IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 31 July 2023, accepted 29 August 2023, date of publication 6 September 2023, date of current version 13 September 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3312580

RESEARCH ARTICLE

Physical Layer Security Design for FDD IM-OTFS Transmissions Based on Secure Mapping

KEJIA MA, ZHENZHEN GAO, JINCHI WANG, AND LINLING CHENG
School of Information and Communications Engineering, Xi'an Jiaotong University, Xi'an 710049, China

Corresponding author: Zhenzhen Gao (zhenzhengao@xjtu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 62071367, and in part by the National Key Research and Development Program of China under Grant 2021YFB2900502.

ABSTRACT In this paper, a physical layer security scheme is proposed for index modulation aided orthogonal time frequency space (IM-OTFS) modulation systems working in Frequency Division Duplex (FDD) mode. In FDD systems, the channel reciprocity, which is the basic assumption for most physical layer security (PLS) techniques, is not applicable. To deal with the security challenge in FDD IM-OTFS systems, Chaos sequence is generated by exploiting the angular reciprocity of the legitimate link to construct the secure mapping rule between the information bits and the modulation symbols as well as the symbol indices. A PLS scheme based on the proposed secure mapping is introduced. The secrecy performance of the proposed PLS scheme is analyzed in terms of Bit Error Rate (BER) and the ergodic secrecy rate. Furthermore, a close-form approximated ergodic secrecy rate is derived to reduce the computational complexity. A truncation method is proposed to obtain robust secure transmissions when the angles of the uplink and downlink legitimate channels are estimated with errors. Simulation results show that the theoretical BER curve approaches the simulated BER curve closely for medium and high signal to noise ratio (SNR) regions, and the eavesdropper's BER is always around 0.5 for all SNRs. The closed-form approximated ergodic secrecy rate fits the ergodic secrecy rate exactly in low and high SNR regions, and can work as a lower bound of the ergodic secrecy rate in medium SNR region. The secure mapping at the legitimate users is not affected by the angle estimation errors by using the truncation method, while the eavesdropper's BER is influenced and the influence is analyzed.

INDEX TERMS Orthogonal time frequency space modulation, index modulation, physical layer security, secure mapping, secrecy rate.

I. INTRODUCTION

Many applications facilitated by 5G or the future 6G involve various high mobility scenarios, such as vehicle-to-vehicle communication system and the satellite communication (SatCom) system [1], which have highly doubly-dispersive radio channels in the time-frequency (TF) domain, and cause challenges to traditional one-dimensional time or frequency modulation schemes. In order to tackle the doubly-selective channels, a novel two-dimensional (2-D) modulation technique, namely orthogonal time frequency space (OTFS), was proposed in [2]. For OTFS modulation, the transmit symbols are implemented in the Delay-Doppler (DD) domain and then transferred onto the time-frequency (TF) domain by using the Inverse Symplectic Finite Fourier Transform (ISFFT) [3]. So that all symbols are spread to the whole TF domain and it does not rely on the orthogonality among subcarriers, therefore, OTFS modulation improves the resistance to Doppler shift.

In 5G and future wireless communication networks, the explosively growing demand of data services requires higher spectral efficiency. Index modulation (IM) is a promising modulation technique which provides high spectral and energy efficiency [4], [5], [6]. The basic idea of IM is to carry the information bits by both the constellation symbols and the activated indices of transmission entities, such as the

The associate editor coordinating the review of this manuscript and approving it for publication was Mehdi Sookhak.

antennas of multi-antenna systems [7], [8] and the subcarriers of multi-carrier systems [9], [10], [11]. Recently, IM is also applied in OTFS systems to improve the transmission performance in high-mobility scenarios. Different IM designs have been proposed for OTFS systems, and most of them focus on improving the decoding performance with reasonable decoding complexity [12], [13], [14], [15], [16]. As security issue becomes more prominent in wireless communication systems due to the open nature of the wireless propagation, it is also necessary to deal with the security challenge in IM aided OTFS (IM-OTFS) systems.

A. RELATED WORK

Different OTFS with IM schemes have been proposed in recent years. The general combination between OTFS modulation and index modulation is investigated in [12]. Further, the authors of [13], [14], and [15] improve the activation scheme or the modulation scheme, therefore the spectral efficiency is upgraded and the modulation order is reduced, so as to improve the spectrum efficiency and reliability of the communication systems. In addition, in [16], an IM aided scheme is proposed to mitigate the in-phase and quadrature (IQ) imbalance effect in OTFS system.

Since both the index dimension and the modulation dimension can carry information bits, IM technique not only improves the spectral efficiency but also provides the probability of introducing extra security in the index dimension. Unfortunately, those works mentioned above do not consider the security of the IM-OTFS system.

Despite this, the physical layer security (PLS) problem has received some attention in the OTFS system. In [17], by implementing the singular value decomposition (SVD) on the equivalent channel matrix of the legitimate link in the DD domain, the right singular matrix is utilized to encode the transmit information to anti-eavesdrop. But it neither excavates the sparsity of the equivalent channel in the DD domain, nor considers the probability that eavesdropper derives the encoding vector due to the correlation between the legitimate link and the illegitimate link. The authors of [18] introduce a multi-antenna Unmanned Aerial Vehicle (UAV) to transmit the artificial noise (AN) in order to anti-eavesdrop when considering the uplink of the Low Earth Orbit (LEO) satellite communication system [19], and the security outage probability (SOP) is derived. However, transmitting AN causes additional power consumption, and its numerical results do not clarify the better performance compared with OFDM system is resulted from the introduction of AN or the slighter ICI in OTFS system. The vehicular networks with OTFS modulation is discussed in [20], the closed-form instantaneous secrecy capacity is derived in Rayleigh fading and Nakagami fading, but the ergodic secrecy capacity is ignored and there is the same problem as [18] when the simulation results are compared with the OFDM system.

However, the PLS problem in the IM-OTFS system still needs attention, especially for FDD systems where channel reciprocity do not strictly exists. Existing PLS schemes such as artificial noise (AN) [21], secure beamforming [22] and the CSI-based random mapping [23] relying on the reciprocity of the legitimate link in TDD systems can not be applied in FDD systems.

A Chaos-based PLS transmission scheme has been proposed in [24]. The idea of using Chaos sequence to design PLS scheme provides a new perspective to solve the security challenge in FDD systems. However, the proposed Chaos-based PLS scheme in [24] depends on the assumption that the chaotic initial values have been secretly shared by the legitimate transceiver. Recently, in [25] and [26], the authors have designed Chaos-based secure schemes for orthogonal frequency division multiplexing based differential chaos shift keying systems. The secure scheme in [25] requires to share a set of chaotic sequences secretly between the legitimate transceiver, while the secure scheme in [26] designs a deep neural network (DNN)-aided receiver to avoid the delivery of reference chaotic signals. These works indicate that security can be enhanced by using Chaos sequences, but the secret sharing of the Chaos sequences between the legitimate transceiver requires extra secure information exchange [24], [25]or extra computation capability [26].

