Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 7963451, 10 pages
https://doi.org/10.1155/2018/7963451

*Research Article*

# PHY-Aided Secure Communication via Weighted Fractional Fourier Transform

**Lei Ni**,[1] **Xinyu Da**,[2] **Hang Hu**,[2] **Yuan Liang**,[1] **and Ruiyang Xu**[1]

[1]*Graduate School, Air Force Engineering University, Xi'an 710077, China*
[2]*College of Information and Navigation, Air Force Engineering University, Xi'an 710077, China*

Correspondence should be addressed to Lei Ni; nileikgd@163.com

Received 23 December 2017; Accepted 10 April 2018; Published 15 May 2018

Academic Editor: Gonzalo Vazquez-Vilar



A weighted fractional Fourier transform (WFRFT) based on channel state information (CSI), aiming to safeguard the physical (PHY) layer security of wireless communication system, is proposed. With the proposed scheme, WFRFT is first applied to satellite communications such that the transmitted signal is distorted and can only be neutralized by inverse-WFRFT with the same parameter. Moreover, by exploiting the physical properties of wireless channels, the CSI matrix is transformed as a secret key. In addition, by adding phase rotation (PR) factors to each branch of the WFRFT system, a new unitary matrix with the encryption properties is constructed, and hence, the satellite communications secrecy is reliably guaranteed due to the variation in signal characteristics. Finally, the efficacy of the security enhancement is evaluated in terms of the average bit error rate (BER) and the secrecy capacity. Simulation results show that the proposed encryption method can make the detection and demodulation more difficult for the eavesdropper.

## 1. Introduction

The satellite communications network plays an indispensable role in both civil and military applications. However, due to the openness of wireless communications, malicious receivers within the cover range can illegitimately access the spectrum bands and analyze the transmission without being detected, which makes the confidential message transferred through a satellite communications network vulnerable to eavesdropping attacks [1]. To handle this issue, conventional approaches for data privacy implemented at upper layer protocol stack [2], which mainly focus on the computational complexity of cryptographic algorithms, have been widely used for guaranteeing communication security [3]. However, most of the existing cryptography-based strategies are computationally secure and thus could be compromised when the eavesdropper has powerful computing capability; for example, quantum computing is available [4, 5]. In addition, it is difficult for legitimate user to design an applicable secret key distribution and management protocol to satisfy the great diversity of wireless scenarios.

Without using any encryption, an emerging technique termed as physical (PHY) layer security has attracted considerable interest in recent years [6, 7]. By exploiting the coding techniques as well as physical properties of wireless channels, PHY layer security has a great potential to achieve "perfect secrecy" and is identified as a significant complement to traditional cryptographic techniques [8]. As introduced in [9, 10], the weighted fractional Fourier transform (WFRFT) is performed as a new paradigm for PHY layer security enhancement. WFRFT, known as a novel time-frequency mathematical tool, is proposed by Shih in 1995 for the first time [11]. The WFRFT-based communication system developed in [12, 13], which can be understood as a fusion of single-carrier (SC) and multicarrier (MC) communication system, not only possesses hybrid carrier characteristics with an optimal fractional order over selective fading channels, but also has a good performance of anti-interception [14]. Moreover, WFRFT signal is encrypted with rotation characteristics, which is widely applied to secret communication system in recent years [15, 16].

According to Wyner's wiretap channel model, there exist three participants: the sender Alice, the purpose receiver

Bob, and the eavesdropper Eve, the same as the traditional cryptology. Under this wiretapping model, we assume that the baseband signal modulation scheme is preknown to Eve, and once Eve has unlimited computational capabilities, a potential issue might arise that Eve is likely to get the correct WFRFT parameter $\alpha$ through scanning the parameter of the whole period [17]. Therefore, it is necessary to take more effective measures to protect the WFRFT signal from being cracked. Motivated by the aforementioned aspects, this paper proposes an encryption scheme based on channel state information (CSI) and WFRFT. In general, the WFRFT-based communication system is reconstructed with a new encrypted unitary matrix, which is determined and dynamically encrypted by the CSI, whereby the proposed scheme renders itself with the following advantages: on the one hand, the unique communication nodes of legitimate channel between Bob and Alice can reduce the possibility of secret leakage in the upper layer. On the other hand, the channel needed for transferring the secret key is saved; thus the channel's efficiency is able to be improved.

Numerical simulation results show that the proposed WFRFT-based PHY layer security scheme is able to overcome the shortcomings of the traditional WFRFT system, and the BER of the eavesdropper is kept above 50%. The remainder of this paper is organized as follows. Section 2 reviews the mathematical concepts of WFRFT. Physical implementation process of $\alpha$th order WFRFT as well as the proposed system model is described in Section 3. Simulation results are revealed and discussed in Section 4. Finally, conclusions are addressed in Section 5.

*Notations*. Vectors and matrices are denoted by lower and upper case boldface letters, respectively. $\mathbf{I}$ represents an identity matrix with appropriate size. $(\cdot)^{-1}$ and $(\cdot)^H$ stand for the inverse and Hermitian transpose operations, respectively. Additionally, $Q(\cdot)$ is the complementary distribution function of the standard Gaussian and $Q(x) = (1/\sqrt{2\pi}) \int_x^\infty e^{-u^2/2} du$.

## 2. Preliminary

*2.1. Weighted Fractional Fourier Transform*. Known as a generalized Fourier transform, the discrete Fourier transform (DFT) of $\alpha$th order WFRFT is expressed as [18]

$$\begin{aligned}\mathscr{F}_{4W}^{\alpha}\left[\mathbf{X}_0\right] = {} & \omega_0(\alpha)\mathbf{X}_0 + \omega_1(\alpha)\mathbf{X}_1 + \omega_2(\alpha)\mathbf{X}_2 \\ & + \omega_3(\alpha)\mathbf{X}_3,\end{aligned} \tag{1}$$

where $\{\mathbf{X}_0, \mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3\}$ are the 1~3 times DFT of complex vector $\mathbf{X}_0$, respectively. Furthermore, the DFT can be defined as a form of a matrix

$$\begin{aligned}\mathbf{X} &= \mathrm{DFT}(\mathbf{x}) \\ &= \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & w & \cdots & w^{(N-1)} \\ 1 & w^2 & \cdots & w^{2(N-1)} \\ \vdots & \vdots & & \vdots \\ 1 & w^{(N-1)} & \cdots & w^{(N-1)(N-1)} \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{N-1} \end{bmatrix} \\ &= \mathbf{F}\mathbf{x},\end{aligned} \tag{2}$$

where $\mathbf{F}$ denotes the DFT matrix, and the elements can be written as $\mathbf{F}(j,k) = w^{(j-1)(k-1)}/\sqrt{N}$. Here, $w$ is equal to $e^{-2\pi i/N}$; besides, the weighting coefficients $\omega_l(\alpha)$ in (1) are generated as

$$\omega_l(\alpha) = \frac{1}{4}\sum_{k=0}^{3} \exp\left[\frac{j2\pi(\alpha - l)k}{4}\right], \tag{3}$$

where $l = 1, 2, 3$, and parameter $\alpha$ is with a cycle of 4, commonly selected in the real interval $[0, 4]$. Note that there is only one WFRFT parameter $\alpha$ in (1), which can be called single parameter WFRFT [19].

