results verify that the proposed symbol-wise OTP secure transmission scheme can achieve perfect secrecy and high reliability.

Keywords physical layer security, one-time pad, wireless channel, physical layer encryption, perfect secrecy

1 Introduction

Wireless communication security is a critical and increasingly challenging issue in wireless networks. Due to the broadcast characteristics of electromagnetic wave propagation, anyone within range of signals can intercept signals and steal information [1]. A sufficient condition for realizing secure communication is a one-time pad (OTP) [2], which is perfect secrecy that cannot be cracked by any computing means. Shannon proves that perfect secrecy can only be achieved if the key entropy is not less than the plaintext entropy [3]. Unfortunately, Shannon only gave the existence and conditions of perfect secrecy but did not give how to implement these conditions in a specific communication system.

In recent years, the physical layer key generation technology has provided the possibility to solve the perfect secrecy problem [4]. Since electromagnetic waves experience irradiation, reflection, and refraction during propagation, wireless channels exhibit different characteristics in different space-time environments and are a natural source of randomness [5]. Based on the reciprocity and spatial decorrelation nature of the wireless channel, legitimate communication parties can extract symmetric secret keys [6, 7]. Physical layer key generation provides a lightweight means of key distribution and encryption, which is suitable for low computational overhead networks such as IoT and wireless sensor networks. Secret key generation includes four steps: random source acquisition, quantization, information reconciled, and privacy amplification [8]. Based on reconciliation keys, legitimate communication users can provide secure transmission by encrypting message bits via OTP cryptographic principles; i.e., each message bit is exclusive OR (XOR) with each secret key. Nevertheless, the parity information exchanged over the public channel during the information reconciliation phase will partially leak keys to the eavesdropper. In addition,

* Corresponding author (email: huangkaizhi@tsinghua.org.cn)

additional protocols are required for information reconciliation compared with existing communication systems [9].

More and more studies focus on the joint design of key generation and OTP encryption to solve the problem [10–14]. Ref. [10] proposed a secure transmission scheme using non-reconciled keys generated from the wireless channel. This integrated scheme reuses channel coding to simultaneously correct key mismatch and transmission errors. Ref. [11] deemed non-reconciled key differences as transmission errors and designed polar codes with stronger error correction ability to improve the secure transmission rate. Subsequently, Ref. [12] proved that the integrated secure transmission scheme using non-reconciled keys outperforms the classical secure transmission scheme using reconciled keys regarding communication overhead and computation complexity. Hu et al. [13] quantitatively analyzed the performance of the secure transmission scheme using non-reconciled keys and showed that the scheme has a higher secrecy capacity.

However, these bit-based OTP secure transmission schemes using non-reconciled keys (BOTP) have problems with their practical application. To encrypt message bits, the analog channel measurements are quantized and encoded into 0/1 bits. When message bits are XOR encryption by mismatched keys, it will lead to bit inversion in the ciphertext. The error ciphertext is modulated at the physical layer, equivalent to constellation hopping [15]. That is to say, the tiny errors between analog channel measurements will be amplified to the Euclidean distance level of the constellation points after quantization and XOR encryption, resulting in a higher bit error rate (BER) for the transmission system.

To avoid this problem, some physical layer encryption (PLE) schemes propose not quantifying the channel state information (CSI) but directly using the continuous CSI as keys to encrypt modulated signals. Ref. [16] proposed a random phase rotation scheme to rotate the modulated symbol by the channel phase, which can achieve a lower BER. Ref. [17] employed the guard intervals to alleviate the impact of the channel estimation errors. Further, Ref. [18] rotated the phase and selected modulation type depending on signal-to-noise ratio (SNR). Considering this scheme suffers information leakage in phase-amplitude-modulated (PAM) signals, Bi et al. [19] randomized the radio signals using a discrete Fourier transform (DFT)-based encryption algorithm. However, perfect secrecy is asymptotically achievable only when the signal block length approaches infinity. In addition, Refs. [20,21] proposed the dynamic mapping rule between the modulated symbols and binary bits. Moreover, the noise mask-based physical layer encryption scheme is proposed to superimpose the valid signal with noise-like signals generated from the wireless channel [22,23]. Ref. [24] proposed an encryption scheme based on random constellation rotation and artificial noise insertion. However, the noise mask's scrambling of the modulated symbols can be ignored when the SNR is large enough. This solution only can improve the security level rather than perfect secrecy [25].

Combining the advantages of bit encryption and symbol encryption, we propose a modulated symbols-based OTP secure transmission scheme using physical layer keys (SOTP). Unlike BOTP secure transmission schemes, we extend the classical bit-level encryption into symbol-level encryption. Our contributions are summarized as follows.

(1) We design a framework for SOTP encryption. Unlike classical physical layer key generation and XOR encryption in the discrete binary space, we propose the cryptographic primitives and mathematical models to build a symbol-wise OTP cryptographic protocol. We prove that the SOTP encryption model can meet the perfect secrecy and correctness requirements. The framework jointly designs the physical layer key generation and physical layer OTP encryption at the physical layer, realizing the integration of security and communication.

(2) We provide a specific scheme of physical layer OTP secure transmission for quadrature amplitude modulation (QAM) and phase-shift keying (PSK) symbols based on physical layer keys. The scheme can dynamically adjust the quantization level. When the quantization level is 1, the scheme is equivalent to the BOTP secure transmission scheme. When the quantization level tends to infinity, the scheme is equivalent to symbol encryption with continuous CSI. This scheme can realize the unification of bit encryption and symbol encryption.

(3) We derive the closed-form expression of symbol error rate (SER), and the optimal quantization level can be selected according to the SNR to achieve a lower SER. We also analyze the SER performance quantitatively and indicate that the proposed scheme can achieve a lower SER. Simulation results show that the proposed SOTP secure transmission scheme can achieve perfect secrecy against the passive eavesdropping attack and is verified to achieve lower SER than existing transmission schemes.

The rest of the paper is organized as follows. Section 2 presents the system model in detail. In Section 3,

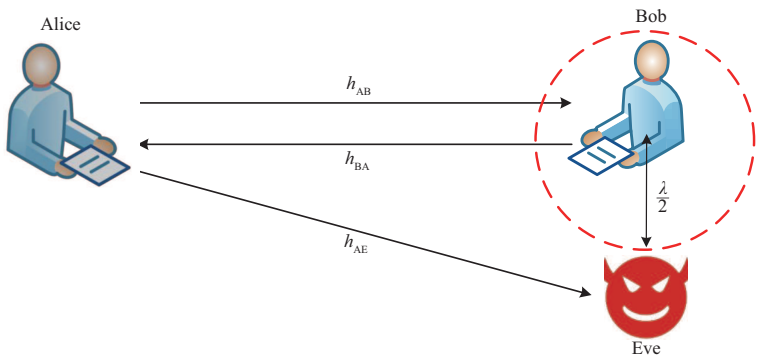

Figure 1 (Color online) System model.

we propose a framework of SOTP encryption. Section 4 provides the specific scheme of physical layer OTP secure transmission for QAM and PSK symbols based on the wireless channel. The performance analysis and discussion are delivered in Section 5. Simulation results and performance evaluation are discussed in Section 6. Finally, we conclude this paper in Section 7.

2 System model

The system model is shown in Figure 1, where Alice and Bob equipped with a single antenna are two legitimate users. Alice and Bob exploit their reciprocal channels in time-division duplex (TDD) mode to generate secret keys, then encrypt and decrypt the transmitted data using the OTP approach. At the same time, Eve is a passive eavesdropper trying to crack private messages. Eve is equipped with multiple antennas and is more than half wavelength away from Bob. Assume that Eve knows the complete key generation and OTP encryption protocol and can also receive the information transmitted over the public channel. Considering the worst case, the computation and communication capabilities of Eve are stronger than Alice's and Bob's.

Assume that the wireless channel between Alice and Bob is a frequency-flat Rayleigh fading channel, where the channel coefficient is essentially invariant during the channel coherence time and is independent at different coherence time. The channel from Alice to Bob h_{AB} and channel from Bob to Alice h_{BA} are equal during the coherence interval based on the channel reciprocity, i.e., $h_{\mathrm{AB}} = h_{\mathrm{BA}}$. The channel is modeled as cyclically symmetric complex Gaussian (CSCG) random variables with zero means and unit variances, namely $h \sim \mathcal{CN}(0,1)$. The transmit power of each frame is P, where the pilot symbol power is αP and the data symbol power is $(1-\alpha)P$. The data symbol is transmitted with a symbol rate of R_{s} and the signal bandwidth B satisfies $B = R_{\mathrm{s}}$.

3 The framework of SOTP encryption

In this section, we design a framework for SOTP encryption. As shown in Figure 2, Alice and Bob generate secret keys from the reciprocal wireless channel. Then modulated symbols are encrypted and decrypted using the OTP method.

3.1 Encryption model of SOTP

We first give the cryptographic primitive and mathematical model of SOTP to build a practical cryptographic protocol.

Definition 1. Plaintext space $\mathcal{S}$: the set of M-ary modulated symbols, for any input message, $s \in \mathcal{S}$.

Ciphertext space $\mathcal{C}$: the set of all possible ciphertext, for any input ciphertext, $c \in \mathcal{C}$.

Key space $\mathcal{K}_{\mathrm{A}}$, $\mathcal{K}_{\mathrm{B}}$: encryption key set $\mathcal{K}_{\mathrm{A}}$ and decryption key set $\mathcal{K}_{\mathrm{B}}$, where $k_{\mathrm{A}} \in \mathcal{K}_{\mathrm{A}}$ and $k_{\mathrm{B}} \in \mathcal{K}_{\mathrm{B}}$.

Key generation algorithm Gen: $\mathcal{H} \to \mathcal{K}$, $\mathcal{H}$ is a infinite set containing continuous channel coefficient h and $k = \mathrm{Gen}(h)$.

Encryption algorithm Enc: $\mathcal{S} \times \mathcal{K}_{\mathrm{A}} \to \mathcal{C}$, where $c := \mathrm{Enc}_{k_{\mathrm{A}}}(s)$.

Channel function: $\mathcal{C} \to \mathcal{Z}$, $\mathcal{Z}$ is the set of all possible received symbols, where $z \in \mathcal{Z}$ is affected by channel fading and noise.

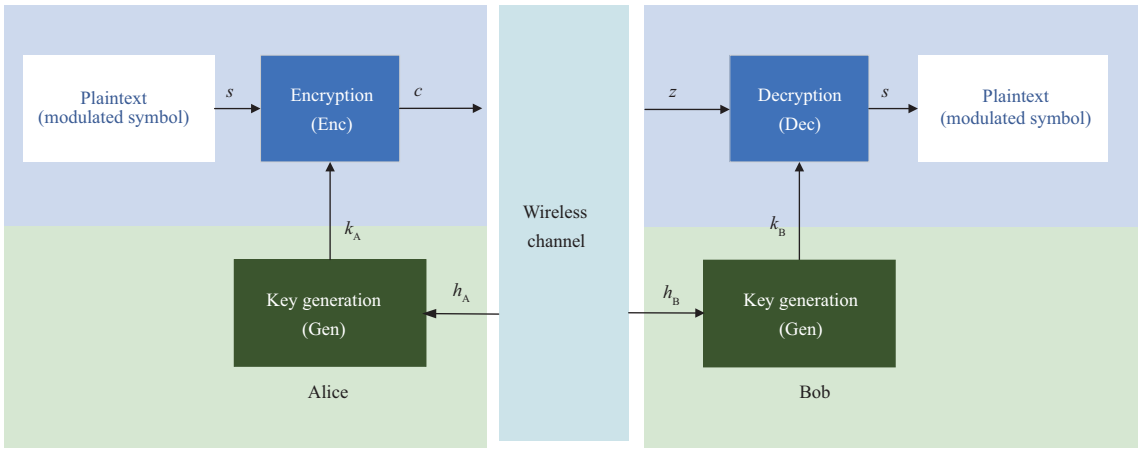

Figure 2 (Color online) Modulated symbols-based OTP encryption model.