B. CONTRIBUTIONS

To solve the PLS problem in FDD IM-OTFS systems, in this paper, we propose a Chaos-based secure mapping scheme to resist eavesdropping. Different from the random mapping scheme in [23] and [27], the secure mapping in this paper is designed based on Chaos sequences by exploiting their sensitivity to the initial values and the aperiodicity. The angular reciprocity [28] which means that an Angles of Arrival (AoA) at one frequency can be translated to an Angles of Departure (AoD) at another frequency has been used recently to design beamforming or precoding in FDD systems. To avoid sharing the initial values at the legitimate transceiver beforehand, we exploit the angular reciprocity of the legitimate link to generate the same Chaos sequence at the legitimate transceiver. The main contributions of this paper can be summarized as follows:

- A secure mapping scheme is designed based on the Chaos sequence, and the initial value of the chaos sequence is derived from the angle reciprocity. Based on the same initial value obtained at the legitimate transceiver, a secure mapping rule is generated by using a sliding window on the Chaos sequence at the legitimate transceiver, which is unavailable at the illegal eavesdropper.
- The theoretical BER and the ergodic secrecy rate of the proposed scheme are analyzed. To simplify the calculation, the approximated ergodic secrecy rate is derived in closed-form. Simulations show that the theoretical BER is close to the simulation BER for medium and high SNRs, and the approximated ergordic secrecy rate is close to the ergodic secrecy rate.

- In a practical case when the angles of the legitimate uplink and downlink are estimated with errors, the legitimate transceiver can not get the same initial values. To make the proposed scheme robust, we propose a method to truncate the initial values so that the truncated values are used as the common initial value at the legitimate transceiver. We also analyze the influence of truncation at the eavesdropper.

The rest of this paper is organized as follows. Section II investigates the IM-OTFS system. The specific secure mapping scheme for FDD IM-OTFS is presented in Section III. In Section IV, the bit error rate and the ergodic secrecy rate of the proposed scheme are analyzed, and the approximated ergodic secrecy rate is derived in closed-form. Section V shows the simulation results and discussions. Finally, conclusions are illustrated in Section VI.

Notations: Scalars, vectors and matrices are denoted by lower-case normal script x, lower-case bold script $\boldsymbol{x}$ and upper-case bold script $\boldsymbol{X}$, respectively. $(\cdot)^*$, $(\cdot)^T$ and $(\cdot)^H$ represents conjugate, transpose and conjugate transpose respectively. $\otimes$ means Kronecker product. $\lfloor x \rfloor$ indicates the closest integer less than or equal to x and $x!$ indicates the factorial of a non-negative integer x. $\boldsymbol{I}_M$ stands for the identity matrix of size $M \times M$, $\boldsymbol{F}_M$ stands for the M-points normalized discrete Fourier transform (DFT) matrix and $\boldsymbol{F}_M^H$ stands for the M-points inverse discrete Fourier transform (IDFT) matrix. $\boldsymbol{x} = vec(\boldsymbol{X})$ means column-wise vectorization. $circ(\cdot)$ means circulant matrix and $diag(\cdot)$ means diagonalization. $\mathbb{E}(\cdot)$ represents the expectation operator.

II. FDD IM-OTFS SYSTEM MODEL

A. SYSTEM MODEL

We consider a high speed mobile scenario using IM-OTFS transmissions using Frequency Division Duplexing (FDD) mode. A legitimate transmitter called Alice transmits private information signal to a legitimate receiver called Bob. Meanwhile, there is a passive eavesdropper Eve trying to overhear the private information signal.

B. IM-OTFS TRANSMISSIONS

We consider an IM-OTFS system with M subcarriers and N symbols, where subcarrier spacing and symbol duration are Δf and T respectively. The block diagram of IM-OTFS is shown in Fig. 1. A total number of m incoming data bits are split into g groups so each of them contains $p = m/g$ bits, and each p bits is mapped on an OTFS subblock in the DD domain with size $n = MN/g$. For each group, p bits are divided into p_1 bits and p_2 bits, which are referred as index bits and information bits. The first $p_1 = \lfloor log_2 C_n^k \rfloor$ bits are used to activate k symbols out of n, and the remaining $p_2 = klog_2 Q$ bits are mapped to the Q-ary constellation points whose information will be carried by the k activated symbols.

In the αth subblock, the indices of the activated symbols are assumed as,

$$\boldsymbol{I}_\alpha = [i_{\alpha,1}, \ldots, i_{\alpha,k}], \tag{1}$$

where $i_{\alpha,\beta} \in \{1, \ldots, n\}, 1 \le \alpha \le g, 1 \le \beta \le k$. k indices will be activated out of $\boldsymbol{I}_\alpha$ according to the index bits. The modulated symbols in this block are expressed as,

$$\boldsymbol{d}_\alpha = [d_\alpha(1), \ldots, d_\alpha(k)]. \tag{2}$$

After activation and modulation in all groups, we can obtain the index set $\boldsymbol{I}$ and the modulation symbol set $\boldsymbol{d}$ for the entire DD domain. The numbers of the index bits and the information bits for all the groups can be calculated as $m_1 = p_1 g = \lfloor log_2 C_n^k \rfloor g$ and $m_2 = p_2 g = k(log_2 Q)g$ respectively, where $m = m_1 + m_2$.

Combining all g groups with OTFS block generator, the $M \times N$ transmitting block $\boldsymbol{X} = \mathcal{F}_{\mathcal{IM}}(\boldsymbol{I}, \boldsymbol{d})$ in the DD domain is created, where $\mathcal{F}_{\mathcal{IM}}(\cdot)$ represents the index modulation operation. Here, we consider the system in which the transmitting and receiving pulses are rectangular pulses for simplicity. Firstly, $\boldsymbol{X}$ in the DD domain is converted by the ISFFT into the TF domain as $\boldsymbol{X}_{TF} \in \mathbb{C}^{M \times N}$, which is equivalent to applying an M-point DFT and an N-point IDFT to the columns and rows to $\boldsymbol{X}$ respectively as follows,

$$\boldsymbol{X}_{TF} = \boldsymbol{F}_M \boldsymbol{X} \boldsymbol{F}_N^H. \tag{3}$$

Then the time domain signal $\boldsymbol{S}$ is obtained by the Heisenberg transform as,

$$\boldsymbol{S} = \boldsymbol{F}_M^H \boldsymbol{X}_{TF} = \boldsymbol{X} \boldsymbol{F}_N^H. \tag{4}$$

By vectoring $\boldsymbol{S}$ into the $MN \times 1$ vector $\boldsymbol{s} = vec(\boldsymbol{S}) = (\boldsymbol{F}_N^H \otimes \boldsymbol{I}_M)\boldsymbol{x}$ and adding a cyclic prefix (CP), the transmit symbols can be transmitted over the time-varying channel, here $\boldsymbol{x} = vec(\mathcal{F}_{\mathcal{IM}}(\boldsymbol{I}, \boldsymbol{d})) \in \mathbb{C}^{MN \times 1}$ in the DD domain is the vector form of $\boldsymbol{X}$.