In addition, (1) can be represented as the following form:

$$\begin{aligned}\mathbf{Y} &= \mathscr{F}_{4W}^{\alpha}\left[\mathbf{X}_0\right] \\ &= \omega_0\mathbf{X}_0 + \omega_1\mathbf{F}\mathbf{X}_0 + \omega_2\mathbf{F}^2\mathbf{X}_0 + \omega_3\mathbf{F}^3\mathbf{X}_0 \\ &= \left(\omega_0\mathbf{I} + \omega_1\mathbf{F} + \omega_2\mathbf{F}^2 + \omega_3\mathbf{F}^3\right)\mathbf{X}_0 \\ &= \mathbf{F}_{4W}(\alpha)\mathbf{X}_0,\end{aligned} \tag{4}$$

where $\mathbf{F}^k$ $(k = 1, 2, 3)$ denotes $k$ times of FFT operation. According to the symmetry of discrete Fourier transform, we can obtain $\mathbf{F}^2 = \mathbf{M}$ and $\mathbf{F}^3 = \mathbf{F}^H$, where $\mathbf{M}$ represents a permutation matrix and can be denoted by

$$\mathbf{M} = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ \vdots & \cdots & 0 & \iddots & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}_{N\times N}. \tag{5}$$

It can be readily verified that $\mathbf{F}_{4W}(\alpha)$ in WFRFT-based communication system is a unitary matrix; besides, the DFT matrix utilized in the orthogonal frequency division multiplexing (OFDM) system is also a unitary matrix. Motivated by this property, in this paper, we consider constructing a new encrypted unitary matrix in WFRFT system to improve the secrecy performance.

*2.2. Encrypted Unitary Matrix.* According to the operational properties of unitary matrix, a new unitary matrix can be derived by multiplying a unitary matrix and a permutation matrix. The construction method of our scheme is described as follows.

First of all, we denote $\mathbf{P}$ as the unitary matrix that needs to be extended.

*Definition 1* (permutation matrix). The necessary and sufficient condition for a permutation matrix $\mathbf{T}$ is that each row or column of $\mathbf{T}$ has only one element equal to one, and the other elements are all zeros.

**Theorem 2.** *Let* $\mathbf{U}$ *be the upper (lower) triangular unitary matrix, then* $\mathbf{U}$ *must be a diagonal matrix satisfying* $|\det(\mathbf{U})| = 1$.

*Definition 3* (PR matrix). The necessary and sufficient condition for a PR matrix $\mathbf{E}$ with $N \times N$ size is that the $(n, n)$ element equals $e^{j2\pi\theta(n,n)}$ $(n = 1, 2, \ldots, N)$, where $\theta(n, n)$ can be chosen in $[0, 1]$, and the other elements of $\mathbf{E}$ are all zeros. It can be observed that the total number of rotation matrices is $N^N$ [20].

Secondly, creating a new unitary matrix $\mathbf{Z} = \mathbf{P} \times \mathbf{E} \times \mathbf{T}$, the original unitary matrix $\mathbf{P}$ can be either a square or a nonsquare matrix theoretically. Since the matrix $\mathbf{F}_{4W}(\alpha)$ in WFRFT system is a unitary matrix, we consider reconstructing $\mathbf{F}_{4W}(\alpha)$ to form a new unitary matrix to enhance the secrecy performance.

In (4), $\mathbf{F}_{4W}(\alpha)$ can be obtained by multiplying a block matrix $\left[\mathbf{I}\ \mathbf{F}\ \mathbf{M}\ \mathbf{F}^H\right]^H$ with a coefficients matrix $[\omega_0(\alpha)\ \omega_1(\alpha)\ \omega_2(\alpha)\ \omega_3(\alpha)]$; since both the block matrix and $\mathbf{F}_{4W}(\alpha)$ are unitary matrices, we can derive that $[\omega_0(\alpha)\ \omega_1(\alpha)\ \omega_2(\alpha)\ \omega_3(\alpha)]$ is also a unitary matrix. To make it easier for practical implementation, a PR matrix $\mathbf{E}$ with $4 \times 4$ size and a permutation matrix $\mathbf{T}$ with $4 \times 4$ size are designed, respectively.

Finally, the new unitary matrix can be calculated as

$$\begin{aligned}\mathbf{Z}_{4W}(\alpha) = {} & [\omega_0(\alpha)\ \omega_1(\alpha)\ \omega_2(\alpha)\ \omega_3(\alpha)] \times \mathbf{E} \times \mathbf{T} \\ & \times \left[\mathbf{I}\ \mathbf{F}\ \mathbf{M}\ \mathbf{F}^H\right]^H;\end{aligned} \tag{6}$$

moreover, the inverse matrix is expressed by

$$\begin{aligned}\mathbf{Z}_{4W}(\alpha)^{-1} = {} & \left[\mathbf{I}\ \mathbf{F}\ \mathbf{M}\ \mathbf{F}^H\right] \times \mathbf{T}^H \times \mathbf{E}^H \\ & \times [\omega_0(\alpha)\ \omega_1(\alpha)\ \omega_2(\alpha)\ \omega_3(\alpha)]^H,\end{aligned} \tag{7}$$

where the PR matrix $\mathbf{E}$ is composed of four diagonal elements $e^{j2\pi\theta(k,k)}$ $(k = 1, 2, 3, 4)$.

Considering that Bob needs to calculate the transpose of $\mathbf{T}$, without loss of generality, we adopt the unit matrix $\mathbf{I}$ as this permutation matrix for simplicity. Therefore, the generation of the PR matrix becomes the key to the construction of this new encrypted unitary matrix.

## 3. Encrypted Unitary Matrix Based on CSI

*3.1. Channel State Information Encryption.* Due to the inherent nature of wireless communications, the uniqueness and short-time reciprocity of the channel make it possible for legitimate user to distribute secret key reliably. In addition, the secure transmission between legitimate users can be guaranteed by exploiting the spatial difference between Bob and Eve. Therefore, we can employ these properties to protect the confidential messages that need to be transmitted, and the specific conversion methods are described in the following subsections.