Decryption algorithm Dec: $\mathcal{Z} \times \mathcal{K}_{\mathrm{B}} \to \mathcal{S}$, where $s := \mathrm{Dec}_{k_{\mathrm{B}}}(z)$.

Let $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ be a SOTP encryption scheme over plaintext space $\mathcal{S}$ of M-ary modulated signals, where $|\mathcal{S}| = M^l$, l is length of modulated symbols. The SOTP encryption scheme is defined as follows.

Definition 2. Key generation algorithm Gen works as follows: let $\mathrm{Gen} : \mathcal{H} \to \mathcal{K}$ be a surjection function, where every k is chosen from $\mathcal{K} = \{0, 1, 2, \ldots, n-1\}^l$ with equal probability by $k = \mathrm{Gen}(h)$, i.e., $\Pr(K = k) = 1/|\mathcal{K}| = 1/n^l$.

Encryption algorithm Enc works as follows: let $f_{\mathrm{s}} : \mathcal{S} \to \mathcal{M}$ be an injection function to map modulated symbols into $\mathcal{M}$, where $\mathcal{M} \subseteq \mathcal{K} = \{0, 1, 2, \ldots, n-1\}^l$. Given an encryption key $k_{\mathrm{A}} \in \mathcal{K}_{\mathrm{A}}$ and a plaintext $s \in \mathcal{S}$, output

$$c = {f_{\mathrm{c}}}^{-1}\left([f_{\mathrm{s}}(s) + k_{\mathrm{A}}] \bmod n\right), \tag{1}$$

where the expression $a \bmod n$ represents the remainder of the Euclidean division of a by b, a is the dividend and b is the divisor.

Decryption algorithm Dec works as follows: let $f_{\mathrm{c}}^{-1} : \mathcal{K} \to \mathcal{C}$ be a bijection function to map key space into ciphertext space, where $|\mathcal{K}| = |\mathcal{C}| = n^l$. Given a decryption key $k_{\mathrm{B}} \in \mathcal{K}_{\mathrm{B}}$ and a received symbol $z \in \mathcal{Z}$, output

$$s_{\mathrm{B}} = f_{\mathrm{s}}^{-1}\left([f_{\mathrm{c}}(z) - k_{\mathrm{B}}] \bmod n\right). \tag{2}$$

3.2 Confidentiality of SOTP encryption

This subsection provides rigorous proof that this SOTP encryption scheme achieves perfect secrecy. Firstly, we give perfect secrecy as defined by Shannon [3].

Definition 3. An encryption scheme over a plaintext space $\mathcal{S}$ is perfect secrecy if for every probability distribution over $\mathcal{S}$, every message $s \in \mathcal{S}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr(C = c) > 0$, it holds

$$\Pr(C = c | S = s) = \Pr(C = c). \tag{3}$$

Definition 3 states that a perfect encryption scheme requires the ciphertext is independent of the plaintext, which means that an eavesdropper cannot obtain any information about the plaintext from the ciphertext. Definition 3 leads us to the following theorem.

Theorem 1. The SOTP encryption scheme is perfect secrecy.

Proof. We give the following lemma to assist the proof of the Theorem 1.

Lemma 1. For any $a, b, c \in \{0, 1, \ldots, n-1\}^l$, there exist an unique sequence b with $c = (a + b) \bmod n$.

Lemma 1 can be easily deduced from the quotient remainder theorem [26], which states that for a given plaintext and ciphertext, the key is uniquely determined. For any arbitrary $s \in \mathcal{S}$ and $c \in \mathcal{C}$, we have

$$\begin{aligned} &\Pr(C = c | S = s) \\ &= \Pr\left\{c = f_{\mathrm{c}}^{-1}\left([f_{\mathrm{s}}(s) + K_{\mathrm{A}}] \bmod n\right) | S = s\right\} \\ &= \Pr\left\{f_{\mathrm{c}}(c) = ([f_{\mathrm{s}}(s) + K_{\mathrm{A}}] \bmod n)\right\} \end{aligned} \tag{4}$$

holds since f_{c}^{-1} is a bijection function. From Lemma 1, we can know that there exists a unique key $K_{\mathrm{A}} = k_{\mathrm{A}}$ such that $f_{\mathrm{c}}(c) = [f_{\mathrm{s}}(s) + K_{\mathrm{A}}] \bmod n$ holds. Therefore, Eq. (4) can be transformed into

$$\begin{aligned}\Pr(C=c|S=s) &= \Pr\{f_{\mathrm{c}}(c) = [f_{\mathrm{s}}(s)+K_{\mathrm{A}}] \bmod n\} \\ &= \Pr\{K_{\mathrm{A}} = k_{\mathrm{A}}\} \\ &= \frac{1}{|\mathcal{K}|}.\end{aligned} \tag{5}$$

Further, $\Pr(C = c)$ can be calculated as

$$\begin{aligned}\Pr(C=c) &= \sum_{s_i \in \mathcal{S}} \Pr(C=c|S=s_i)\Pr(S=s_i) \\ &= \frac{1}{|\mathcal{K}|} \sum_{s_i \in \mathcal{S}} \Pr(S=s_i) \\ &= \frac{1}{|\mathcal{K}|}.\end{aligned} \tag{6}$$

Accordingly, we have

$$\Pr(C=c|S=s) = \Pr(C=c) = \frac{1}{|\mathcal{K}|}. \tag{7}$$

According to Definition 3, the SOTP encryption scheme can achieve perfect secrecy, so Theorem 1 is proven.

3.3 Correctness of SOTP encryption

In this subsection, we analyze the correctness of the SOTP encryption model. The received symbol of Bob forms a Markov chain $s \to c \to z$. $s_{\mathrm{B}} = \mathrm{Dec}_{k_{\mathrm{B}}}(z_{\mathrm{B}}) = s$ means $s_{\mathrm{B}} = \mathrm{Dec}_{k_{\mathrm{B}}}(c) = s$; hence, we consider a weaker condition

$$\begin{aligned}s_{\mathrm{B}} &= \mathrm{Dec}_{k_{\mathrm{B}}}(c) \\ &= \mathrm{Dec}_{k_{\mathrm{B}}}(\mathrm{Enc}_{k_{\mathrm{A}}}(s)) \\ &= \mathrm{Dec}_{k_{\mathrm{B}}}\left({f_{\mathrm{c}}}^{-1}([f_{\mathrm{s}}(s)+k_{\mathrm{A}}] \bmod n)\right) \\ &= f_{\mathrm{s}}^{-1}\left[f_{\mathrm{c}}\left({f_{\mathrm{c}}}^{-1}([f_{\mathrm{s}}(s)+k_{\mathrm{A}}] \bmod n)\right) - k_{\mathrm{B}}\right] \bmod n \\ &= f_{\mathrm{s}}^{-1}([f_{\mathrm{s}}(s)+k_{\mathrm{A}}-k_{\mathrm{B}}] \bmod n),\end{aligned} \tag{8}$$

holds due to the identity and distributive of modulo operations, i.e., $(a \bmod n) \bmod n = a \bmod n$ and $(a+b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$. Despite that keys k_{A} and k_{B} are slightly different due to the noise, the channel coding with a sufficiently large l is employed to implement a noise-free channel. Thus, Bob can correctly recover the private message sent from Alice, i.e., $s_{\mathrm{B}} = \mathrm{Dec}_{k_{\mathrm{B}}}(z_{\mathrm{B}}) = s$, which means the SOTP encryption framework can meet the correctness requirement.

4 The SOTP secure transmission scheme for QAM and PSK symbols

This section provides a specific scheme of physical layer OTP encryption for modulated symbols, including QAM and PSK signals, as shown in Figure 3. This scheme mainly consists of 3 steps: Alice and Bob first generate secret keys from wireless channels. Then Alice encrypts modulated symbols using secret keys and transmits ciphertexts to Bob. Finally, Bob decrypts and demodulates received signals to recover message bits.

4.1 Physical layer key generation

Alice and Bob send pilot sequences to probe the channel and perform least squares (LS) channel estimation to obtain channel estimates,

$$\hat{h}_{\mathrm{A}} = h_{\mathrm{BA}} + \varepsilon_{\mathrm{A}}, \tag{9}$$

$$\hat{h}_{\mathrm{B}} = h_{\mathrm{AB}} + \varepsilon_{\mathrm{B}}, \tag{10}$$

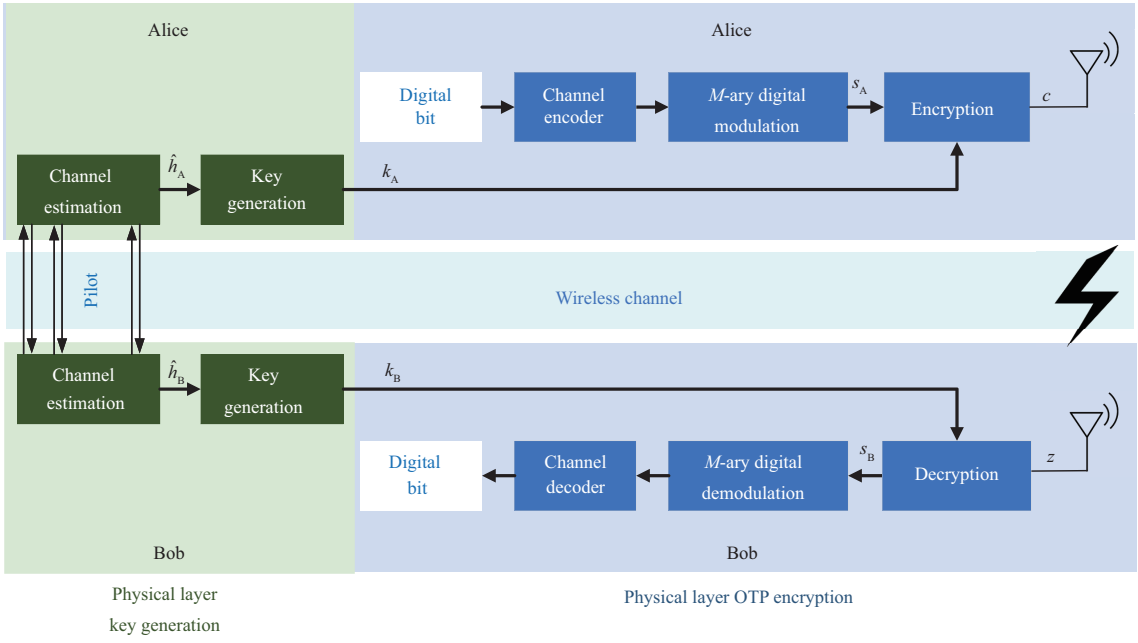

Figure 3 (Color online) Modulated symbols-based OTP secure transmission scheme using physical layer keys.

where $\varepsilon_{\rm A}$ and $\varepsilon_{\rm B}$ are channel estimation errors following CSCG distribution with zero mean and variance γ_p^{-1}. $\gamma_p = \alpha P/\sigma_n^2$ and σ_n^2 is the power of additional white Gaussian noise (AWGN). Similarly, Eve can also acquire

$$\hat{h}_{\rm E} = h_{\rm AE} + \varepsilon_{\rm E}, \tag{11}$$

where $h_{\rm AE}$ is the channel from Alice to Eve and $\varepsilon_{\rm E}$ is the estimation error.