The received signal at Bob after removing the CP can be written as,

$$\boldsymbol{r} = \boldsymbol{H}\boldsymbol{s} + \widetilde{\boldsymbol{w}}, \tag{5}$$

where $\boldsymbol{H} = \sum_i^P h_i \boldsymbol{\Pi}^{l_i} \boldsymbol{\Delta}^{k_i} \in \mathbb{C}^{MN \times MN}$ is the time-domain channel matrix, in which P is the number of propagation paths, $h_i \sim \mathcal{CN}(0, 1/P)$ is the complex gain of the i-th path, $\boldsymbol{\Pi} = circ\{[0, 1, \ldots, 0]_{MN \times 1}^T\} \in \mathbb{C}^{MN \times MN}$ is a permutation matrix, $\boldsymbol{\Delta} = diag\{e^{j\frac{2\pi \cdot 0}{MN}}, e^{j\frac{2\pi \cdot 1}{MN}}, \ldots, e^{j\frac{2\pi \cdot (MN-1)}{MN}}\} \in \mathbb{C}^{MN \times MN}$ is a diagonal matrix, l_i and k_i represent the integer delay and Doppler taps respectively. $\widetilde{\boldsymbol{w}} \in \mathbb{C}^{MN \times 1}$ is the additive white Gaussian noise (AWGN) that is distributed as $\widetilde{\boldsymbol{w}} \sim \mathcal{CN}(\boldsymbol{0}, N_0 \boldsymbol{I}_M)$. Then the reverse operations are performed on $\boldsymbol{r}$. Firstly, we reshape the vector $\boldsymbol{r}$ to the matrix form $\boldsymbol{R} \in \mathbb{C}^{M \times N}$, then the Wigner transform and the SFFT are implemented to get the received matrix $\boldsymbol{Y} \in \mathbb{C}^{M \times N}$ in the DD domain as

$$\boldsymbol{Y} = \boldsymbol{F}_M^H (\boldsymbol{F}_M \boldsymbol{R}) \boldsymbol{F}_N = \boldsymbol{R} \boldsymbol{F}_N. \tag{6}$$

Finally, by column-wise vectorization, the input-output relationship of the IM-OTFS system can be derived as,

$$\begin{aligned} \boldsymbol{y} &= vec(\boldsymbol{Y}) \\ &= (\boldsymbol{F}_N \otimes \boldsymbol{I}_M)\boldsymbol{H}(\boldsymbol{F}_N^H \otimes \boldsymbol{I}_M)\boldsymbol{x} + (\boldsymbol{F}_N \otimes \boldsymbol{I}_M)\widetilde{\boldsymbol{w}} \\ &= \boldsymbol{H}_{eff}\boldsymbol{x} + \boldsymbol{w}, \end{aligned} \tag{7}$$

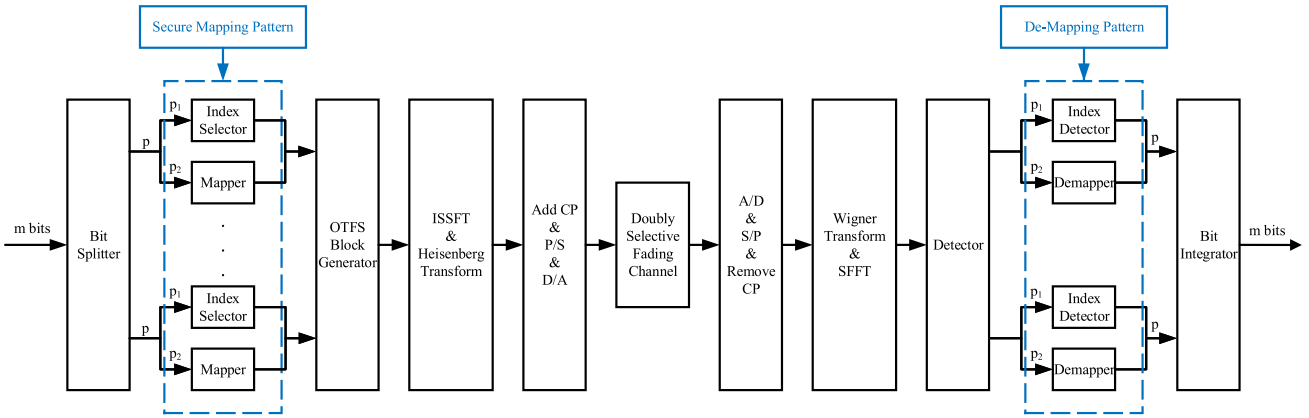

FIGURE 1. Block diagram of secure mapping aided IM-OTFS system.

where $\boldsymbol{H}_{eff} = (\boldsymbol{F}_N \otimes \boldsymbol{I}_M)\boldsymbol{H}(\boldsymbol{F}_N^H \otimes \boldsymbol{I}_M)$ is the effective channel matrix and $\boldsymbol{w}$ is the equivalent noise in the DD domain. Similarly, the received signal at Eve can be expressed as,

$$\boldsymbol{y}_e = \boldsymbol{G}_{eff}\boldsymbol{x} + \boldsymbol{w}_e, \tag{8}$$

where $\boldsymbol{G}_{eff}, \boldsymbol{w}_e$ are the effective channel matrix and the equivalent noise of the Alice-Eve link.

III. THE PROPOSED SECURE MAPPING SCHEME

Gray mapping is widely used in wireless communication systems to map the bits to constellation symbols. Since Gray mapping is a commonly-known mapping, it can not bring any secrecy to the communication system. In this section, we propose a secure mapping scheme based on Chaos sequence by exploiting its sensitivity to the initial value and the the aperiodicity property to resist eavesdropping without any extra cost.

As illustrated in Equ. (7), we have the effective channel matrix $\boldsymbol{H}_{eff}$ in the DD domain and it can be written as,

$$\boldsymbol{H}_{eff} = \sum_{i=1}^{P} h_i \boldsymbol{T}_i, \tag{9}$$

where h_i is the complex gain of the i-th path, and $\boldsymbol{T}_i \in \mathbb{C}^{MN \times MN}$ represents the influence for the phase in the i-th path.

Although the channel reciprocity is no longer exists in FDD systems, we can still obtain some reciprocity parameters. In [29], the arbitrary channel path's angles at uplink and downlink, the delay for each multipath and the depolarization matrix for reflection are regarded as the same in FDD systems. In [28], the angular reciprocity has been used to extend the bi-directional training for time division duplex (TDD) systems to FDD systems. Angular reciprocity has been used for channel reconstruction of the uplink and downlink channel in [30] and [31]. In [32], deviation distribution of the dominant direction of arrival (DoA) estimated at the uplink and downlink carrier has shown that the deviations of DoAs from the uplink and downlink are no more than 5 degrees [32].

By exploiting the angular reciprocity of the legitimate link, Alice and Bob can obtain the same angular parameter respectively, while this angular parameter is unavailable at Eve since she is located differently from Bob. Inspired by the fact that Chaos sequences have the aperiodicity property and are highly sensitive to the initial value, we propose a secure mapping scheme based on Chaos sequence generating by the same angular parameter at Alice and Bob.