Firstly, Bob sends a training array to Alice, and Alice takes advantage of it to estimate the CSI of legitimate channel. Meanwhile, Bob estimates the CSI through the pilot sequence sent by Alice. It is assumed that the CSI is perfect at the legitimate transmitter; thus the CSI matrices estimated by Alice and Bob are completely identical. Under this assumption, it is necessary to convert the estimated legitimate CSI into a secret key by certain means. In this paper, the single Hash function [21], as a frequently used method in the encryption algorithms, is introduced. The single Hash function can be generalized as

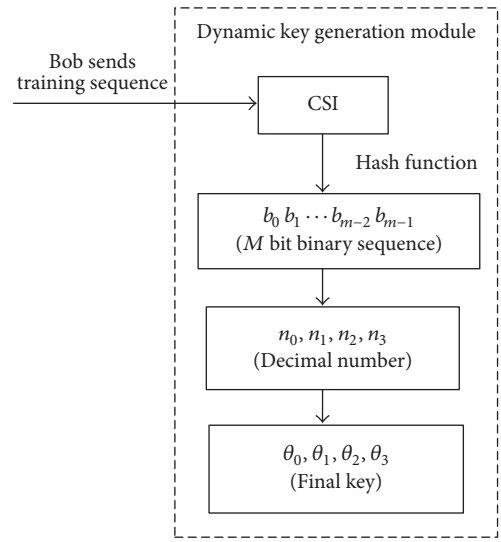



Figure 1: Flow chart of key generation method.

$$h = H(L), \tag{8}$$

where $h$ is the fixed-length Hash value, $H(\cdot)$ is a one-way Hash function, and $L$ denotes the input sequence of arbitrary length.

The mapping of the compression function can help us to convert any variable length input string into a fixed-length output string. Moreover, the Hash function has a good performance in collision-resistance and the uniformity of mapping distribution. According to the previous analyses, we can utilize the Hash function to map the estimated CSI matrix into a bit string with fixed length, and due to the one-way property of the Hash function, even if the key sequence is known by Eve, the correct CSI matrix cannot be obtained.

In this paper, two main Hash algorithms are proposed: MD5 and SHA-1 algorithm [22], then we can convert the CSI matrix into a binary sequence of 128 bits or 160 bits. Moreover, the four diagonal elements of the PR matrix $\mathbf{E}$ can be derived by transforming the binary key sequence into the decimal numbers; these four decimal numbers $n_1$, $n_2$, $n_3$, $n_4$ are of paramount importance for the PR matrix $\mathbf{E}$ and the corresponding phase factors can be calculated by the following equation:

$$\theta_k = \frac{n_k}{2^{32}} \times 2\pi \quad k = 0, 1, 2, 3. \tag{9}$$

However, there are many ways to convert binary bits into four decimal numbers, considering that the receiver needs to obtain encrypted unitary matrix with the same size; the 128 bits are divided into four groups in our work, then the binary bits of each group are converted to four decimal numbers. Figure 1 demonstrates the generation method for the secret key.

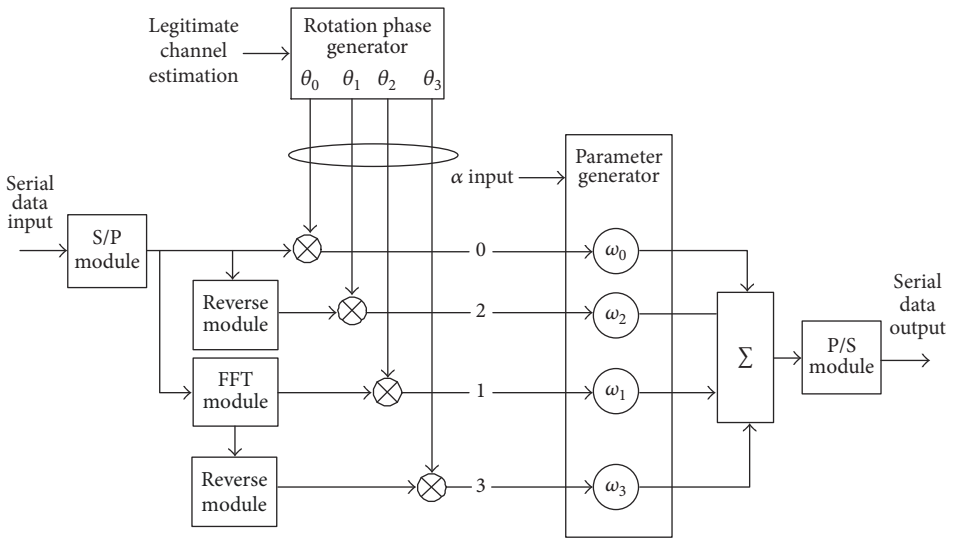



Figure 2: Generation of the constellation scrambling sequence.

For any $\mathbf{E} = \begin{bmatrix} e^{j\theta_0} & & & \\ & e^{j\theta_1} & & \\ & & e^{j\theta_2} & \\ & & & e^{j\theta_3} \end{bmatrix}$, $\boldsymbol{\theta} = [\theta_0, \theta_1, \theta_2, \theta_3]$, the new unitary matrix $\mathbf{Z}_{4W}(\alpha, \boldsymbol{\theta})$ can be calculated according to

$$\begin{aligned} \mathbf{Z}_{4W}(\alpha, \boldsymbol{\theta}) &= \left[\omega_0(\alpha) \;\; \omega_1(\alpha) \;\; \omega_2(\alpha) \;\; \omega_3(\alpha)\right] \times \mathbf{E} \times \mathbf{T} \\ &\quad \times \left[\mathbf{I} \;\; \mathbf{F} \;\; \mathbf{M} \;\; \mathbf{F}^H\right]^T \\ &= \omega_0(\alpha) e^{j\theta_0}\mathbf{I} + \omega_1(\alpha) e^{j\theta_1}\mathbf{F} + \omega_2(\alpha) e^{j\theta_2}\mathbf{M} \\ &\quad + \omega_3(\alpha) e^{j\theta_3}\mathbf{F}^H, \end{aligned} \tag{10}$$

where $\mathbf{T} = \mathbf{I}$, and the corresponding decryption matrix is expressed as

$$\begin{aligned} \left[\mathbf{Z}_{4W}(\alpha, \boldsymbol{\theta})\right]^{-1} &= \omega_0(-\alpha) e^{-j\theta_0}\mathbf{I} + \omega_1(-\alpha) e^{-j\theta_3}\mathbf{F} \\ &\quad + \omega_2(-\alpha) e^{-j\theta_2}\mathbf{M} + \omega_3(-\alpha) e^{-j\theta_1}\mathbf{F}^H. \end{aligned} \tag{11}$$

It is readily known that the inverse matrix $\mathbf{F}_{4W}(\alpha)^{-1}$ can be obtained by changing the input parameter $\alpha$; that is, $\mathbf{F}_{4W}(\alpha)^{-1} = \mathbf{F}_{4W}(-\alpha)$. However, the deduction process of (10) and (11) shows that the new unitary matrix does not have such property; that is, $\mathbf{Z}_{4W}(-\alpha, \boldsymbol{\theta}) \neq [\mathbf{Z}_{4W}(\alpha, \boldsymbol{\theta})]^{-1}$. Therefore, even if the WFRFT parameter $\alpha$ is known to Eve, the original $\mathbf{X}_0$ cannot be directly neutralized at the nonpurpose receiver.