According to Definition 2, every $k \in \mathcal{K}$ is chosen from $\mathcal{K} = \{0, 1, 2, \ldots, n-1\}^l$ with equal probability. Hence, unlike classical key generation algorithms where channel estimates are quantized and encoded into 0/1 digital bit, we generate discrete uniformly distributed random secret keys. For ease of description, we decouple the complex variable $\hat{h}$ into the real part $\hat{h}^{\rm Re}$ and imaginary part $\hat{h}^{\rm Im}$ in the same way as [6]. Next, the empirical cumulative distribution function (eCDF) over the channel samples is calculated as follows:

$$F_{\hat{h}^{\rm Re}}(x) = \frac{|\{i : \hat{h}_i^{\rm Re} \leqslant x\}|}{n}. \tag{12}$$

Then channel estimation results are quantized into n-ary sequences with n discrete values as

$$k_i^{\rm Re} = {\rm Gen}(\hat{h}_i^{\rm Re}) = \begin{cases} 0, & \hat{F}(\hat{h}_i^{\rm Re}) \in [0, 1/n), \\ 1, & \hat{F}(\hat{h}_i^{\rm Re}) \in [1/n, 2/n), \\ \vdots & \vdots \\ n-1, & \hat{F}(\hat{h}_i^{\rm Re}) \in [(n-1)/n, 1]. \end{cases} \tag{13}$$

Note that we only give the key generation algorithm for $k_i^{\rm Re}$. $k_i^{\rm Im}$ and $k_i^{\rm Re}$ are independent and identically distributed (i.i.d.) and can be generated in the same way. After the above operations, Alice and Bob can obtain equally distributed keys to encrypt modulated symbols.

4.2 Encrypt symbols using OTP method

4.2.1 *QAM symbols*

Rectangular QAM signal constellations are easily generated from two PAM signals impressed on the in-phase and quadrature carriers, which are the most widely used constellation structures in practical communication. Alice first generates the baseband modulated symbol $s_{\rm A}$ by the channel coding and digital modulation block in Figure 3. The M-ary QAM rectangular constellation can be equivalent to two individual $\sqrt{M}$-ary amplitude-shift keying (ASK) constellations as $s = s^{\rm Re} + s^{\rm Im}$, where $s^{\rm Re}$ and

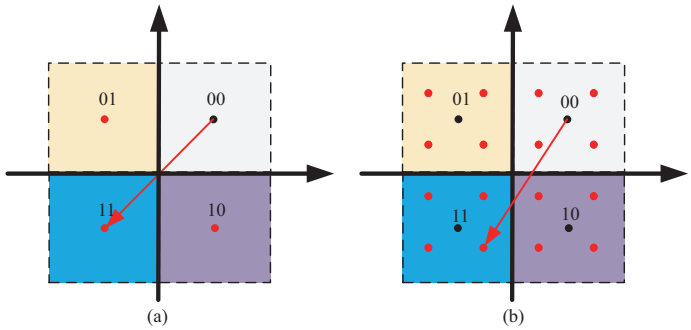

Figure 4 (Color online) SOTP encryption process on the 4-QAM constellation diagram. (a) $\delta = 1$; (b) $\delta = 2$.

s^{Im} are in-phase and quadrature components of symbols, respectively. Therefore, we can use real and imaginary channel coefficients to encrypt in-phase and quadrature components of symbols separately. In the encryption stage, the baseband QAM symbol is the input of encryption function Enc, where $f_{\mathrm{s}}: \mathcal{S} \to \mathcal{M}$ and $f_{\mathrm{c}}: \mathcal{C} \to \mathcal{K}$ are defined as follows:

$$f_{\mathrm{s}}(s) = \frac{s - L_{\min}}{d_{\min}}\delta, \tag{14}$$

$$f_{\mathrm{c}}(c) = f_{\mathrm{s}}(c) = \frac{c - L_{\min}}{d_{\min}}\delta, \tag{15}$$

where $d_{\min} = \sqrt{6E_{\mathrm{s}}/(M-1)}$ is the minimum Euclidean distance of the M-ary QAM constellation, E_{s} is the average symbol energy. $L_{\min} = -\sqrt{M}d_{\min}/2$ is the lower bound of the ciphertext symbol. $\delta = n/\sqrt{M}$ is the quantization level. According to Definition 2, the encryption process can be expressed mathematically as

$$c_{\mathrm{A}} = \mathrm{Enc}_{k_{\mathrm{A}}^{\mathrm{Re}}}\left(s_{\mathrm{A}}^{\mathrm{Re}}\right) + j \cdot \mathrm{Enc}_{k_{\mathrm{A}}^{\mathrm{Im}}}\left(s_{\mathrm{A}}^{\mathrm{Im}}\right), \tag{16}$$

where

$$\begin{aligned} c_{\mathrm{A}}^{\mathrm{Re}} &= \mathrm{Enc}_{k_{\mathrm{A}}^{\mathrm{Re}}}\left(s_{\mathrm{A}}^{\mathrm{Re}}\right) \\ &= f_{\mathrm{c}}^{-1}\left(\left[f_{\mathrm{s}}\left(s_{\mathrm{A}}^{\mathrm{Re}}\right) + k_{\mathrm{A}}^{\mathrm{Re}}\right] \bmod n\right), \end{aligned} \tag{17}$$

and

$$\begin{aligned} c_{\mathrm{A}}^{\mathrm{Im}} &= \mathrm{Enc}_{k_{\mathrm{A}}^{\mathrm{Im}}}\left(s_{\mathrm{A}}^{\mathrm{Im}}\right) \\ &= f_{\mathrm{c}}^{-1}\left(\left[f_{\mathrm{s}}\left(s_{\mathrm{A}}^{\mathrm{Im}}\right) + k_{\mathrm{A}}^{\mathrm{Im}}\right] \bmod n\right). \end{aligned} \tag{18}$$

For clear description, Figure 4 takes 4-QAM as an example to explain the encryption process in detail, where the black dots represent the plaintext constellation points, and the red dots represent the ciphertext constellation points. Original Plaintext constellation points are scattered within a rectangular complex plane region. The encryption operation is essential that secret keys shift symbol constellation points in the in-phase and quadrature directions. When $\delta = 1$, the ciphertext shares the same constellation as the plaintext, as shown in Figure 4(a). The encryption operation is equivalent to encrypting message bits and then modulating them into symbols, i.e., BOTP encryption. That is to say, BOTP encryption is a particular case of SOTP encryption. When $\delta \geqslant 2$, the encryption operation randomly maps a regular 4-QAM constellation to high order QAM, where the ciphertext space is δ times the plaintext space. As shown in Figure 4(b), when $\delta = 2$, the ciphertext constellation becomes the 16-QAM constellation.

Note that the average power of ciphertext symbols would not be the same as that of plaintext symbols. On the one hand, this energy difference may let the eavesdropper infer the modulation method according to the surge of transmission power. On the other hand, this additional power increases the transmission power. Thus, the ciphertext symbols are normalized before the digital to analog converter (DAC). The average power of ciphertext symbols is

$$\begin{aligned} E_{\mathrm{c}} &= \left[\left(c_{\mathrm{A}}^{\mathrm{Re}}\right)^2 + \left(c_{\mathrm{A}}^{\mathrm{Im}}\right)^2\right] \\ &= 2 \times \frac{M\delta^2 - 1}{12\delta^2} d_{\min}^2 \\ &= \frac{\left(M\delta^2 - 1\right) d_{\min}^2}{6\delta^2}. \end{aligned} \tag{19}$$

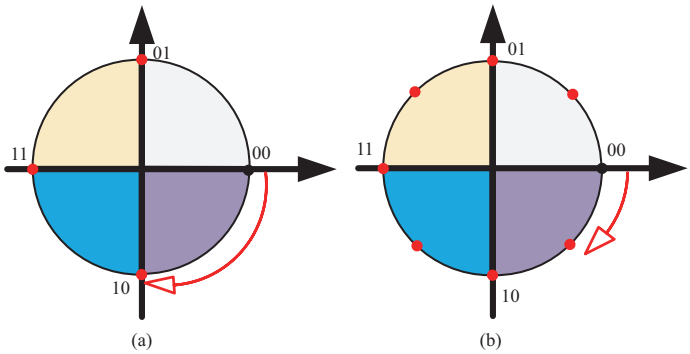

Figure 5 (Color online) SOTP encryption process on the 4-PSK constellation diagram. (a) $\delta = 1$; (b) $\delta = 2$.

The normalized factor β is calculated as

$$\beta = \sqrt{\frac{E_{\mathrm{s}}}{E_{\mathrm{c}}}} = \sqrt{\frac{\delta^2 (M-1)}{M\delta^2 - 1}}. \tag{20}$$

Thus, the normalized ciphertext symbol is computed as $\bar{c}_{\mathrm{A}} = \beta c_{\mathrm{A}}$. As a result, the ciphertext symbols have the same power as the plaintext symbols.

4.2.2 *PSK symbols*

Due to its high bandwidth efficiency and high anti-noise performance, PSK modulation has an extensive application in LTE systems. Alice first generates the baseband modulated symbol s_{A} by the channel coding and digital modulation block in Figure 3, which is the input of the encryption function. Note that PSK signals only modulate the phase information, so we only encrypt the phase of PSK signals. Plaintext space is the set of PSK symbol phases, and $f_{\mathrm{s}} : \mathcal{S} \to \mathcal{M}$ and $f_{\mathrm{c}} : \mathcal{C} \to \mathcal{K}$ are defined as follows:

$$f_{\mathrm{s}}(s) = \frac{sM\delta}{2\pi}, \tag{21}$$

$$f_{\mathrm{c}}(c) = \frac{cM\delta}{2\pi}, \tag{22}$$

where $\delta = N/M$ is the quantization level. According to Definition 2, the encryption can be expressed mathematically as

$$\begin{aligned} c_{\mathrm{A}} &= \mathrm{Enc}_{k_{\mathrm{A}}}\left(s_{\mathrm{A}}^{\theta}\right) \\ &= f_{\mathrm{c}}^{-1}\left(\left[f_{\mathrm{s}}\left(s_{\mathrm{A}}^{\theta}\right) + k_{\mathrm{A}}\right] \bmod n\right), \end{aligned} \tag{23}$$

where s_{A}^{θ} is the phase of s_{A}. Finally, Alice transmits ciphertext symbol $\bar{c}_{\mathrm{A}} = |s_{\mathrm{A}}| \, \mathrm{e}^{\mathrm{j}c_{\mathrm{A}}}$ over the wireless channel to Bob.

For clear description, Figure 5 takes the 4-PSK constellation as an example to explain the encryption process in detail, where the black dots represent the plaintext constellation points and the red dots represent the ciphertext constellation points. The plaintext and ciphertext constellation points are scattered over a circular area. The encryption operation is essentially that secret keys rotate symbol constellation points to obtain an encrypted constellation. When $\delta = 1$, the ciphertext shares the same constellation as the plaintext, as shown in Figure 5(a). The encryption operation is equivalent to the BOTP encryption scheme, which means BOTP encryption is a particular case of SOTP encryption. When $\delta \geqslant 2$, the encryption operation will randomly map a regular 4-PSK constellation to a high-order PSK constellation, as shown in Figure 5(b).