Without loss of generality, let's take the following 2 dimensional chaotic sequence generation as an example [33],

$$\begin{cases} x_{n+1} = (ax_n + by_n^{\gamma}) mod\, \beta \\ y_{n+1} = (cy_n + r_n) mod\, \beta \end{cases} \tag{10}$$

where x_n and y_n are state variables, a, b, c, r are quantitative parameters, γ is the highest-order polynomial, β is modulus coefficient, r_n is the random perturbation factor, the Chaos initial values x_0 and y_0 are in the interval (0, 1). The parameters $a, b, c, \gamma, \beta, r_n$ can be available for all parties including Eve. Although the two-dimensional Chaos sequence is taken as an example here, the following design can also be implemented for one dimensional or higher dimensional Chaos sequences [34].

Instead of sharing the Chaos initial value as a key between the legitimate users, in this paper, we propose to generate the Chaos initial value locally at Alice and Bob by exploiting the angular reciprocity. Since the Chaos initial values are in (0, 1), after normalizing the angles obtained at Alice and Bob, a Sigmoid mapping is performed to map the angles to values in (0, 1) which will be used as the Chaos initial values at Alice and Bob respectively. Thanks to the angular reciprocity, Alice and Bob can obtain the same Chaos initial value and generate the same chaotic sequence.

In the following, we will design the secure mapping from the information bits to the modulation symbols based on the sequence $\{x_n\}$, and design the secure mapping from the index bits to the activated indices of symbols based on the sequence $\{y_n\}$.

For each group, p_1 bits are used to activate k symbols from the OTFS subblock which contains n symbols, as illustrated

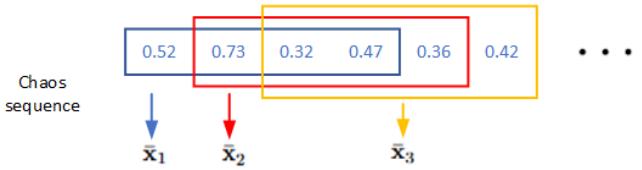

FIGURE 2. A sliding window operating on the Chaos sequence when $Q = 4$.

in Section II-B. Then p_2 bits are mapped to the Q-ary constellation to generate k activate symbols.

To make the bit-to-symbol mapping changes randomly for Eve from one symbol to another, a sliding window is designed in Fig. 2. For the Q-ary constellation, the length of the sliding window is Q. For the first symbol, the elements of $\{x_n\}$ in the sliding window construct a vector $\bar{\mathbf{x}}_1$. For the second symbol, the sliding window shift across one element of $\{x_n\}$, and the elements inside the sliding window are denoted as $\bar{\mathbf{x}}_2$. Similarly, for each of the k activated symbols we can get a vector $\bar{\mathbf{x}}_l, l = 1, \cdots, k$. Then we sort the elements in $\bar{\mathbf{x}}_l$ in descending order, and the total number of the sorting patterns is $N_M = Q!$ which is the same to the total number of the bit-to-symbol mapping patterns. In this way we construct a one-to-one mapping for each symbol between the sorted pattern of Chaotic elements and the bit-to-symbol mapping pattern, and this one-to-one mapping is determined by the Chaotic sequence between Alice and Bob, which is unknown to Eve.

Assume $d_\alpha(l)$ in Equ. (2) comes from a QPSK constellation, so $Q = 4$, and $N_M = 24$. The windowed Chaotic vector is denoted as $\bar{\mathbf{x}}_l = [\gamma_1, \gamma_2, \gamma_3, \gamma_4]$. Here, $s_i, i = \{1, 2, 3, 4\}$ is the QPSK constellation points. An illustration of the correspondence that pairs the sorting pattern of $\bar{\mathbf{x}}_l$ with the symbol mapping pattern for this example is shown in Table 1.

Then, the secure mapping from the index bits to the activated indices of symbols based on the sequence $\{y_n\}$ is discussed. Similarly, we want to design a secure mapping which makes the indices activation change randomly for Eve from one OTFS subblock to another. For example, assume that $M = 4$ and $N = 2$, and we divide the $MN = 8$ points into $g = 2$ groups and activate $k = 3$ points out of $n = MN/g = 4$ in each group. The length of the sliding window for this case is 4. We can generate the windowed Chaotic vector for each OTFS subblock in the same way as we generate the windowed Chaotic vector for the modulation symbols. The correspondence between the chaotic sequence sorting patterns and the index activation patterns is shown in Table 2, where $p_i, i = \{1, 2, 3, 4\}$ represents the indices of 4 points in the OTFS subblock and the mark "$\rightarrow$" represents that the point is activated.

By performing the above secure mapping for the information bits and the index bits, the transmitting block in DD domain can be represented as $\mathbf{X} = \mathcal{F}_{S_{IM}}(\boldsymbol{I}, \boldsymbol{d})$, where $\mathcal{F}_{S_{IM}}(\cdot)$ denotes the secure mapping designed in this section.

TABLE 1. Illustration of correspondence between the chaotic sequence sorting patterns and the bit-to-symbol mapping patterns with $Q = P = 4$.