Figure 2 depicts the generation of the constellation scrambling sequence. The input data symbols are divided into four subchannels by using a serial to parallel (S/P) converter, and the WFRFT operation is implemented through one FFT module and two reverse modules. It should be noticed that the WFRFT still holds its properties after phase rotation and the PR factors are added to each branch of WFRFT system for further changing the paradigm of transmitted signal, thus making the detection and demodulation more difficult for the Eve.

*3.2. Signal Model Based Encrypted Unitary Matrix.* The block diagram of the WFRFT-based communication system based on a new encrypted unitary matrix is depicted in Figure 3. After modulation of the input sequence $\mathbf{X}_0$, the baseband symbol can be represented as

$$\begin{aligned} \mathbf{S}_0 &= \mathbf{Z}_{4W}(\alpha, \boldsymbol{\theta})\mathbf{X}_0 \\ &= \omega_1(\alpha) e^{j\theta_1}\mathbf{X}_0 + \omega_3(\alpha) e^{j\theta_3}\mathbf{X}_1 + \omega_2(\alpha) e^{j\theta_2}\mathbf{X}_2 \\ &\quad + \omega_0(\alpha) e^{j\theta_0}\mathbf{X}_3, \end{aligned} \tag{12}$$

where the transmitting signal $\mathbf{S}_t = \mathbf{S}_0 + \mathbf{n}$ and $\mathbf{n}$ is the additive white Gaussian noise (AWGN).

Similarly, from the legitimate receiver's side, we can retrieve the original transmitting sequence by using the parameter $-\alpha$ and $\boldsymbol{\theta}$. The original input data then can be obtained after the demodulation. In general, our proposed scheme is determined and dynamically encrypted by the CSI, which can lead to a better PHY layer security performance.

$$\begin{aligned} \mathbf{Y}_0 &= \left[\mathbf{Z}_{4W}(\alpha, \boldsymbol{\theta})\right]^{-1}\mathbf{S}_t = \left[\mathbf{Z}_{4W}(\alpha, \boldsymbol{\theta})\right]^{-1}(\mathbf{S}_0 + \mathbf{n}) \\ &= \omega_0(-\alpha) e^{-j\theta_0}\mathbf{I}\mathbf{S}_0 + \omega_1(-\alpha) e^{-j\theta_3}\mathbf{F}\mathbf{S}_0 \\ &\quad + \omega_2(-\alpha) e^{-j\theta_2}\mathbf{M}\mathbf{S}_0 + \omega_3(-\alpha) e^{-j\theta_1}\mathbf{F}^H\mathbf{S}_0 + \mathbf{n}' \\ &= \omega_0(-\alpha) e^{-j\theta_0}\mathbf{S}_0 + \omega_1(-\alpha) e^{-j\theta_3}\mathbf{S}_1 \\ &\quad + \omega_2(-\alpha) e^{-j\theta_2}\mathbf{S}_2 + \omega_3(-\alpha) e^{-j\theta_1}\mathbf{S}_3 + \mathbf{n}'. \end{aligned} \tag{13}$$

*3.3. Security Performance of Proposed Model.* In this paper, it is assumed that the new unitary matrix encrypted WFRFT is preshared by legitimate users but traditional WFRFT is performed by illegitimate user. In (1), the first item is the objective signal, and the other three can be regarded as the

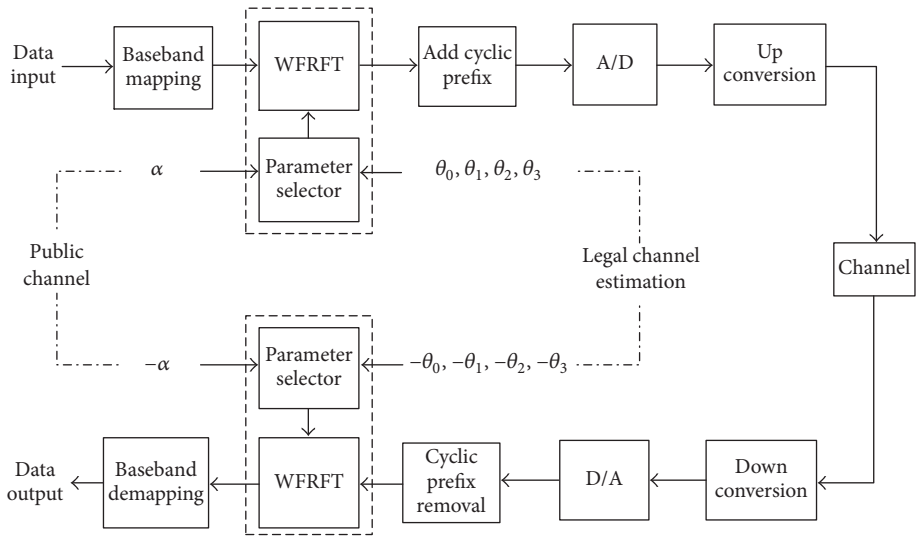



Figure 3: Architecture of the WFRFT-based PHY layer security system.

noise for Eve. Note that $\mathbf{X}_0$ and its 0~3 times DFT $\mathbf{X}_l$ ($l = 1, 2, 3$) have the same power $P$. Due to the diffusion and confusion property of the constellation, which is affected by the coefficients of WFRFT and the superposition of four basic signals in (1), symbols at Eve deviate from the original constellation points by a certain phase $\theta_{\text{rotation}}$. Then, the rotation phase can be rewritten as

$$\theta'_{\text{rotation}} = \theta_{\text{rotation}} + \theta_{\text{random}}, \tag{14}$$

where $\theta_{\text{random}}$ is determined by the channel state information. Typically, the impact factor is $\cos^2\theta'_{\text{rotation}} = \cos^2(3\pi\alpha/4 + \theta_{\text{random}})$ for the illegal receiver [17].