4.3 Decrypt symbols using OTP method

4.3.1 *QAM symbols*

Alice transmits ciphertexts over the wireless channel to Bob. Bob recovers original symbols by taking the inverse operation. Firstly, upon receiving noisy signals, the RF downconverter samples the incoming signal and observes a stream of complex baseband symbol vectors z_{B}. Then Bob restores the range of

ciphertext symbols via $c_{\mathrm{B}} = z_{\mathrm{B}}/\beta$. Next, Bob inverses map ciphertext symbols with the knowledge of keys k_{B}, which is represented as

$$s_{\mathrm{B}} = \mathrm{Dec}_{k_{\mathrm{B}}^{\mathrm{Re}}}\left(c_{\mathrm{B}}^{\mathrm{Re}}\right) + j \cdot \mathrm{Dec}_{k_{\mathrm{B}}^{\mathrm{Im}}}\left(c_{\mathrm{B}}^{\mathrm{Im}}\right), \tag{24}$$

where

$$\begin{aligned} s_{\mathrm{B}}^{\mathrm{Re}} &= \mathrm{Dec}_{k_{\mathrm{B}}^{\mathrm{Re}}}\left(c_{\mathrm{B}}^{\mathrm{Re}}\right) \\ &= f_{\mathrm{s}}^{-1}\left(\left[f_{\mathrm{c}}\left(e_{\mathrm{B}}^{\mathrm{Re}}\right) - k_{\mathrm{B}}^{\mathrm{Re}}\right] \bmod n\right), \end{aligned} \tag{25}$$

and

$$\begin{aligned} s_{\mathrm{B}}^{\mathrm{Im}} &= \mathrm{Dec}_{k_{\mathrm{B}}^{\mathrm{Re}}}\left(c_{\mathrm{B}}^{\mathrm{Im}}\right) \\ &= f_{\mathrm{s}}^{-1}\left(\left[f_{\mathrm{c}}\left(e_{\mathrm{B}}^{\mathrm{Im}}\right) - k_{\mathrm{B}}^{\mathrm{Im}}\right] \bmod n\right). \end{aligned} \tag{26}$$

The decryption operation is essentially secret keys shift ciphertext symbols in opposite direction to recover plaintexts. The maximum likelihood (ML) algorithm is used to demodulate decryption symbols. In the case of the equal prior probability of transmitted symbols, the optimal decision rule is expressed as

$$\hat{s} = \arg\max_{1 \leqslant i \leqslant M} \Pr\left(s_{\mathrm{B}} | s_i\right), \tag{27}$$

where $\Pr\left(s_{\mathrm{B}}|s_i\right)$ is the likelihood function. Finally, channel decoding is utilized to correct error bits to recover message bits.

4.3.2 *PSK symbols*

Upon receiving noisy signals, the RF downconverter samples the incoming signal and observes a stream of complex baseband symbol vectors z_{B}. Bob reconstructs original symbols by taking the inverse operation. Bob first reverse-rotates ciphertext symbols with the knowledge of secret keys k_{B}. The decryption symbol s_{B} can be decrypted by

$$\begin{aligned} s_{\mathrm{B}}^{\theta} &= \mathrm{Dec}_{k_{\mathrm{B}}}\left(z_{\mathrm{B}}^{\theta}\right) \\ &= f_{\mathrm{s}}^{-1}\left(\left[f_{\mathrm{c}}\left(z_{\mathrm{B}}^{\theta}\right) - k_{\mathrm{B}}\right] \bmod n\right). \end{aligned} \tag{28}$$

Then maximum likelihood (ML) algorithm is used to demodulate decryption symbols. In the case of the equal prior probability of transmitted symbols, the optimal decision rule is expressed as

$$\hat{s} = \arg\max_{1 \leqslant i \leqslant M} \Pr\left(s_{\mathrm{B}} | s_i\right), \tag{29}$$

where $\Pr\left(s_{\mathrm{B}}|s_i\right)$ is the likelihood function. Finally, channel decoding is utilized to correct error bits to recover message bits.

5 Performance analysis and discussion

In this section, we analyze the security and reliability of the proposed scheme.

5.1 Security analysis

According to Kerckhoff's principle [26], we assume that Eve knows everything about the cryptosystem except secret keys. That is to say, the encryption algorithm and transmission scheme are completely disclosed. The security of communication systems does not depend on the secrecy of algorithms. Specifically, Eve is a capable eavesdropper with capabilities following: (i) knowledge of all steps of key generation and signals transmitted over the public channel; (ii) strong computational and processing power; (iii) knowledge of the modulation type and cipher function.

We focus on information disclose attacks against passive eavesdropping, where attackers try to demodulate the transmitted data correctly. Due to the spatial decorrelation of wireless channels in multipath environments, the eavesdropping channel is independent of the legitimate channel, i.e., $I\left(h_{\mathrm{AB}}, h_{\mathrm{BA}}; h_{\mathrm{AE}}\right) = 0$. Secret keys are extracted directly from the wireless channel. Thus, we have

$$I\left(h_{\mathrm{AB}}, h_{\mathrm{BA}}; h_{\mathrm{AE}}\right) \geqslant I\left(k_{\mathrm{A}}, k_{\mathrm{B}}; k_{\mathrm{E}}\right) = 0. \tag{30}$$

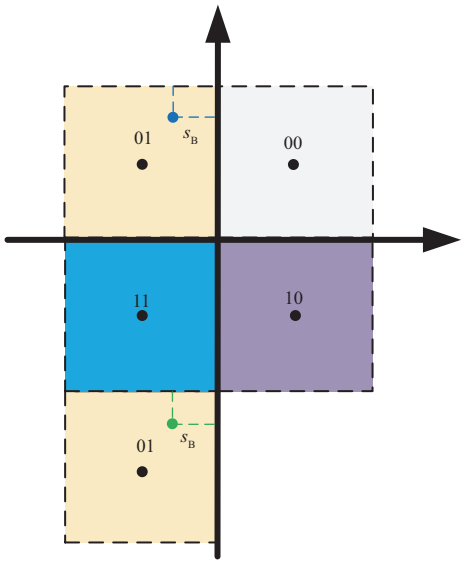

Figure 6 (Color online) Constellation and decision regions for 4-QAM of SOTP secure transmission scheme.

That is, Eve cannot obtain any information about secret keys. According to Theorem 1, the SOTP encryption is perfect secrecy, which means ciphertexts are independent of plaintexts $I(s;c)=0$. Eve's received signal z_{E} forms a Markov chain $s_{\mathrm{A}} \to c \to z_{\mathrm{E}}$. According to the data processing inequality, we have

$$I(s_{\mathrm{A}};c) \geqslant I(s_{\mathrm{A}};z_{\mathrm{E}}) = 0. \tag{31}$$

Accordingly, the proposed SOTP secure transmission scheme can achieve perfect secrecy.

5.2 Reliability analysis

5.2.1 *SER performance*

For simplicity but without loss of generalization, we only analyze the SER of the SOTP secure transmission scheme for QAM signals. The analysis for SER of PSK symbols is similar to QAM, which will be illustrated in the simulation. Specifically, M-ary QAM rectangular constellations can be demodulated according to the $\sqrt{M}$-ASK of the in-phase and quadrature directions, respectively. The in-phase component of the QAM symbol recovered by Bob is given by

$$\begin{aligned} s_{\mathrm{B}}^{\mathrm{Re}} &= \mathrm{Dec}_{k_{\mathrm{B}}^{\mathrm{Re}}}\left(z_{\mathrm{B}}^{\mathrm{Re}}\right) \\ &= f_{\mathrm{s}}^{-1}\left(\left[f_{\mathrm{c}}\left(c_{\mathrm{A}}^{\mathrm{Re}}+\frac{\varepsilon_n^{\mathrm{Re}}}{\beta}\right)-k_{\mathrm{B}}^{\mathrm{Re}}\right] \bmod n\right) \\ &= f_{\mathrm{s}}^{-1}\left(\left[f_{\mathrm{s}}\left(s_{\mathrm{A}}^{\mathrm{Re}}\right)+k_{\mathrm{A}}^{\mathrm{Re}}-k_{\mathrm{B}}^{\mathrm{Re}}+f_{\mathrm{c}}\left(\frac{\varepsilon_n^{\mathrm{Re}}}{\beta}\right)+\frac{\delta L_{\min}}{d_{\min}}\right] \bmod n\right). \end{aligned} \tag{32}$$

For simplicity, the effect of channel fading is ignored in (32), which can be eliminated via channel equalization techniques. Notice that the modulo operation ensures that the ciphertext space is equal to the key space. From another perspective, the modulo operation is equivalent to shifting the decision field on the constellation, as shown in Figure 6.

Therefore, we can perform symbol decisions by observing the positions of constellation points before the modulo operation. The decrypted symbol before the modulo operation is given as

$$\begin{aligned} \tilde{s}_{\mathrm{B}}^{\mathrm{Re}} &= f_{\mathrm{s}}^{-1}\left(f_{\mathrm{s}}\left(s_{\mathrm{A}}^{\mathrm{Re}}\right)+k_{\mathrm{A}}^{\mathrm{Re}}-k_{\mathrm{B}}^{\mathrm{Re}}+f_{\mathrm{c}}\left(\frac{\varepsilon_n^{\mathrm{Re}}}{\beta}\right)+\frac{\delta L_{\min}}{d_{\min}}\right) \\ &= s_{\mathrm{A}}^{\mathrm{Re}}+\frac{k_{\mathrm{A}}^{\mathrm{Re}}-k_{\mathrm{B}}^{\mathrm{Re}}}{\delta}d_{\min}+\frac{\varepsilon_n^{\mathrm{Re}}}{\beta}. \end{aligned} \tag{33}$$

Eq. (33) shows that the error comes from the key difference and added noise. Let

$$\varepsilon^{\mathrm{Re}} = \frac{k_{\mathrm{A}}^{\mathrm{Re}}-k_{\mathrm{B}}^{\mathrm{Re}}}{\delta}d_{\min}+\frac{\varepsilon_n^{\mathrm{Re}}}{\beta} \tag{34}$$

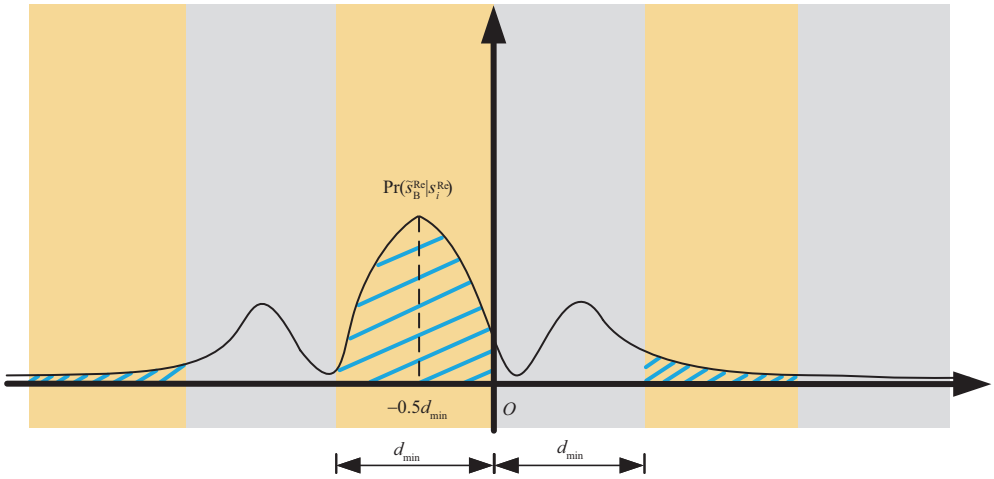

Figure 7 (Color online) Likelihood function and optimal decision regions for 4-QAM of SOTP secure transmission scheme.

be the error in the in-phase direction, which follows the Gaussian mixture distribution (GMM) with probability density function (PDF) $f_{\varepsilon^{\mathrm{Re}}}(u)$. Since the probability of correct detection for the QAM constellation is the product of correct decision probabilities for constituent ASK systems, the SER is written as

$$P_e = 1 - \left(P_{\mathrm{c}}^{\mathrm{Re}}\right)^2, \tag{35}$$

where $P_{\mathrm{c}}^{\mathrm{Re}}$ is the correct decision probability of the in-phase direction. Figure 7 shows the likelihood function of 4-QAM symbols in the in-phase direction (i.e., 2-ASK) and the division of the optimal decision regions. It is worth noting that the modulo operation makes the error decision probability of each symbol the same. For simplicity but without loss of generality, assuming that the prior probability of transmitted symbols is equal, $P_{\mathrm{c}}^{\mathrm{Re}}$ can be written as

$$P_{\mathrm{c}}^{\mathrm{Re}} = \int \Pr\left(\tilde{s}_{\mathrm{B}}^{\mathrm{Re}}|s_i^{\mathrm{Re}}\right) \mathrm{d}\tilde{s}_{\mathrm{B}}^{\mathrm{Re}}. \tag{36}$$

Further, we give the following proposition.