Chaotic Sequence Sorting Pattern χ	Bit-to-Symbol Mapping Pattern
1.$\gamma_1 > \gamma_2 > \gamma_3 > \gamma_4$	$00 \rightarrow s_1, 01 \rightarrow s_2, 10 \rightarrow s_3, 11 \rightarrow s_4$
2.$\gamma_1 > \gamma_2 > \gamma_4 > \gamma_3$	$00 \rightarrow s_1, 01 \rightarrow s_2, 10 \rightarrow s_4, 11 \rightarrow s_3$
3.$\gamma_1 > \gamma_3 > \gamma_2 > \gamma_4$	$00 \rightarrow s_1, 01 \rightarrow s_3, 10 \rightarrow s_2, 11 \rightarrow s_4$
4.$\gamma_1 > \gamma_3 > \gamma_4 > \gamma_2$	$00 \rightarrow s_1, 01 \rightarrow s_3, 10 \rightarrow s_4, 11 \rightarrow s_2$
5.$\gamma_1 > \gamma_4 > \gamma_2 > \gamma_3$	$00 \rightarrow s_1, 01 \rightarrow s_4, 10 \rightarrow s_2, 11 \rightarrow s_3$
6.$\gamma_1 > \gamma_4 > \gamma_3 > \gamma_2$	$00 \rightarrow s_1, 01 \rightarrow s_4, 10 \rightarrow s_3, 11 \rightarrow s_2$
7.$\gamma_2 > \gamma_1 > \gamma_3 > \gamma_4$	$00 \rightarrow s_2, 01 \rightarrow s_1, 10 \rightarrow s_3, 11 \rightarrow s_4$
8.$\gamma_2 > \gamma_1 > \gamma_4 > \gamma_3$	$00 \rightarrow s_2, 01 \rightarrow s_1, 10 \rightarrow s_4, 11 \rightarrow s_3$
9.$\gamma_2 > \gamma_3 > \gamma_1 > \gamma_4$	$00 \rightarrow s_2, 01 \rightarrow s_3, 10 \rightarrow s_1, 11 \rightarrow s_4$
10.$\gamma_2 > \gamma_3 > \gamma_4 > \gamma_1$	$00 \rightarrow s_2, 01 \rightarrow s_3, 10 \rightarrow s_4, 11 \rightarrow s_1$
11.$\gamma_2 > \gamma_4 > \gamma_1 > \gamma_3$	$00 \rightarrow s_2, 01 \rightarrow s_4, 10 \rightarrow s_1, 11 \rightarrow s_3$
12.$\gamma_2 > \gamma_4 > \gamma_3 > \gamma_1$	$00 \rightarrow s_2, 01 \rightarrow s_4, 10 \rightarrow s_3, 11 \rightarrow s_1$
13.$\gamma_3 > \gamma_1 > \gamma_2 > \gamma_4$	$00 \rightarrow s_3, 01 \rightarrow s_1, 10 \rightarrow s_2, 11 \rightarrow s_4$
14.$\gamma_3 > \gamma_1 > \gamma_4 > \gamma_2$	$00 \rightarrow s_3, 01 \rightarrow s_1, 10 \rightarrow s_4, 11 \rightarrow s_2$
15.$\gamma_3 > \gamma_2 > \gamma_1 > \gamma_4$	$00 \rightarrow s_3, 01 \rightarrow s_2, 10 \rightarrow s_1, 11 \rightarrow s_4$
16.$\gamma_3 > \gamma_2 > \gamma_4 > \gamma_1$	$00 \rightarrow s_3, 01 \rightarrow s_2, 10 \rightarrow s_4, 11 \rightarrow s_1$
17.$\gamma_3 > \gamma_4 > \gamma_1 > \gamma_2$	$00 \rightarrow s_3, 01 \rightarrow s_4, 10 \rightarrow s_1, 11 \rightarrow s_2$
18.$\gamma_3 > \gamma_4 > \gamma_2 > \gamma_1$	$00 \rightarrow s_3, 01 \rightarrow s_4, 10 \rightarrow s_2, 11 \rightarrow s_1$
19.$\gamma_4 > \gamma_1 > \gamma_2 > \gamma_3$	$00 \rightarrow s_4, 01 \rightarrow s_1, 10 \rightarrow s_2, 11 \rightarrow s_3$
20.$\gamma_4 > \gamma_1 > \gamma_3 > \gamma_2$	$00 \rightarrow s_4, 01 \rightarrow s_1, 10 \rightarrow s_3, 11 \rightarrow s_2$
21.$\gamma_4 > \gamma_2 > \gamma_1 > \gamma_3$	$00 \rightarrow s_4, 01 \rightarrow s_2, 10 \rightarrow s_1, 11 \rightarrow s_3$
22.$\gamma_4 > \gamma_2 > \gamma_3 > \gamma_1$	$00 \rightarrow s_4, 01 \rightarrow s_2, 10 \rightarrow s_3, 11 \rightarrow s_1$
23.$\gamma_4 > \gamma_3 > \gamma_1 > \gamma_2$	$00 \rightarrow s_4, 01 \rightarrow s_3, 10 \rightarrow s_1, 11 \rightarrow s_2$
24.$\gamma_4 > \gamma_3 > \gamma_2 > \gamma_1$	$00 \rightarrow s_4, 01 \rightarrow s_3, 10 \rightarrow s_2, 11 \rightarrow s_1$

IV. PERFORMANCE ANALYSIS OF THE PROPOSED SCHEME

A. OPTIMAL DETECTION

The received signals at Bob and Eve are respectively

$$\boldsymbol{y} = \boldsymbol{H}_{eff}\boldsymbol{x} + \boldsymbol{w}, \tag{11}$$

$$\boldsymbol{y}_e = \boldsymbol{G}_{eff}\boldsymbol{x} + \boldsymbol{w}_e, \tag{12}$$

where $\boldsymbol{x} = vec(\mathbf{X}) = \mathcal{F}_{S_{IM}}(\boldsymbol{I}, \boldsymbol{d})$. The detector in the IM-OTFS system needs to detect the information bit carried by the modulation symbols and the index bits carried on the active indices. Considering all possible index patterns and their corresponding signal constellation points, Let $\mathbb{X}$ denote all possible transmitting block, the maximum-likelihood (ML) detection can be written as,

$$\{\hat{\boldsymbol{I}}, \hat{\boldsymbol{d}}\} = \mathcal{F}^{-1}_{S_{IM}}\{\arg\min_{\mathbf{X}\in\mathbb{X}} \left\|\boldsymbol{y} - \boldsymbol{H}_{eff}\mathcal{F}_{S_{IM}}(\boldsymbol{I}, \boldsymbol{d})\right\|^2\}, \tag{13}$$

$$\{\hat{\boldsymbol{I}}_e, \hat{\boldsymbol{d}}_e\} = \mathcal{F}^{-1}_{E_{IM}}\{\arg\min_{\mathbf{X}\in\mathbb{X}} \left\|\boldsymbol{y}_e - \boldsymbol{G}_{eff}\mathcal{F}_{S_{IM}}(\boldsymbol{I}, \boldsymbol{d}\right\|^2\}, \tag{14}$$

TABLE 2. Illustration of correspondence between the chaotic sequence sorting patterns and the activation patterns with $Q = 4, P = 4, M = 4, N = 2, g = 2, n = 4, k = 1$.