Moreover, the equivalent signal after performing WFRFT is given by

$$P_e = |\omega_0|^2 \cos^2\left(\frac{3\pi\alpha}{4} + \theta_{\text{random}}\right) P_b, \tag{15}$$

then, the equivalent power $P_e$ satisfies

$$\begin{aligned} P_e &= |\omega_0|^2 \cos^2\left(\frac{3\pi\alpha}{4} + \theta_0\right) P \\ &= \cos^2\frac{\pi\alpha}{4}\cos^2\frac{\pi\alpha}{2}\cos^2\left(\frac{3\pi\alpha}{4} + \theta_{\text{random}}\right) P_b. \end{aligned} \tag{16}$$

The BER at the illegal receiver with M-APSK modulation can be expressed as

$$\mathscr{P}_e = (M-1)\, Q\left(\sqrt{\frac{d_{\min}^2}{2} \cdot \frac{\cos^2(\pi\alpha/4)\cos^2(\pi\alpha/2)\cos^2(3\pi\alpha/4 + \theta_{\text{random}})}{1 - \cos^2(\pi\alpha/4)\cos^2(\pi\alpha/2)\cos^2(3\pi\alpha/4 + \theta_{\text{random}}) + 1/\text{SNR}_b}}\right), \tag{17}$$

where $M$ indicates the order of modulation, $\text{SNR}_b$ is the signal-to-noise ratio of the legitimate receiver, and $d_{\min}$ denotes the minimum Euclidean distance of M-APSK signal.

In addition to the BER, the secrecy capacity is also an important evaluation index considered in the proposed system. It stands for the limits on the amount of messages that can be reliably transferred in a way that an illegitimate receiver cannot decode the information. According to [23, 24], it is defined as

$$C = C_b - C_e, \tag{18}$$

where $C_b = \log_2(1 + P_b/N_b)$ and $C_e = \log_2(1 + P_b/N_b)$ are the channel capacity of the legitimate receiver and the illegitimate receiver, separately. $P_b/N_b$ and $P_e/N_e$ are signal-to-noise ratio at the legitimate and the illegitimate receiver correspondingly.

For our proposed system, the secrecy capacity is given out

$$\begin{aligned} C = \log_2\left(1 + \frac{P_b}{N_b}\right) - \log_2\Bigg(1 \\ + \frac{|\omega_0|^2 \cos^2(3\pi\alpha/4 + \theta_{\text{random}})\, P_b}{\left[1 - |\omega_0|^2 \cos^2(3\pi\alpha/4 + \theta_{\text{random}})\right] P_b + N_e}\Bigg). \end{aligned} \tag{19}$$

From the perspective of the illegitimate receiver, the signal-to-noise ratio will become constantly low; thus $C$

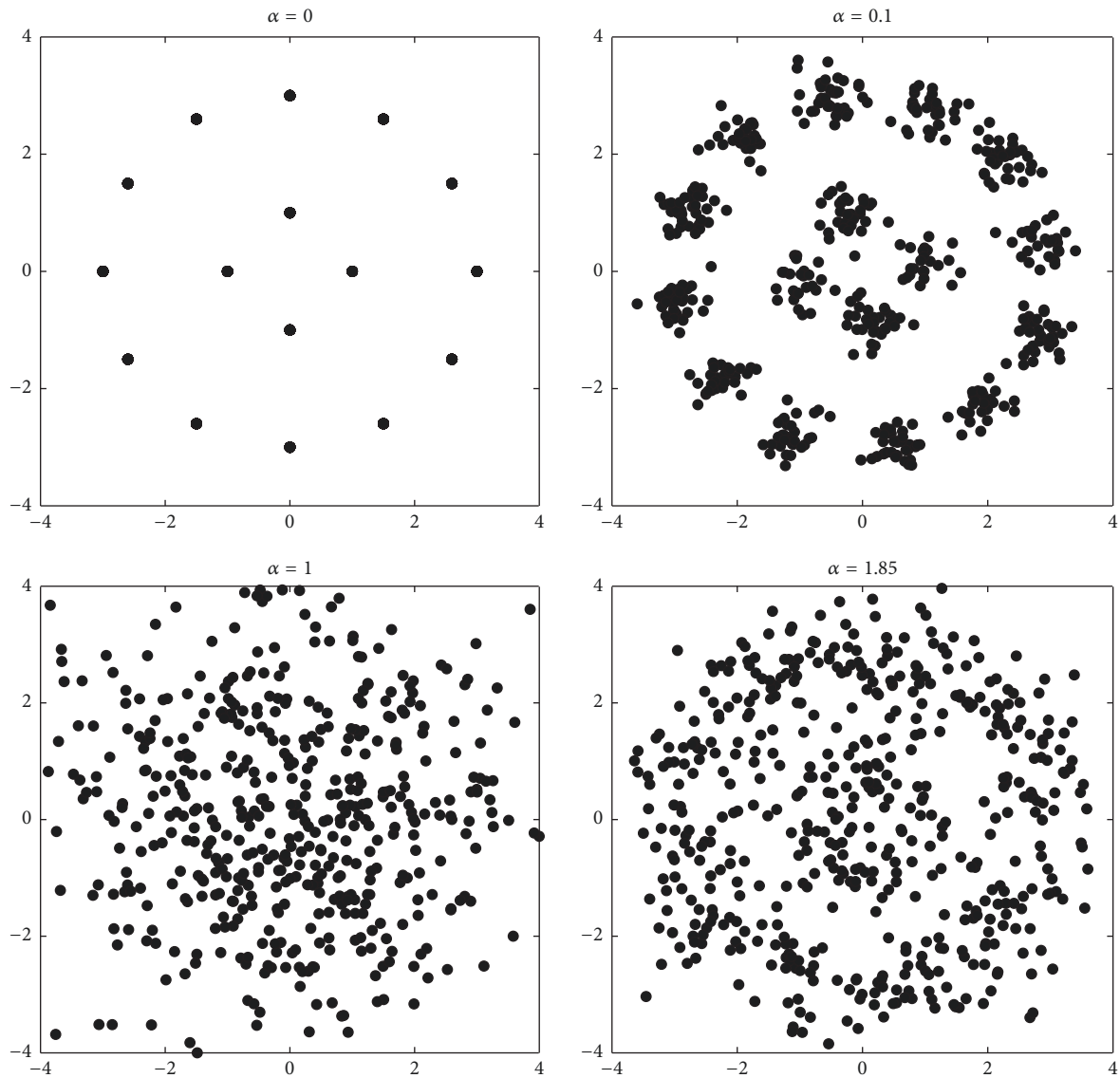



Figure 4: The constellation diagram of WFRFT signal.

will become larger. The larger $C$ is, the more secure the transmission will be.

## 4. Simulation Results

In this section, numerical simulation results are provided to evaluate the secrecy performance of our proposed WFRFT-based PHY layer security scheme. Since high-order modulation is widely applied to the satellite communications, the uncoded APSK modulation is adopted in the following examples, and we evaluate the BER of proposed system with block length of $N = 1024$. $\boldsymbol{\theta}$ is a random generated PR vector. In addition, we set the premises that the mechanism of WFRFT method is known by the illegal Eve, including WFRFT parameter $\alpha$, and Eve attempts to neutralize the transmitted satellite signal in wireless media.