Proposition 1. The SER of the SOTP secure transmission scheme for QAM signals is given by

$$P_e = 1 - \left(\sum_{\lambda\in\mathbb{Z}} \int_{\left(\lambda\sqrt{M}-0.5\right)d_{\min}}^{\left(\lambda\sqrt{M}+0.5\right)d_{\min}} f_{\varepsilon^{\mathrm{Re}}}(u)\,\mathrm{d}u\right)^2, \tag{37}$$

where $f_{\varepsilon^{\mathrm{Re}}}(u) = \sum \Pr(k_{\mathrm{A}}^{\mathrm{Re}} - k_{\mathrm{B}}^{\mathrm{Re}} = \frac{\delta}{d_{\min}}x)\frac{\beta}{\sqrt{\pi\sigma_n^2}}\mathrm{e}^{-\frac{(u-x)^2\beta^2}{\sigma_n^2}}$.

Proof. See Appendix A.

From (37), SER is a function of the quantization level δ. On the one hand, the higher the quantization level, the smaller the quantization interval, and the higher the key disagreement ratio after quantization. On the other hand, increasing the quantization level means that the Euclidean distance between the ciphertext symbols is smaller. Even if the keys of the legitimate communication parties are inconsistent, the difference between the erroneous ciphertexts will be reduced compared with the Euclidean distance of the original symbols. Therefore, to achieve a lower SER, we aim to minimize the SER by adjusting the quantization level δ, subject to transmit power constraints. Accordingly, the problem is formulated as

$$\min_{\delta} P_e \quad \text{s.t. } \delta \in \mathbb{Z}^+,\ 0 < \alpha < 1. \tag{38}$$

Figure 8 presents P_e versus the SNR and δ. We take 16-QAM as the baseband modulation and set $\alpha = 0.5$. Notably, the SER decreases significantly in the high SNR region as δ increases, starting to converge when $\delta > 20$. However, in the low SNR region, $\delta = 1$ achieves better reliability. Therefore, we can dynamically choose the quantization level according to the SNR, that is, choosing a larger δ for high SNR and a smaller δ for low SNR.

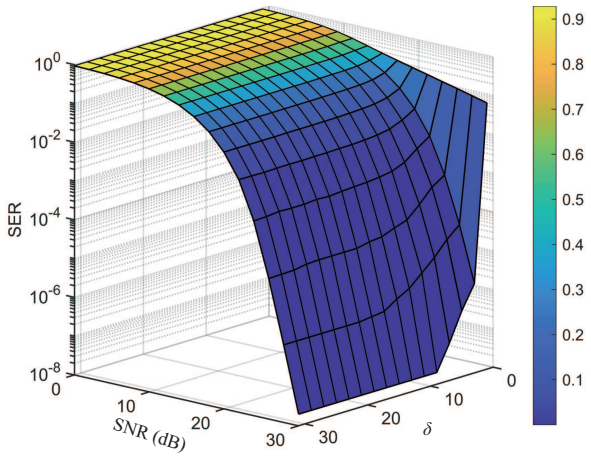

Figure 8 (Color online) SER versus the SNR and quantization level δ.

5.2.2 *Compared with existing schemes*

Based on (38) and Figure 8, we discuss two specific cases: $\delta = 1$ and $\delta \to \infty$. Firstly, we adjust $\delta = 1$ in the low SNR region. When $\delta = 1$, the proposed scheme is equivalent to the BOTP secure transmission scheme [10–13]; i.e., the message bits are first XORed with binary secret keys and then modulated for transmission. When $\delta = 1$, $f_{\varepsilon^{\mathrm{Re}}}(u)$ is simplified as

$$f_{\varepsilon^{\mathrm{Re}}}(u) = \Pr(X=0)\frac{\beta}{\sqrt{\pi\sigma_n^2}}\mathrm{e}^{-\frac{(u)^2\beta^2}{\sigma_n^2}} + \Pr(X=1)\frac{\beta}{\sqrt{\pi\sigma_n^2}}\left(\mathrm{e}^{-\frac{(u-1)^2\beta^2}{\sigma_n^2}} + \mathrm{e}^{-\frac{(u+1)^2\beta^2}{\sigma_n^2}}\right). \tag{39}$$

Further, Eq. (37) is further simplified as

$$P_e = 1 - \left(\sum_{\lambda\in\{-1,0,1\}}\int_{(\lambda\sqrt{M}-0.5)d_{\min}}^{(\lambda\sqrt{M}+0.5)d_{\min}} f_{\varepsilon^{\mathrm{Re}}}(u)\,\mathrm{d}u\right)^2. \tag{40}$$

Next, we consider another case when δ tends to infinity in the high SNR region. The in-phase component of the ciphertext before the modulo operation is given as

$$\begin{aligned}\tilde{c}_{\mathrm{A}}^{\mathrm{Re}} &= f_{\mathrm{c}}^{-1}\left(f_{\mathrm{s}}\left(s_{\mathrm{A}}^{\mathrm{Re}}\right) + k_{\mathrm{A}}^{\mathrm{Re}}\right)\\ &= s_{\mathrm{A}}^{\mathrm{Re}} + f_{\mathrm{c}}^{-1}\left(k_{\mathrm{A}}^{\mathrm{Re}}\right)\\ &= s_{\mathrm{A}}^{\mathrm{Re}} + \frac{k^{\mathrm{Re}}d_{\min}}{\delta} + L_{\min},\end{aligned} \tag{41}$$

where the shift caused by the encryption key is

$$\frac{k^{\mathrm{Re}}d_{\min}}{\delta} + L_{\min} = \frac{k^{\mathrm{Re}}}{n}\sqrt{M}d_{\min} + L_{\min}, \tag{42}$$

where $k^{\mathrm{Re}}/n = \hat{F}_{\hat{h}^{\mathrm{Re}}}(\hat{h}^{\mathrm{Re}})$ is approximately a continuous distribution on $(0,1)$ when $\delta \to \infty$. That is to say, when $\delta \to \infty$, this scheme is equivalent to no longer quantizing CSI but using continuous CSI as secret keys for encryption. After the modulo operation, $c_{\mathrm{A}}^{\mathrm{Re}}$ obeys a uniform distribution on $(-0.5\sqrt{M}d_{\min}, 0.5\sqrt{M}d_{\min})$. Similarly, for the PSK signal, when $\delta \to \infty$, the phase of the ciphertext is a continuous uniform distribution on $(0, 2\pi)$. At this time, the scheme is equivalent to using the continuous channel information to encrypt symbols, as shown in Figures 9 and 10.

Further, the SER when $\delta \to \infty$ in the high SNR region is given in the following proposition.

Proposition 2. When $\delta \to \infty$, the SER in the high SNR region is simplified as

$$P_e = 1 - \mathrm{erf}^2\left(\sqrt{\frac{\pi\gamma_p}{8M}}\right). \tag{43}$$

Proof. See Appendix B.

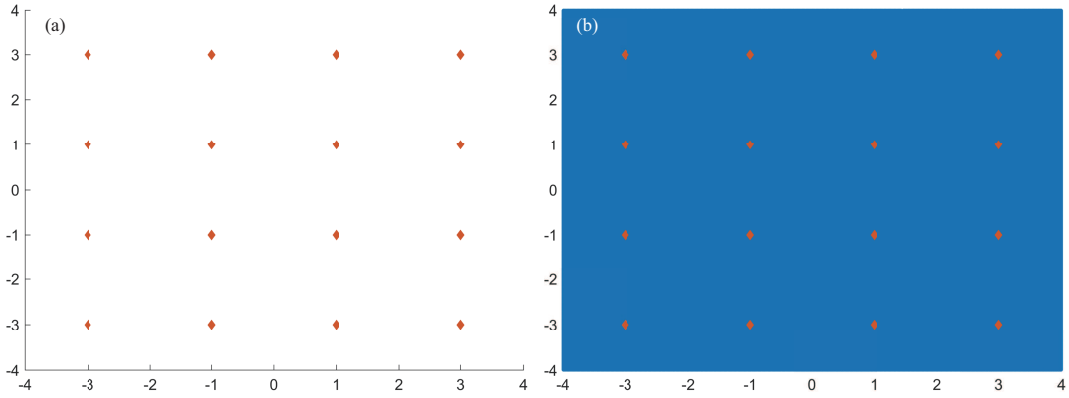

Figure 9 (Color online) QAM constellation diagram with (a) $\delta = 1$ and (b) $\delta \to \infty$.

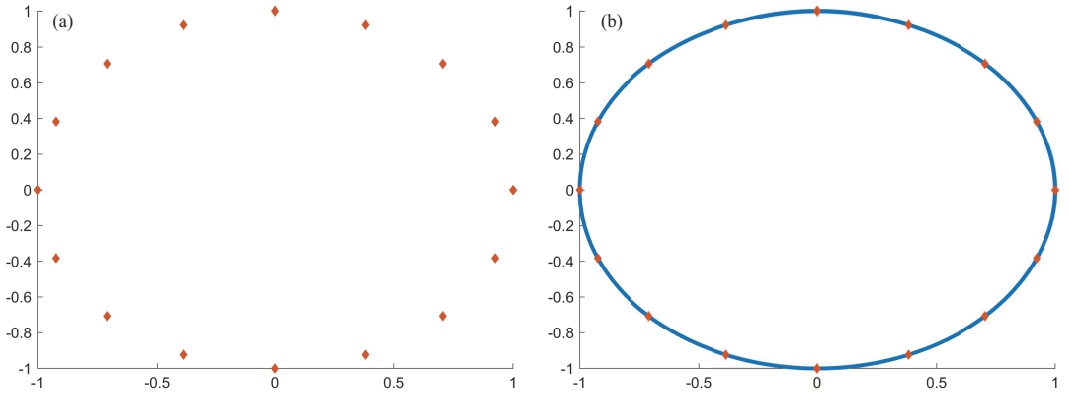

Figure 10 (Color online) PSK constellation diagram with $\delta = 1$ and $\delta \to \infty$.