Chaotic Sequence Sorting Pattern χ	Activation Pattern
1.$\gamma_1 > \gamma_2 > \gamma_3 > \gamma_4$	$00 \to p_1, 01 \to p_2, 10 \to p_3, 11 \to p_4$
2.$\gamma_1 > \gamma_2 > \gamma_4 > \gamma_3$	$00 \to p_1, 01 \to p_2, 10 \to p_4, 11 \to p_3$
3.$\gamma_1 > \gamma_3 > \gamma_2 > \gamma_4$	$00 \to p_1, 01 \to p_3, 10 \to p_2, 11 \to p_4$
4.$\gamma_1 > \gamma_3 > \gamma_4 > \gamma_2$	$00 \to p_1, 01 \to p_3, 10 \to p_4, 11 \to p_2$
5.$\gamma_1 > \gamma_4 > \gamma_2 > \gamma_3$	$00 \to p_1, 01 \to p_4, 10 \to p_2, 11 \to p_3$
6.$\gamma_1 > \gamma_4 > \gamma_3 > \gamma_2$	$00 \to p_1, 01 \to p_4, 10 \to p_3, 11 \to p_2$
7.$\gamma_2 > \gamma_1 > \gamma_3 > \gamma_4$	$00 \to p_2, 01 \to p_1, 10 \to p_3, 11 \to p_4$
8.$\gamma_2 > \gamma_1 > \gamma_4 > \gamma_3$	$00 \to p_2, 01 \to p_1, 10 \to p_4, 11 \to p_3$
9.$\gamma_2 > \gamma_3 > \gamma_1 > \gamma_4$	$00 \to p_2, 01 \to p_3, 10 \to p_1, 11 \to p_4$
10.$\gamma_2 > \gamma_3 > \gamma_4 > \gamma_1$	$00 \to p_2, 01 \to p_3, 10 \to p_4, 11 \to p_1$
11.$\gamma_2 > \gamma_4 > \gamma_1 > \gamma_3$	$00 \to p_2, 01 \to p_4, 10 \to p_1, 11 \to p_3$
12.$\gamma_2 > \gamma_4 > \gamma_3 > \gamma_1$	$00 \to p_2, 01 \to p_4, 10 \to p_3, 11 \to p_1$
13.$\gamma_3 > \gamma_1 > \gamma_2 > \gamma_4$	$00 \to p_3, 01 \to p_1, 10 \to p_2, 11 \to p_4$
14.$\gamma_3 > \gamma_1 > \gamma_4 > \gamma_2$	$00 \to p_3, 01 \to p_1, 10 \to p_4, 11 \to p_2$
15.$\gamma_3 > \gamma_2 > \gamma_1 > \gamma_4$	$00 \to p_3, 01 \to p_2, 10 \to p_1, 11 \to p_4$
16.$\gamma_3 > \gamma_2 > \gamma_4 > \gamma_1$	$00 \to p_3, 01 \to p_2, 10 \to p_4, 11 \to p_1$
17.$\gamma_3 > \gamma_4 > \gamma_1 > \gamma_2$	$00 \to p_3, 01 \to p_4, 10 \to p_1, 11 \to p_2$
18.$\gamma_3 > \gamma_4 > \gamma_2 > \gamma_1$	$00 \to p_3, 01 \to p_4, 10 \to p_2, 11 \to p_1$
19.$\gamma_4 > \gamma_1 > \gamma_2 > \gamma_3$	$00 \to p_4, 01 \to p_1, 10 \to p_2, 11 \to p_3$
20.$\gamma_4 > \gamma_1 > \gamma_3 > \gamma_2$	$00 \to p_4, 01 \to p_1, 10 \to p_3, 11 \to p_2$
21.$\gamma_4 > \gamma_2 > \gamma_1 > \gamma_3$	$00 \to p_4, 01 \to p_2, 10 \to p_1, 11 \to p_3$
22.$\gamma_4 > \gamma_2 > \gamma_3 > \gamma_1$	$00 \to p_4, 01 \to p_2, 10 \to p_3, 11 \to p_1$
23.$\gamma_4 > \gamma_3 > \gamma_1 > \gamma_2$	$00 \to p_4, 01 \to p_3, 10 \to p_1, 11 \to p_2$
23.$\gamma_4 > \gamma_3 > \gamma_2 > \gamma_1$	$00 \to p_4, 01 \to p_3, 10 \to p_2, 11 \to p_1$

where $\mathcal{F}_{S_{IM}}^{-1}(\cdot)$ denotes the secure de-mapping from the symbols and the activated indices to the bits, which is the inverse operation of the secure mapping. Since Eve has no idea of the secure mapping used by the legitimate transceiver, the de-mapping operation $\mathcal{F}_{E_{IM}}^{-1}$ at Eve has no relation to the secure de-mapping used at Bob. Furthermore, the secure mapping and de-mapping changes randomly from one symbol to another, it is almost impossible for Eve to estimate the correct mapping pattern.

The decoding complexity of ML detection would extremely increase with larger size of each subblock and higher order of modulation, to relieve the complexity issue, the Minimum Mean Square Error and ML power (MMSE-ML) detection in [16] can be used to reduce the computation complexity.

B. ANALYSIS OF BER

1) BER of the Legitimate Receiver.

We assume that the legitimate transceiver estimate the angles for the uplink and downlink perfectly, which means they obtain the same secure mapping rule. The input-output relationship can be rewritten as [35],

$$\begin{aligned} \boldsymbol{y} &= \boldsymbol{H}_{\mathit{eff}}\boldsymbol{x} + \boldsymbol{w} \\ &= \sum_{i=1}^{P} h_i \boldsymbol{T}_i \boldsymbol{x} + \boldsymbol{w} \\ &= \boldsymbol{\Phi}(\boldsymbol{x})\boldsymbol{h} + \boldsymbol{w}, \end{aligned} \tag{15}$$

where $\boldsymbol{h} = [h_1, h_2, \ldots, h_P]^T \in \mathbb{C}^{P\times 1}$ and $\boldsymbol{\Phi}(\boldsymbol{x}) = [\boldsymbol{T}_1\boldsymbol{x}|\boldsymbol{T}_2\boldsymbol{x}|\ldots|\boldsymbol{T}_P\boldsymbol{x}] \in \mathbb{C}^{MN\times P}$. Hence, if $\boldsymbol{x}$ is transmitted but detected as $\hat{\boldsymbol{x}}$ over the channel $\boldsymbol{h}$, the conditional pairwise error probability (CPEP) can be expressed as,

$$\begin{aligned} Pr(\hat{\boldsymbol{x}}|\boldsymbol{x}, \boldsymbol{h}) &= Q\Big(\sqrt{\frac{\big\|[\boldsymbol{\Phi}(\hat{\boldsymbol{x}}) - \boldsymbol{\Phi}(\boldsymbol{x})]\boldsymbol{h}\big\|^2}{2N_0}}\Big) \\ &= Q\Big(\sqrt{\frac{\boldsymbol{h}^H\Gamma(\Delta\boldsymbol{x})\boldsymbol{h}}{2N_0}}\Big), \end{aligned} \tag{16}$$

where $Q(\cdot)$ represents the Gaussian tail function and $\Gamma(\Delta\boldsymbol{x}) = \boldsymbol{\Phi}(\Delta\boldsymbol{x})^H\boldsymbol{\Phi}(\Delta\boldsymbol{x})$, $\Delta\boldsymbol{x} = \boldsymbol{x} - \hat{\boldsymbol{x}}$, here, $\Gamma(\Delta\boldsymbol{x})$ is a Hermitian matrix. According to the approximation of $Q(\cdot)$ and the distribution of $\boldsymbol{h}$, the unconditional pairwise error probability (UPEP) can be calculated as [11], [15], [36], and [37],

$$\begin{aligned} Pr(\hat{\boldsymbol{x}}|\boldsymbol{x}) &\cong \mathbb{E}_{\boldsymbol{h}}\Big\{\frac{1}{12}e^{-\frac{\boldsymbol{h}^H\Gamma(\Delta\boldsymbol{x})\boldsymbol{h}}{4N_0P}} + \frac{1}{4}e^{-\frac{\boldsymbol{h}^H\Gamma(\Delta\boldsymbol{x})\boldsymbol{h}}{3N_0P}}\Big\} \\ &= \frac{1/12}{det(\boldsymbol{I}_P + q_1\Gamma(\Delta\boldsymbol{x}))} + \frac{1/4}{det(\boldsymbol{I}_P + q_2\Gamma(\Delta\boldsymbol{x}))} \\ &= \frac{1}{12\prod_{i=1}^{r}(1+q_1\lambda_i)} + \frac{1}{4\prod_{i=1}^{r}(1+q_2\lambda_i)}, \end{aligned} \tag{17}$$

where λ_i is the eigenvalue of $\Gamma(\Delta\boldsymbol{x})$ and $r = rank(\Gamma(\Delta\boldsymbol{x}))$, $q_1 = 1/(4N_0P)$, $q_2 = 1/(3N_0P)$. We assume that $n_{\boldsymbol{x}}$ is the number of all possible realizations of $\boldsymbol{x}$ and $e(\hat{\boldsymbol{x}}, \boldsymbol{x})$ is the number of bits errors for the corresponding pairwise error events, so the theoretical BER is,

$$P_e = \frac{1}{mn_{\boldsymbol{x}}}\sum_{\boldsymbol{x}}\sum_{\hat{\boldsymbol{x}}\neq\boldsymbol{x}} Pr(\hat{\boldsymbol{x}}|\boldsymbol{x})e(\hat{\boldsymbol{x}}, \boldsymbol{x}). \tag{18}$$

2) BER of the Illegitimate Receiver.