*4.1. Constellation Scrambling of the Signal.* In the first experiment, we analyze the constellation scrambling of WFRFT signal with $\alpha = 0, 0.1, 1, 1.85$. Figure 4 shows the constellation diagram of single parameter WFRFT, and Figure 5 depicts the constellation diagram of APSK signal after the implementation of encrypted WFRFT.

Comparing to the single parameter WFRFT, the constellation distribution of the encrypted WFRFT-APSK signal has a larger range of diffusion with the same order $\alpha$. Furthermore, it can be observed that the aliasing effect of the constellation is better; that is to say, the signal constellation spreads faster after the implementation of encrypted WFRFT. This change would be beneficial for security promotion. In particular, when $\alpha = 1$, the constellation of the original signal is fully confused, and the constellation diagram of the signal is closer to the Gaussian distribution on the complex plane.

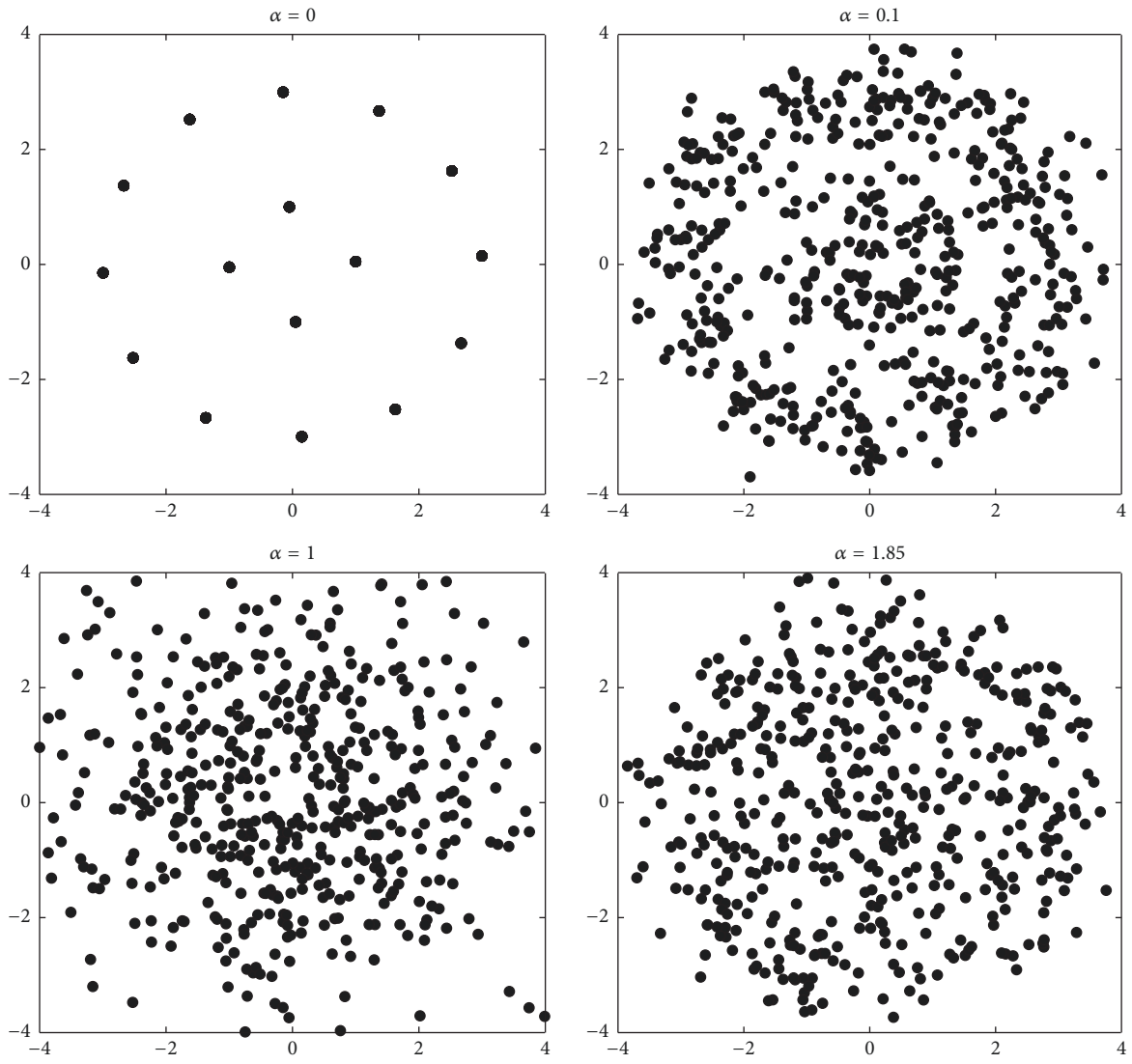



Figure 5: The constellation diagram of encrypted WFRFT-APSK signal.