Table 1 Performance comparison of different transmission schemes

Scheme	Perfect secrecy		BER
	QAM	PSK	
Phase rotation [16–18]	No	Yes	Low
DFT-based PLE [19]	No	Yes	Low
Dynamic mapping [20, 21]	Yes	Yes	High
Noise mask [22, 23]	No	No	–
BOTP secure transmission scheme [10–13]	Yes	Yes	High
Proposed SOTP secure transmission scheme [19]	Yes	Yes	Low

5.3 Discussion

Our proposed scheme unifies existing bit-based OTP and symbol-based encryption schemes. When $\delta = 1$, the scheme is equivalent to the BOTP secure transmission scheme. When $\delta \to \infty$, the scheme is equivalent to the PLE scheme using continuous CSI. Table 1 compares the performance in terms of perfect secrecy and BER. The proposed scheme can achieve perfect secrecy both for QAM and PSK symbols. In addition, the proposed scheme can adjust the quantization level according to the SNR to achieve the optimal BER, which has better reliability than the BOTP secure transmission scheme.

6 Simulation results and performance evaluation

In this section, we present the simulation results along with our analysis.

6.1 Security evaluation

To visually evaluate the security performance of the proposed scheme, we plot constellation diagrams and statistical distribution of Eve's received signals with different PLE schemes, where the black dots represent

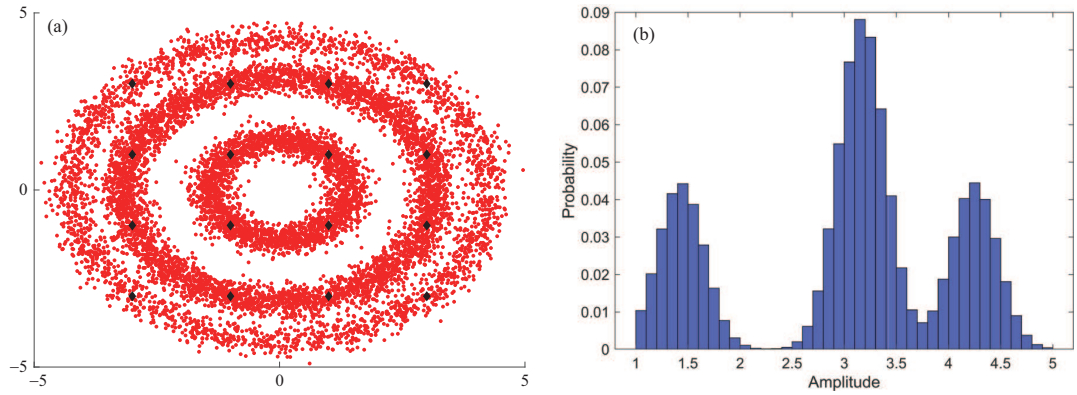

Figure 11 (Color online) Phase rotation scheme in [16]. (a) Constellation diagram; (b) statistical distribution of amplitude.

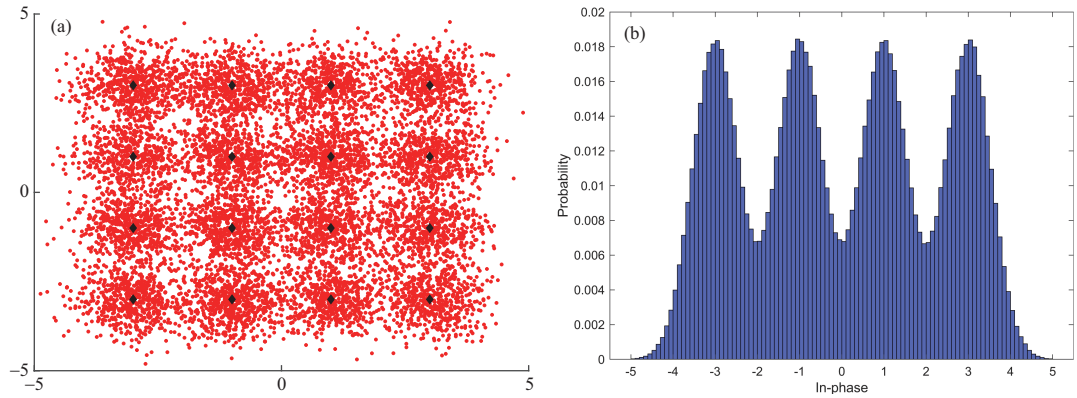

Figure 12 (Color online) Noise mask scheme in [22, 23]. (a) Constellation diagram; (b) statistical distribution of the in-phase component.

original QAM symbols, and the red dots represent symbols received by Eve. For a fair comparison, 16-QAM is used for baseband modulation. The SNR is set to 20 dB and the power allocation factor $\alpha = 0.5$. Obviously, the constellation diagram encrypted via phase rotation has statistical characteristics, as shown in Figure 11. Eve can easily identify the amplitude information of transmitted symbols from the statistical distribution of amplitude. The same problem exists in the noise mask scheme. Although the added noise mask can shift the constellation points in the in-phase and quadrature directions, the encrypted constellation points are not uniformly distributed on the plane because the noise mask obeys the Gaussian distribution, as shown in Figure 12. Eve can distinguish transmitted symbols by using a clustering algorithm. On the contrary, the constellation diagram of the proposed SOTP secure transmission scheme is randomly in the rectangular area, as shown in Figure 13. The statistical distribution of ciphertext symbols in the in-phase and quadrature directions is uniform, so Eve cannot obtain any information from the ciphertext.

Next, to qualitatively evaluate the security performance of the proposed scheme, Figure 14 plots the Shannon capacity of the eavesdropping channel with different transmission schemes. For a fair comparison, we set the same transmission power and power allocation factor $\alpha = 0.5$ for all schemes. Besides, 16-QAM and 16-PSK are taken as baseband modulation. The capacity of the eavesdropping channel is calculated using the mutual information estimators provided by the information-theoretical estimators (ITE) Toolbox [27]. As shown in Figure 14, the eavesdropping channel capacities of BOTP and SOTP secure transmission scheme approach 0, which indicates that the classical bitwise XOR encryption and the proposed symbol-wise OTP encryption scheme can achieve perfect secrecy. Note that the eavesdropping channel capacities of the phase rotation scheme only exhibit perfect secrecy for PSK symbols. This is because only the phase information of symbols is encrypted, but the amplitude information is leaked to Eve. Similarly, Eve can also eavesdrop on partial private information of QAM symbols in the DFT-based PLE scheme [19]. Actually, Eve can perform an inverse discrete Fourier transform (IDFT) on the ciphertext symbols before stealing the leaked amplitude information. For the noise mask-based

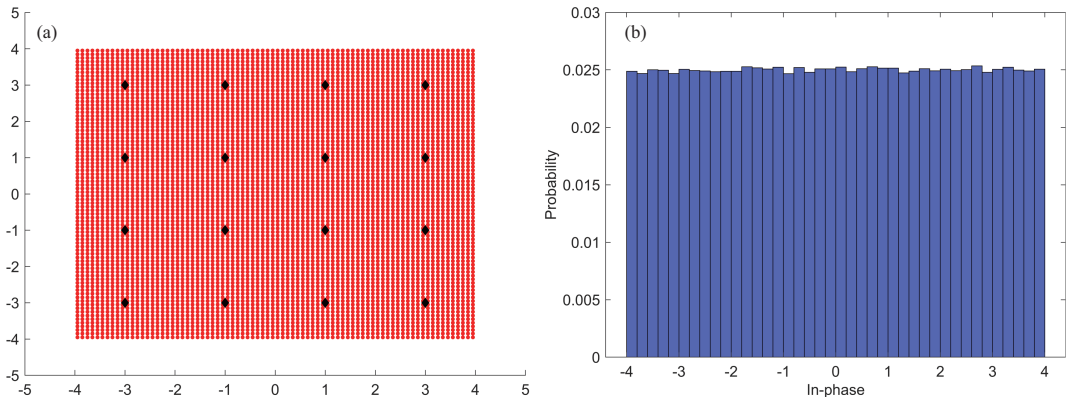

Figure 13 (Color online) Proposed scheme with $\delta = 30$. (a) Constellation diagram; (b) statistical distribution of the in-phase component.

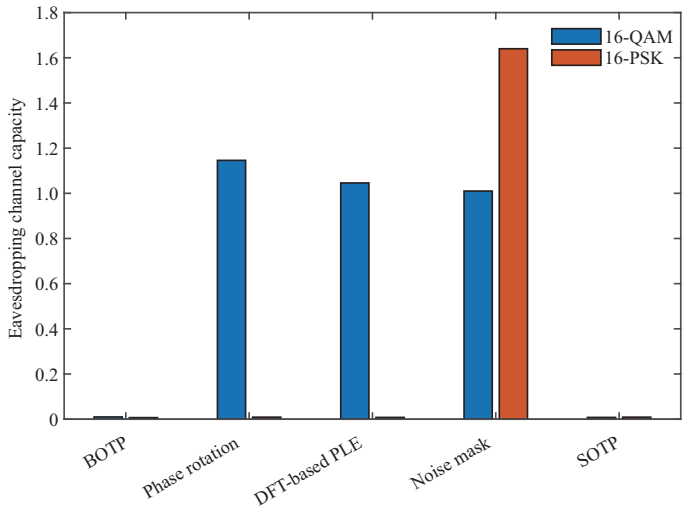

Figure 14 (Color online) Eavesdropping channel capacity of different transmission schemes.

encryption scheme, the effect of the noise mask can be ignored in the high SNR region, failing to protect privacy at the physical layer.

6.2 Reliability evaluation

Figure 15 shows the theoretical and simulated results of SER as a function of quantization level δ. For simplicity but without loss of generalization, we set the power allocation factor $\alpha = 0.5$ and take 16-QAM as baseband modulation. In Figure 15, on the one hand, the simulation results are in excellent agreement with the theoretically derived results. On the other hand, the SER increases gradually with the increase of δ in the low SNR region. While the SER gradually decreases to converge with the rise of δ in the high SNR region. The reason is that when the channel condition is better, the channel estimation error between legitimate communication parties is negligible. If we set $\delta = 1$, once the quantization sequence is mismatched, the tiny channel estimation error will be amplified to the Euclidean distance level error of the constellation points. When a higher or even infinite quantization level (i.e., analog CSI) is selected, the Euclidean distance between the ciphertext symbols is reduced compared with that of original symbols, as shown in Figures 4 and 5. In this case, the decrypted signal is similar to the noisy QAM or PSK signal. That is, the key difference is equivalent to adding extra noise to the QAM or PSK signal. Therefore, the scheme can achieve high reliability when δ is large due to noise immunity similar to QAM and PSK constellations. Conversely, the initial channel estimation error is significant when the poor channel condition. When δ is set higher, the key disagreement ratio will increase, shifting encrypted ciphertext symbols to different decision domains.

To validate the superiority of our proposed scheme, Figure 16 compares the BER performance with

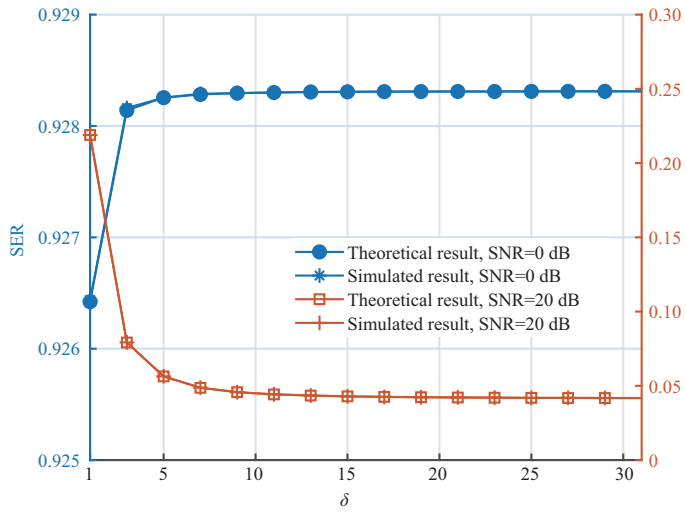

Figure 15 (Color online) Theoretical and simulated results of SER as a function of δ.