Suppose that the illegitimate receiver Eve can estimate the modulation symbols and active indices correctly in the DD domain, we now analyse the BER of converting the symbols into bits. Because the Chaotic sequence is a random sequence, all kinds of sorting patterns of the Chaotic elements inside the sliding window equally appear. The probability of converting any symbol in $\mathbf{x}(i), i = \{1, 2, \ldots, MN\}$ to each possible bit realization is equally $1/M$. Within all possible bit realizations, there is only one case when the number of error bits is 0, and there are $C_{N_b}^m$ cases when that is m, m =

$\{1, 2, \ldots, N_b\}$ with N_b being the number of information bits carried by one symbol in the transmitting block $\mathbf{X}$. So, the BER of each symbol is,

$$P_{Eve} = \frac{1}{M}(\frac{1}{N_b} \times C_{N_b}^1 + \frac{2}{N_b} \times C_{N_b}^2 + \ldots + \frac{N_b}{N_b} \times C_{N_b}^{N_b}) = \frac{1}{M} \sum_{m=1}^{N_b} \frac{m}{N_b} C_{N_b}^m = \frac{1}{2}. \quad (19)$$

The BER of the information bits at Eve is 0.5 which means Eve can not decode the information bits correctly. When Eve can obtain the specific indices of active points, the BER analysis of index bits is similar to that of information bits.

C. ANALYSIS OF SECRECY RATE

In this section, we investigate the ergodic secrecy rate of the secure mapping aided IM-OTFS system. Here, we have the transmitted vector $\boldsymbol{x} \in \mathbb{C}^{MN\times 1}$ and the channel matrix $\boldsymbol{H}_{eff} \in \mathbb{C}^{MN\times MN}$ in the DD domain. The MN points in the DD domain are divided into g groups and each group contains $n = MN/g$ points, and k out of n points are activated then. To represent the specific activation status, we introduce a block diagonal matrix $\boldsymbol{E} \in \mathbb{C}^{MN\times MN}$,

$$\boldsymbol{E} = \begin{bmatrix} \boldsymbol{E}_1 & & & \\ & \boldsymbol{E}_2 & & \\ & & \ddots & \\ & & & \boldsymbol{E}_g \end{bmatrix}, \quad (20)$$

where $\boldsymbol{E}_i \in \mathbb{C}^{n\times n}$, $i \in \{1, 2, \ldots, g\}$ is an n-dimensional diagonal matrix whose principal diagonal elements are 0 or 1, and there are k elements of 1 and $(n-k)$ elements of 0. Since each group has $f_1 = C_n^k$ activation statuses, there are $F_1 = (f_1)^g$ activation statuses in total, which means the matrix $\boldsymbol{E}$ has F_1 possible realizations. Meanwhile, $f_2 = kg$ points are activated, so $\boldsymbol{x}$ has $F_2 = Q^{f_2}$ possible realizations. Hence, the data rate achieved by legitimate receiver is as shown in (21), at the bottom of the next page, and the derivation is shown in Appendix A.

Similarly, according to the chain rule for the mutual information, we can obtain the illegitimate receiver's data rate that is composed by two parts as shown in (22), at the bottom of the next page. Each part of (22) is derived in Appendix B.

Finally, let

$$R = R_b - R_e = I(\boldsymbol{x}, \boldsymbol{E}; \boldsymbol{y}_b) - I(\boldsymbol{x}, \boldsymbol{E}; \boldsymbol{y}_e), \quad (23)$$

the ergodic secrecy rate of the proposed scheme is,

$$R_s = max\{R, 0\}. \quad (24)$$

In addition, if we consider to activate kg indices from MN points directly instead of grouping before activating, we just replace block diagonal matrix $\boldsymbol{E}$ with diagonal matrix $\boldsymbol{E}' \in \mathbb{C}^{MN\times MN}$. In the principal diagonal of $\boldsymbol{E}'$, kg elements are 1 and the remaining $(MN - kg)$ elements are 0. Under this condition, there are $F_1' = C_{MN}^{kg}$ activation statuses and $F_2' = Q^{kg}$ possible $\boldsymbol{x}$ realizations in total. And then, we can obtain the ergodic secrecy rate of the scheme without grouping in a similar way as described above.

D. APPROXIMATION OF SECRECY RATE

On the basis of the ergodic secrecy rate, we now derive a closed-form approximation of R_s. According to (21), we have the lower bound of R_b,

$$R_{bl} = log_2(F_1F_2) - (\frac{1}{ln2} - 1) - \frac{1}{F_1F_2} \times \sum_{d=1}^{F_1}\sum_{k=1}^{F_2} log_2 \sum_{d_2=1}^{F_1}\sum_{k_2=1}^{F_2} (1 + \frac{\sigma_h^2\alpha_b}{2\sigma^2})^{-1}. \quad (25)$$

The derivation is shown in Appendix C. Observing (21) and (25), we can obtain that $\lim_{SNR\to 0} R_b = 0$, $\lim_{SNR\to+\infty} R_b = log_2(F_1F_2)$, $\lim_{SNR\to 0} R_{bl} = -(\frac{1}{ln2} - 1)$, $\lim_{SNR\to+\infty} R_{bl} = log_2(F_1F_2) - (\frac{1}{ln2} - 1)$. So, R_b and R_{bl} have the same difference in both high and low SNR. Due to the monotonicity of R_b and R_{bl}, it is reasonable to imply that the difference between R_b and R_{bl} is $(\frac{1}{ln2} - 1)$ approximately within the whole SNR range [38], [39]. Therefore, the approximated R_b can be written as,

$$R_{b,app} = log_2(F_1F_2) - \frac{1}{F_1F_2} \sum_{d=1}^{F_1}\sum_{k=1}^{F_2} \times log_2 \sum_{d_2=1}^{F_1}\sum_{k_2=1}^{F_2} (1 + \frac{\sigma_h^2\alpha_b}{2\sigma^2})^{-1}. \quad (26)$$

Similarly, we can derive the approximation of each part of R_e, which is shown in Appendix D, and compose them to obtain the approximated R_e,

$$R_{e,app} = \frac{1}{F_1} I_{app}(\boldsymbol{E}; \boldsymbol{y}_e|\boldsymbol{x}) + \frac{1}{F_2} I_{app}(\boldsymbol{x}; \boldsymbol{y}_e). \quad (27)$$

Hence, let $R_{app} = R_{b,app} - R_{e,app}$, the approximated ergodic secrecy rate is,

$$R_{s,app} = max\{R_{app}, 0\}. \quad (28)$$

V. ESTIMATED ANGLE WITH ERRORS

In the above sections, we have proposed a Chaos-based secure mapping scheme to resist eavesdropping in FDD IM-OTFS systems by exploiting the angular reciprocity of the legitimate link, and the secrecy performances in terms of BER and secrecy rate have been analyzed. It could happen that angles estimated at Alice and Bob for the uplink and downlink may not be the same due to estimation errors. This would result in the mismatch of the initial values of the Chaotic sequences at Alice and Bob, and make the legitimate communication unsuccessful. To make the legitimate transmission more robust to the angle estimation errors, a truncation method is

proposed to truncate the initial values at Alice and Bob to get a common initial value.