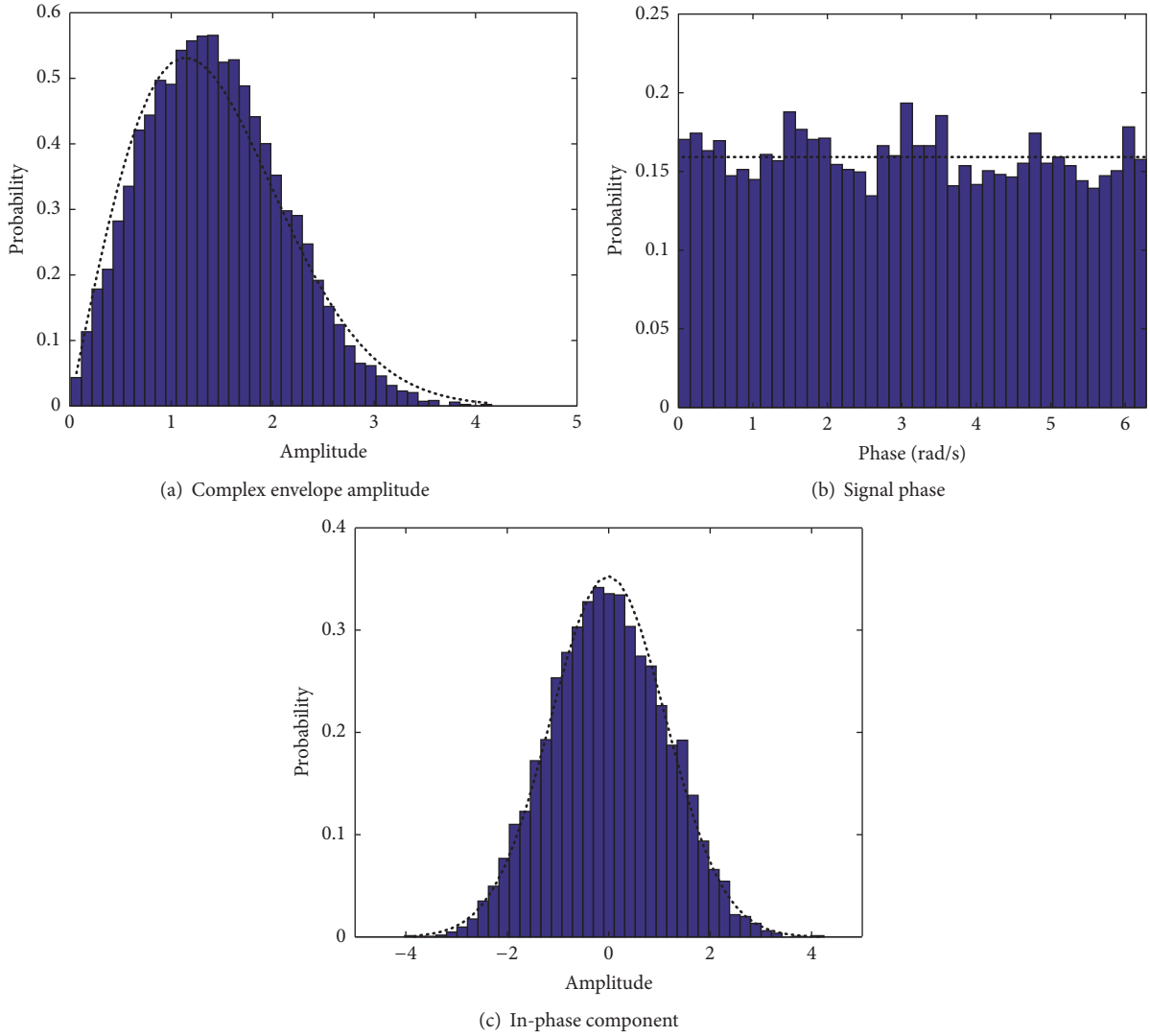
*4.2. Statistical Properties of the Signal.* The modulation identification based on high-order cumulant is being treated as an auspicious technique for blind signal detection. However, the high-order cumulant is insensitive to add-Gaussian noise, and the high-order cumulant for Gaussian signal is always zero, which makes this signal detection method invalid. Therefore, if the characteristics of modulation signal are similar to those of Gaussian noise, it could be considered that the signal has better antidetection ability and security performance.

Figures 6(a)–6(c) show the statistical results of our encrypted WFRFT signal and the degree of approximation to Gaussian signal. In the simulations, the input mapped 16APSK signals are adopted and the WFRFT parameter $\alpha$ is set to 1. Figure 6(a) depicts the statistical result of the complex envelope amplitude of the signal, Figure 6(b) exhibits the phase statistical property of the signal, and Figure 6(c) reveals the distribution of the in-phase component of the signal.

In Figure 6(a), the black dotted line represents the probability density curve of Rayleigh distribution with the same mean and variance as the signal envelope. In Figure 6(b), the black dotted line indicates a uniform distribution with a probability density of $1/2\pi$. In Figure 6(c), the black dotted line denotes the probability density curve of Gaussian distribution with the same mean and variance as the statistical in-phase component of the signal.

It is visible from the simulation results that the statistical complex envelope of the encrypted WFRFT-APSK signal is fitted to the Rayleigh distribution, and the phase distribution of the signal is uniform. Moreover, the distribution of the in-phase component of the signal is very close to the Gaussian distribution, which indicates that the modulation signal can achieve "covert communication" by resisting the detection and interception of the eavesdropper.

*4.3. Security Performance of the System.* Figure 7 depicts the BER performances at the illegal receiver and the legitimate




(a) Complex envelope amplitude

(b) Signal phase

(c) In-phase component

Figure 6: WFRFT-APSK signal statistical properties.

receiver with $\alpha = 0.3$ and $\alpha = 0.8$. The uncoded 16PSK, 16QAM, and 16APSK modulation signals are considered. It can be observed that no matter which modulation mode is adopted, the BER at Eve is maintained between 0.4 and 0.5, which indicates that the illegal receiver can hardly get any reliable messages intended for the legitimate receiver. For Bob, the proposed scheme is suitable for common scenarios without deteriorating the BER performance. In general, the proposed encryption method can guarantee the satellite communications system with additional security, which is crucial for military and dedicated communications.

Figure 8 shows the secrecy capacity of proposed system with $\mathrm{SNR}_b = -10, 0, 10$ dB. In this paper, it is assumed that there is only one legitimate user and one illegal user in the wiretap channel model, and each user is equipped with a single antenna. It can be seen that the secrecy capacity is constantly a positive value when $\mathrm{SNR}_b > 0$ dB with any $\alpha$ selected in the real range $[0, 4]$, which means that the proposed scheme can guarantee the security of the communication effectually. Besides, let $\mathrm{SNR}_b = 10$ dB, the proper selection range of $\alpha$ becomes smaller, and secure communication can be obtained in $[0.2, 3.8]$.

## 5. Conclusions

The WFRFT signal has a good performance of low probability of interception; however, the antiscanning characteristic also indicates that the WFRFT method is based on a large amount of computation. To avoid the eavesdropper intercepting transmission by using exhaustive search method, this paper proposes an encrypted modulation scheme based on the unique legitimate CSI. The simulation results show that the APSK signal after performing the new unitary matrix has better antiscanning characteristics on the basis of maintaining the constellation characteristics and statistical properties of the original WFRFT signal. In general, the nonpurpose receiver cannot demodulate the useful signal correctly even if the WFRFT parameter $\alpha$ is being decoded.

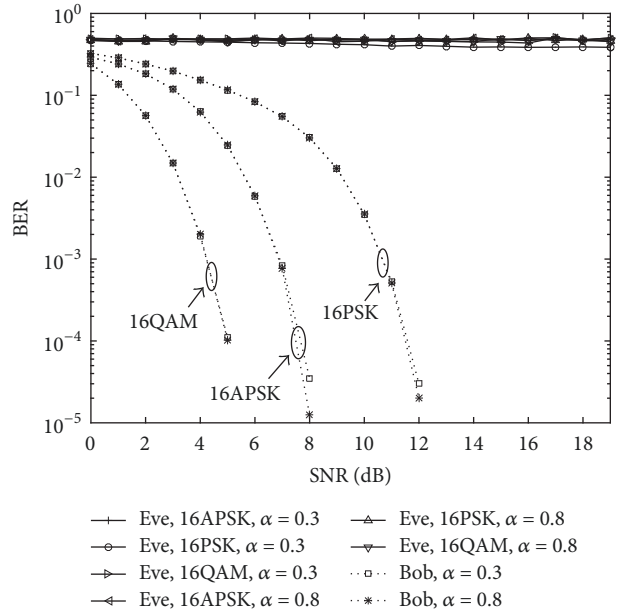



Figure 7: BER performance of the proposed scheme over AWGN channel.