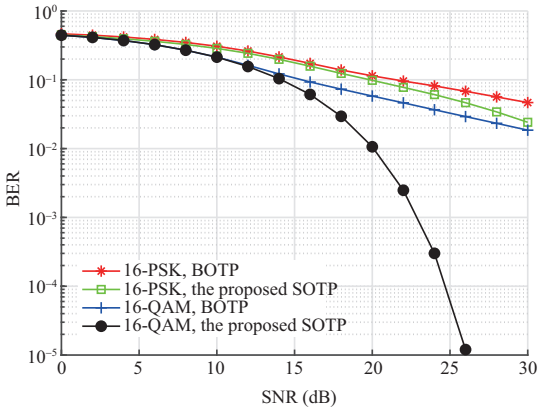

Figure 16 (Color online) BER with different transmission schemes versus SNR.

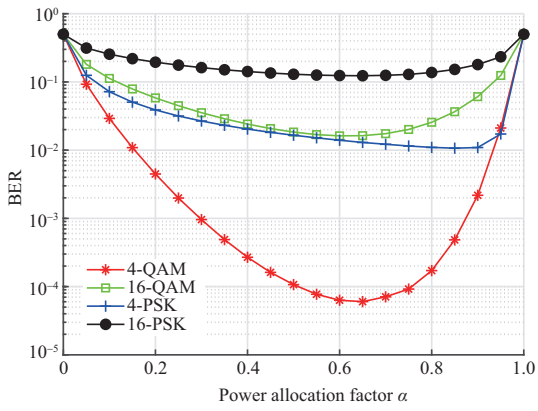

Figure 17 (Color online) BER versus the power allocation factor α.

different transmission schemes versus SNR. We employ Gray-coded mapping as the mapping rule and set the same transmission power for all schemes. In the proposed scheme, we choose the optimal quantization level δ according to the SNR by solving the optimization problem of (38). Our proposed scheme has better BER performance than BOTP secure transmission schemes [10–13]. Especially, under the condition of high SNR, the BER of the proposed scheme is significantly reduced. The reason is that in the BOTP secure transmission scheme, the channel estimation error will be amplified to the level of Euclidean distance of constellation points after quantization and XOR encryption. Our proposed scheme makes the most of the properties of modulation in the complex fields, which converts traditional bit-level encryption in Boolean algebra fields to analog signals mapping in the complex fields. The scheme can dynamically adjust the quantization level according to the SNR, achieving a better reliable performance.

Figure 17 shows BER versus the power allocation factor α. As seen from the figure, whether it is PSK or QAM modulation, the optimal power distribution factor is greater than 0.5. This is because the key difference is an essential cause of bit errors compared with transmission errors, so more power must be allocated for channel estimation.

7 Conclusion

In this paper, combining the advantages of bit encryption and symbol encryption, we propose a modulated symbols-based OTP secure transmission scheme using physical layer keys. Unlike classical key generation and XOR encryption in the discrete binary space, our proposed scheme makes the most of the modulation

properties in the complex fields, which converts traditional bit-level encryption in Boolean algebra fields to analog signals mapping in the complex fields. We provide a specific scheme of physical layer OTP encryption for QAM and PSK symbols based on the wireless channel. The scheme can dynamically adjust the quantization level according to the SNR, achieving a better SER performance. Theoretical analysis and simulation results show that the scheme can achieve secure and reliable transmission.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. U22A2001, 62301608) and National Key Research and Development Program of China (Grant Nos. 2022YFB2902202, 2022YFB2902205).

References

1 Lv L, Li Z, Ding H Y, et al. Secure coordinated direct and untrusted relay transmissions via interference engineering. Sci China Inf Sci, 2022, 65: 182304
2 Vernam G S. Secret signaling system. U.S. Patent 1310719, 1919
3 Shannon C E. Communication theory of secrecy systems. Bell Syst Technical J, 1949, 28: 656–715
4 Sun L, Du Q. Physical layer security with its applications in 5G networks: a review. China Commun, 2017, 14: 1–14
5 Jin L, Hu X, Lou Y, et al. Introduction to wireless endogenous security and safety: problems, attributes, structures and functions. China Commun, 2021, 18: 88–99
6 Gong S X, Tao X F, Li N, et al. Secret key generation over a Nakagami-m fading channel with correlated eavesdropping channel. Sci China Inf Sci, 2022, 65: 192304
7 Wan Z, Huang K, Lou Y, et al. Channel covariance matrix based secret key generation for low-power terminals in frequency division duplex systems. Electron Lett, 2021, 57: 324–327
8 Zhang J, Duong T Q, Marshall A, et al. Key generation from wireless channels: a review. IEEE Access, 2016, 4: 614–626
9 Li G, Zhang Z, Yu Y, et al. A hybrid information reconciliation method for physical layer key generation. Entropy, 2019, 21: 688
10 Peng L, Li G, Zhang J, et al. Securing M2M transmissions using nonreconciled secret keys generated from wireless channels. In: Proceedings of IEEE Globecom Workshops (GC Wkshps), 2018. 1–6
11 Wan Z, Huang K. Non-reconciliation secret keys based secure transmission scheme using polar codes. In: Proceedings of IEEE 5th International Conference on Computer and Communications (ICCC), 2019. 1499–1504
12 Li G, Zhang Z, Zhang J, et al. Encrypting wireless communications on the fly using one-time pad and key generation. IEEE Internet Things J, 2021, 8: 357–369
13 Hu X, Jin L, Huang K, et al. A secure communication scheme based on equivalent interference channel assisted by physical layer secret keys. Secure Commun Networks, 2020. doi: 10.1155/2020/8840645
14 Wang M, Huang K, Wan Z, et al. Non-reconciled physical-layer keys-assisted secure communication scheme based on channel correlation. Entropy, 2022, 24: 1167
15 Bang I, Kim T. Secure modulation based on constellation mapping obfuscation in OFDM based TDD systems. IEEE Access, 2020, 8: 197644–197653
16 Chen B, Zhu C, Li W, et al. Original symbol phase rotated secure transmission against powerful massive MIMO eavesdropper. IEEE Access, 2016, 4: 3016–3025
17 Althunibat S, Sucasas V, Rodriguez J. A physical-layer security scheme by phase-based adaptive modulation. IEEE Trans Veh Technol, 2017, 66: 9931–9942
18 Loganathan L D, Rengaraj R, Konganathan G, et al. Physical layer security using an adaptive modulation scheme for improved confidentiality. IET Commun, 2019, 13: 3383–3390
19 Bi S, Yuan X, Zhang Y J A. DFT-based physical layer encryption for achieving perfect secrecy. In: Proceedings of IEEE International Conference on Communications (ICC), 2013. 2211–2216
20 Mao T, Wang Q, Wen M, et al. Secure single-input-multiple-output media-based modulation. IEEE Trans Veh Technol, 2020, 69: 4105–4117
21 Husain M I, Mahant S, Sridhar R. CD-PHY: physical layer security in wireless networks through constellation diversity. In: Proceedings of IEEE Military Communications Conference, 2012. 1–9
22 Chorti A. Masked-OFDM: a physical layer encryption for future OFDM applications. In: Proceedings of IEEE Globecom Workshops, 2010. 1254–1258
23 Xi C, Gao Y, Nan S, et al. Constellation symbol obfuscation design approach for physical layer security. In: Proceedings of the 10th International Conference on Communication Software and Networks (ICCSN), 2018. 264–269
24 Ma R, Dai L, Wang Z, et al. Secure communication in TDS-OFDM system using constellation rotation and noise insertion. IEEE Trans Consumer Electron, 2010, 56: 1328–1332
25 Xiong T, Lou W, Zhang J, et al. MIO: enhancing wireless communications security through physical layer multiple inter-symbol obfuscation. IEEE Trans Inform Forensic Secur, 2015, 10: 1678–1691
26 Katz J, Lindell Y. Introduction to Modern Cryptography. 2nd ed. Boca Raton: Chapman and Hall/CRC, 2014
27 Szabo Z. Information theoretical estimators toolbox. J Mach Learn Res, 2014, 15: 283–287

Appendix A

Here we derive the SER of SOTP secure transmission scheme. Let

$$X = \frac{k_{\mathrm{A}}^{\mathrm{Re}} - k_{\mathrm{B}}^{\mathrm{Re}}}{\delta} d_{\min} \tag{A1}$$

be the error between secret keys of Alice and Bob; the CDF of X is written as

$$\begin{aligned}
\Pr\left(X = x\right) &= \Pr\left(\frac{k_{\mathrm{A}}^{\mathrm{Re}} - k_{\mathrm{B}}^{\mathrm{Re}}}{\delta} d_{\min} = x\right) \\
&= \sum_{u \in \mathcal{K}} \Pr\left(k_{\mathrm{A}}^{\mathrm{Re}} = u + \frac{x\delta}{d_{\min}}, k_{\mathrm{B}}^{\mathrm{Re}} = u\right) \\
&= \sum_{u \in \mathcal{K}} \Pr\left(F_{\hat{h}_{\mathrm{A}}^{\mathrm{Re}}}^{-1}\left(\frac{x\delta + u d_{\min}}{\sqrt{M}\delta d_{\min}}\right) \leqslant \hat{h}_{\mathrm{A}}^{\mathrm{Re}} < F_{\hat{h}_{\mathrm{A}}^{\mathrm{Re}}}^{-1}\left(\frac{x\delta + (u+1) d_{\min}}{\sqrt{M}\delta d_{\min}}\right), F_{\hat{h}_{\mathrm{B}}^{\mathrm{Re}}}^{-1}\left(\frac{u}{\sqrt{M}\delta}\right) \leqslant \hat{h}_{\mathrm{B}}^{\mathrm{Re}} < F_{\hat{h}_{\mathrm{B}}^{\mathrm{Re}}}^{-1}\left(\frac{u+1}{\sqrt{M}\delta}\right)\right) \\
&= \sum_{u \in \mathcal{K}} \Pr\left(x_1 - h^{\mathrm{Re}} \leqslant \varepsilon_{\mathrm{A}}^{\mathrm{Re}} < x_2 - h^{\mathrm{Re}}, x_3 - h^{\mathrm{Re}} \leqslant \varepsilon_{\mathrm{B}}^{\mathrm{Re}} < x_4 - h^{\mathrm{Re}}\right) \\
&= \sum_{u \in \mathcal{K}} \int_{-\infty}^{\infty} \left[F_{\varepsilon_{\mathrm{A}}^{\mathrm{Re}}}\left(x_2 - v\right) - F_{\varepsilon_{\mathrm{A}}^{\mathrm{Re}}}\left(x_1 - v\right)\right] \left[F_{\varepsilon_{\mathrm{B}}^{\mathrm{Re}}}\left(x_4 - v\right) - F_{\varepsilon_{\mathrm{B}}^{\mathrm{Re}}}\left(x_3 - v\right)\right] f_{h^{\mathrm{Re}}}\left(v\right) \mathrm{d}v.
\end{aligned} \tag{A2}$$

Eq. (A2) holds because the noise at Alice and Bob is independent. Since $\hat{h}_{\mathrm{A}}^{\mathrm{Re}}, \hat{h}_{\mathrm{B}}^{\mathrm{Re}} \sim \mathcal{N}\left(0, 0.5 + 0.5/\gamma_p\right)$, $\varepsilon_{\mathrm{A}}^{\mathrm{Re}}, \varepsilon_{\mathrm{B}}^{\mathrm{Re}} \sim \mathcal{N}\left(0, 0.5/\gamma_p\right)$, and $h^{\mathrm{Re}} \sim \mathcal{N}\left(0, 0.5\right)$, we have

$$F_{\hat{h}_{\mathrm{A}}^{\mathrm{Re}}}^{-1}\left(p\right) = F_{\hat{h}_{\mathrm{B}}^{\mathrm{Re}}}^{-1}\left(p\right) = \sqrt{1 + \gamma_p^{-1}} \mathrm{erf}^{-1}\left(2p - 1\right), \tag{A3}$$

$$F_{\varepsilon_{\mathrm{A}}^{\mathrm{Re}}}\left(z\right) = F_{\varepsilon_{\mathrm{B}}^{\mathrm{Re}}}\left(z\right) = 0.5\left[1 + \mathrm{erf}\left(\frac{z}{\sqrt{\gamma_p^{-1}}}\right)\right], \tag{A4}$$

$$f_{h^{\mathrm{Re}}}\left(v\right) = \frac{1}{\sqrt{\pi}} \mathrm{e}^{-v^2}. \tag{A5}$$

Further, since $\frac{\varepsilon_n^{\mathrm{Re}}}{\beta} \sim \mathcal{N}\left(0, 0.5\sigma_n^2/\beta^2\right)$, $f_{\varepsilon^{\mathrm{Re}}}\left(u\right)$ is given as

$$f_{\varepsilon^{\mathrm{Re}}}\left(u\right) = \sum_{x \in X} \Pr\left(X = x\right) \frac{\beta}{\sqrt{\pi\sigma_n^2}} \mathrm{e}^{-\frac{(u-x)^2\beta^2}{\sigma_n^2}}. \tag{A6}$$

Since $\tilde{s}_{\mathrm{B}}^{\mathrm{Re}} = s_i^{\mathrm{Re}} + \varepsilon^{\mathrm{Re}}$, Eq. (37) is written as

$$\begin{aligned}
P_e &= 1 - \left(\int \Pr\left(\tilde{s}_{\mathrm{B}}^{\mathrm{Re}} | s_i^{\mathrm{Re}}\right) \mathrm{d}\tilde{s}_{\mathrm{B}}^{\mathrm{Re}}\right)^2 \\
&= 1 - \left(\sum_{\lambda \in \mathbb{Z}} \int_{\left(\lambda\sqrt{M} - 0.5\right) d_{\min}}^{\left(\lambda\sqrt{M} + 0.5\right) d_{\min}} f_{\varepsilon^{\mathrm{Re}}}\left(u\right) \mathrm{d}u\right)^2.
\end{aligned} \tag{A7}$$

By substituting (A2) and (A6) into (35), we can obtain Proposition 1.

Appendix B

Here we derive the SER of the SOTP secure transmission scheme when $\delta \to \infty$. In the high SNR region, the error in the transmission can be ignored, so $\varepsilon^{\mathrm{Re}}$ is simplified as

$$\varepsilon^{\mathrm{Re}} = \frac{k_{\mathrm{A}}^{\mathrm{Re}} - k_{\mathrm{B}}^{\mathrm{Re}}}{\delta} d_{\min} = \frac{k_{\mathrm{A}}^{\mathrm{Re}} - k_{\mathrm{B}}^{\mathrm{Re}}}{n} \sqrt{M} d_{\min}, \tag{B1}$$

where $\frac{k_{\mathrm{A}}^{\mathrm{Re}}}{n}, \frac{k_{\mathrm{B}}^{\mathrm{Re}}}{n} \sim \mathcal{U}\left(0, 1\right)$. Let $Y = \frac{k_{\mathrm{A}}^{\mathrm{Re}}}{n} - \frac{k_{\mathrm{B}}^{\mathrm{Re}}}{n}$; the CDF of Y is written as

$$\begin{aligned}
\Pr\left(Y \leqslant y\right) &= \Pr\left(\frac{k_{\mathrm{A}}^{\mathrm{Re}}}{n} - \frac{k_{\mathrm{B}}^{\mathrm{Re}}}{n} \leqslant y\right) \\
&= \int_0^1 \Pr\left(\frac{k_{\mathrm{A}}^{\mathrm{Re}}}{n} - \frac{k_{\mathrm{B}}^{\mathrm{Re}}}{n} \leqslant y | \frac{k_{\mathrm{B}}^{\mathrm{Re}}}{n} = w\right) \Pr\left(\frac{k_{\mathrm{B}}^{\mathrm{Re}}}{n} = w\right) \mathrm{d}w \\
&= \int_0^1 \Pr\left(\hat{h}_{\mathrm{A}}^{\mathrm{Re}} \leqslant F_{\hat{h}_{\mathrm{A}}^{\mathrm{Re}}}^{-1}\left(y + w\right) | \hat{h}_{\mathrm{B}}^{\mathrm{Re}} = F_{\hat{h}_{\mathrm{B}}^{\mathrm{Re}}}^{-1}\left(w\right)\right) \mathrm{d}w \\
&= \int_0^1 \Pr\left(\varepsilon_{\mathrm{A}}^{\mathrm{Re}} - \varepsilon_{\mathrm{B}}^{\mathrm{Re}} \leqslant F_{\hat{h}_{\mathrm{A}}^{\mathrm{Re}}}^{-1}\left(y + w\right) - F_{\hat{h}_{\mathrm{B}}^{\mathrm{Re}}}^{-1}\left(w\right)\right) \mathrm{d}w.
\end{aligned} \tag{B2}$$

When $0 < y \leqslant 1$, Eq. (B2) is further derived as

$$\begin{aligned}
\Pr\left(Y \leqslant y\right) &= \int_0^1 \Pr\left(\varepsilon_{\mathrm{A}}^{\mathrm{Re}} - \varepsilon_{\mathrm{B}}^{\mathrm{Re}} \leqslant F_{\hat{h}_{\mathrm{A}}^{\mathrm{Re}}}^{-1}\left(y + w\right) - F_{\hat{h}_{\mathrm{B}}^{\mathrm{Re}}}^{-1}\left(w\right)\right) \mathrm{d}w \\
&\geqslant \int_0^1 \Pr\left(\varepsilon_{\mathrm{A}}^{\mathrm{Re}} - \varepsilon_{\mathrm{B}}^{\mathrm{Re}} \leqslant 2F^{-1}\left(\frac{y+1}{2}\right)\right) \mathrm{d}w \\
&\geqslant \int_0^1 \Pr\left(\varepsilon_{\mathrm{A}}^{\mathrm{Re}} - \varepsilon_{\mathrm{B}}^{\mathrm{Re}} \leqslant \sqrt{\pi\left(1 + \gamma_p^{-1}\right)} y\right) \mathrm{d}w \\
&\geqslant \Pr\left(\frac{\varepsilon_{\mathrm{A}}^{\mathrm{Re}} - \varepsilon_{\mathrm{B}}^{\mathrm{Re}}}{\sqrt{\pi\left(1 + \gamma_p^{-1}\right)}} \leqslant y\right),
\end{aligned} \tag{B3}$$

where $F^{-1}_{\hat{h}^{\mathrm{Re}}_{\mathrm{A}}}(u) = F^{-1}_{\hat{h}^{\mathrm{Re}}_{\mathrm{B}}}(u) = F^{-1}(u)$. Similarly, when $-1 \leqslant z < 0$, we have

$$\begin{aligned}\Pr(Y \leqslant y) &= \int_0^1 \Pr\left(\varepsilon^{\mathrm{Re}}_{\mathrm{A}} - \varepsilon^{\mathrm{Re}}_{\mathrm{B}} \leqslant F^{-1}_{\hat{h}^{\mathrm{Re}}_{\mathrm{A}}}(y+w) - F^{-1}_{\hat{h}^{\mathrm{Re}}_{\mathrm{B}}}(w)\right)\mathrm{d}w \\ &\leqslant \int_0^1 \Pr\left(\varepsilon^{\mathrm{Re}}_{\mathrm{A}} - \varepsilon^{\mathrm{Re}}_{\mathrm{B}} \leqslant 2F^{-1}\left(\frac{y+1}{2}\right)\right)\mathrm{d}w \\ &\leqslant \int_0^1 \Pr\left(\varepsilon^{\mathrm{Re}}_{\mathrm{A}} - \varepsilon^{\mathrm{Re}}_{\mathrm{B}} \leqslant \sqrt{\pi\left(1+\gamma_p^{-1}\right)y}\right)\mathrm{d}w \\ &\leqslant \Pr\left(\frac{\varepsilon^{\mathrm{Re}}_{\mathrm{A}} - \varepsilon^{\mathrm{Re}}_{\mathrm{B}}}{\sqrt{\pi\left(1+\gamma_p^{-1}\right)}} \leqslant y\right).\end{aligned} \tag{B4}$$

Eqs. (B3) and (B4) hold using the extreme values of the function $F^{-1}(y+w) - F^{-1}(w)$ and $F^{-1}(\frac{y+1}{2})$, respectively. Since $\varepsilon^{\mathrm{Re}}_{\mathrm{A}} - \varepsilon^{\mathrm{Re}}_{\mathrm{B}} \sim \mathcal{N}(0, 1/\gamma_p)$, the distribution of Y can be approximated by a Gaussian distribution with zero mean and variance $1/\pi\gamma_p$ in the high SNR region. Therefore, $\varepsilon^{\mathrm{Re}}$ is further derived as $\varepsilon^{\mathrm{Re}} \sim N\left(0, Md^2_{\min}/(\pi\gamma_p)\right)$. Assuming that Alice transmits s^{Re}_i, the decision field in the in-phase direction is mainly concentrated in $[\frac{2i-\sqrt{M}-2}{2}d_{\min}, \frac{2i-\sqrt{M}}{2}d_{\min}]$. The correct decision probability of the in-phase direction is written as

$$\begin{aligned}P^{\mathrm{Re}}_{\mathrm{c}} &= \int_{\frac{2i-\sqrt{M}-2}{2}d_{\min}}^{\frac{2i-\sqrt{M}}{2}d_{\min}} \Pr\left(s^{\mathrm{Re}}_{\mathrm{B}} | s^{\mathrm{Re}}_i\right)\mathrm{d}s^{\mathrm{Re}}_{\mathrm{B}} \\ &= 2\int_{s^{\mathrm{Re}}_i}^{\frac{2i-\sqrt{M}}{2}d_{\min}} \frac{1}{\sqrt{2\pi M d^2_{\min}/(\pi\gamma_p)}} \mathrm{e}^{-\frac{(s^{\mathrm{Re}}_{\mathrm{B}} - s^{\mathrm{Re}}_i)^2 \pi\gamma_p}{2Md^2_{\min}}}\mathrm{d}s^{\mathrm{Re}}_{\mathrm{B}} \\ &= \mathrm{erf}\left(\sqrt{\frac{\pi\gamma_p}{8M}}\right).\end{aligned} \tag{B5}$$

The SER P_e is further derived as

$$P_e = 1 - \mathrm{erf}^2\left(\sqrt{\frac{\pi\gamma_p}{8M}}\right). \tag{B6}$$