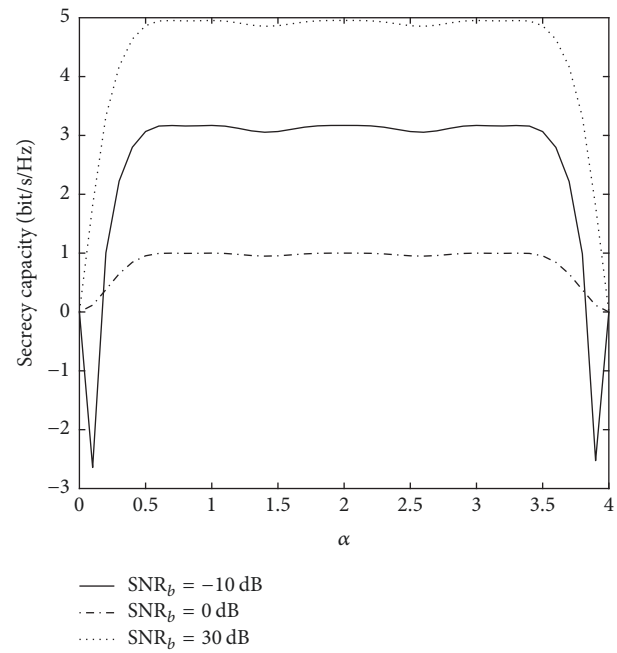



Figure 8: The secrecy capacity of proposed system.

## Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

## Acknowledgments

This work is supported by the National Natural Science Foundation of China under Grant 61571460, Grant 61671475, and Grant 60972042 and in part by the National Post-Doctoral Program for Innovative Talents, under Grant BX201700108. In addition, Lei Ni wants to thank the support from JZ Yang over the past years.

## References

[1] W. Mei, Z. Chen, and J. Fang, "Artificial Noise Aided Energy Efficiency Optimization in MIMOME System with SWIPT," *IEEE Communications Letters*, vol. 21, no. 8, pp. 1795–1798, 2017.

[2] D. Chen, N. Zhang, and Z. Qin, "S2M: a lightweight acoustic fingerprints based wireless device authentication protocol," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 88–100, 2017.

[3] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

[4] W. Trappe, "The challenges facing physical layer security," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 16–20, 2015.

[5] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[6] D.-H. Chen, Y.-C. He, X. Lin, and R. Zhao, "Both Worst-Case and Chance-Constrained Robust Secure SWIPT in MISO Interference Channels," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 2, pp. 306–317, 2018.

[7] W. Mei, Z. Chen, L. Li, J. Fang, and S. Li, "On Artificial-Noise-Aided Transmit Design for Multiuser MISO Systems with Integrated Services," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 9, pp. 8179–8195, 2017.

[8] S. S. Kalamkar and A. Banerjee, "Secure Communication via a Wireless Energy Harvesting Untrusted Relay," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2199–2213, 2017.

[9] T. Zhao, Q. Ran, L. Yuan, Y. Chi, and J. Ma, "Security of image encryption scheme based on multi-parameter fractional Fourier transform," *Optics Communications*, vol. 376, pp. 47–51, 2016.

[10] Y. Hui, B. Li, and Z. Tong, "4-weighted fractional Fourier transform over doubly selective channels and optimal order selecting algorithm," *IEEE Electronics Letters*, vol. 51, no. 2, pp. 177–179, 2015.

[11] C.-C. Shih, "Fractionalization of Fourier transform," *Optics Communications*, vol. 118, no. 5-6, pp. 495–498, 1995.

[12] S. S. Das and S. Tiwari, "Discrete Fourier transform spreading-based generalised frequency division multiplexing," *IEEE Electronics Letters*, vol. 51, no. 10, pp. 789–791, 2015.

[13] L. Mei, Q. Zhang, X. Sha, and N. Zhang, "WFRFT precoding for narrowband interference suppression in DFT-based block transmission systems," *IEEE Communications Letters*, vol. 17, no. 10, pp. 1916–1919, 2013.

[14] K. Huang, R. Tao, and Y. Wang, "Fractional Fourier domain equalization for single carrier broadband wireless systems," *Science China Information Sciences*, vol. 55, no. 10, pp. 2257–2268, 2012.

[15] F. Xiaojie, S. Xuejun, and L. Yong, "Secret communication using parallel combinatory spreading WFRFT," *IEEE Communications Letters*, vol. 19, no. 1, pp. 62–65, 2015.

[16] Y. Li, X. Sha, and K. Wang, "Hybrid carrier communication with partial FFT demodulation over underwater acoustic channels," *IEEE Communications Letters*, vol. 17, no. 12, pp. 2260–2263, 2013.

[17] E. Jorswieck, S. Tomasin, and A. Sezgin, "Broadcasting into the Uncertainty: Authentication and Confidentiality by Physical-Layer Processing," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1702–1724, 2015.

[18] L. Mei, X. J. Sha, Q. W. Ran, and N. T. Zhang, "Research on the application of 4-weighted fractional Fourier transform in communication system," *Science China Information Sciences*, vol. 53, no. 6, pp. 1251–1260, 2010.

[19] Z. Wang, L. Mei, X. Wang, X. Sha, and N. Zhang, "BER analysis of hybrid carrier system based on WFRFT with carrier frequency offset," *IEEE Electronics Letters*, vol. 51, no. 21, pp. 1708-1709, 2015.

[20] Y. He, B. Shi, and Y. Yang, "Periodic complete complementary codes based on displaced Polyphase Orthogonal Sequence," *Signal Processing*, vol. 23, pp. 941–945, 2007.

[21] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, "Directed diffusion for wireless sensor networking," *IEEE/ACM Transactions on Networking*, vol. 11, no. 1, pp. 2–16, 2003.

[22] R. Rivest, "The MD5 Message-Digest Algorithm," RFC Editor RFC1321, 1992.

[23] W. Mei, Z. Chen, and J. Fang, "Secrecy Capacity Region Maximization in Gaussian MISO Channels with Integrated Services," *IEEE Signal Processing Letters*, vol. 23, no. 8, pp. 1146–1150, 2016.

[24] X. Fang, N. Zhang, S. Zhang, D. Chen, X. Sha, and X. Shen, "On Physical Layer Security: Weighted Fractional Fourier Transform Based User Cooperation," *IEEE Transactions on Wireless Communications*, vol. 16, no. 8, pp. 5498–5510, 2017.