Assume that the estimated angles at Alice and Bob are 35 and 35.5 respectively, after normalization and performing a Sigmoid mapping to the values, we can observe that mapped decimals at Alice and Bob become different starting at the fourth decimal place. If the estimated angle at Bob is 35.01, the mapped decimals have the same value until the fifth decimal place. Based on this observation, we can truncate the mapped decimals at the decimal place where the mapped decimals become different. The truncated decimals have the same value and they are used as the Chaos initial value by Alice and Bob based on the estimated angles with errors.

While the truncation operation increases the robustness of the secure mapping by allowing Alice and Bob to obtain the same initial value of the chaotic sequence despite the existence of angle estimation bias, it also gives the eavesdropper a chance to get the same initial value by using the truncation operation. It is intuitive that when Eve's estimated angle of the Alice-Eve link deviates further from the angles at Alice and Bob, it is more likely that Eve can not obtain the same initial value as Alice and Bob even she performs truncation on her initial value. However, if Eve's estimated angle is close to the angles at Alice and Bob, the legitimate transmission could be insecure. We will discuss the insecure region when performing the truncation to obtain a robust secure transmission through simulations in the following section.

VI. SIMULATION RESULTS AND DISCUSSION

In this section, numerical results are presented to evaluate the BER and the ergodic secrecy rate of our proposed scheme. We consider a channel with $P = 4$ propagation paths. The Doppler shift tap of the i-th path is uniformly drawn from the set $[-k_{max}, k_{max}]$, and the delay taps belong to $[1, l_{max}]$ excluding the first path ($l_1 = 0$). Assume that $k_{max} = 2$ and $l_{max} = 4$. In the simulations, the angle DOA_{up} of the uplink and the angle DOA_{down} of the downlink is 35 degrees. The coefficients for the Chaos sequence generator are $a = 2$, $b = 3$, $c = 1.7$, $\beta = 1$, and r_n is a random number between (0, 1). In the following simulations, we first consider the case when Alice and Bob can estimate their angles perfectly, then we analyze the influence of angle estimation errors on the secrecy performance.

As shown in Fig. 3, the closed-form approximated ergodic secrecy rate is compared with the simulated ergodic secrecy rate when $M = 2, N = 2, k = 1$. The curves show that

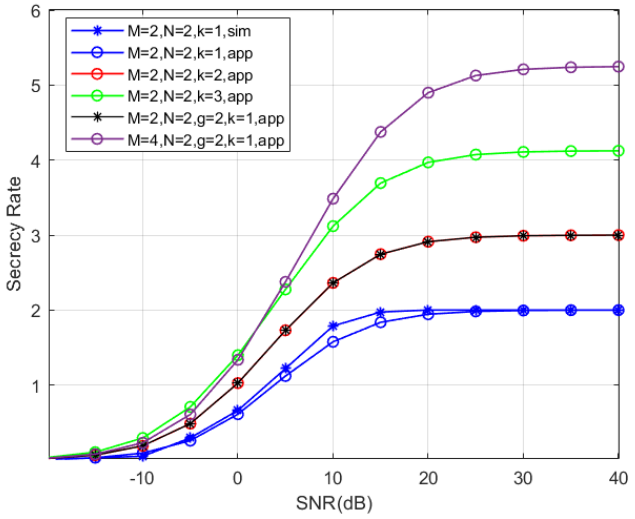

FIGURE 3. Ergodic secrecy rate under different conditions.

the closed-form approximated ergodic secrecy rate fits the simulated secrecy rate well in both high and low SNR regions, while there is a small gap in the moderate SNR region. Since the closed-form approximated ergodic secrecy rate can approximate the ergodic secrecy rate well with a much lower computational complexity, in the following simulations, the closed-form approximated secrecy rate is used to illustrate the secrecy performance. From Fig. 3 we can see that when $M = 2, N = 2, k = 2$ without grouping, i.e, $g = 1$, $log_2 C_{MN}^{kg} = log_2 C_4^2$ is not an integer, which causes that the index bits $p_1 = \lfloor log_2 C_{MN}^{kg} \rfloor = 2$ can decide 4 activation patterns but we actually have 6 possible activation patterns when we want to activate 2 points out of 4. Under this situation, we have to make a trade-off according to the less patterns. As an example, a look-up table with $M = 2, N = 2$ and $k = 2$ is shown in Table 3. Therefore, compared to the grouping case with $M = 2, N = 2, g = 2, k = 1$ represented by a black curve, the ergodic secrecy rate is the same as the red curve. This proves that grouping does not affect the secrecy rate while ensuring that the index carries the same number of bits. Compared to the black curve, when M increases to 4, the ergodic secrecy rate increases as the dimension of OTFS block increases. Compared to the black and red curves, when k increases to 3, the secrecy rate ascends with the increasing number of activated points which carries more index bits.

The BER performance of the proposed secure scheme is investigated in Fig. 4. In the simulations, we have

$$I(\boldsymbol{x}, \boldsymbol{E}; \boldsymbol{y}_b) = log_2(F_1 F_2) - \frac{1}{F_1 F_2} \sum_{d=1}^{F_1} \sum_{k=1}^{F_2} \mathbb{E}_{\boldsymbol{H}_{eff}, \boldsymbol{w}_b} \left\{ log_2 \sum_{d_2=1}^{F_1} \sum_{k_2=1}^{F_2} exp(-\frac{\left\| \boldsymbol{d}_{d,k}^{d_2,k_2} + \boldsymbol{w}_b \right\|^2 - \|\boldsymbol{w}_b\|^2}{\sigma^2}) \right\}. \tag{21}$$

$$I(\boldsymbol{x}, \boldsymbol{E}; \boldsymbol{y}_e) = \frac{1}{F_1} I(\boldsymbol{E}; \boldsymbol{y}_e | \boldsymbol{x}) + \frac{1}{F_2} I(\boldsymbol{x}; \boldsymbol{y}_e). \tag{22}$$

TABLE 3. Activation patterns look-up table with $M = 2, N = 2, k = 2$.

Index Bits	Activation Patterns
[0,0]	$[\boldsymbol{d}_1,\boldsymbol{d}_2,0,0]$
[0,1]	$[0,\boldsymbol{d}_1,\boldsymbol{d}_2,0]$
[1,0]	$[0,0,\boldsymbol{d}_1,\boldsymbol{d}_2]$
[1,1]	$[\boldsymbol{d}_1,0,0,\boldsymbol{d}_2]$

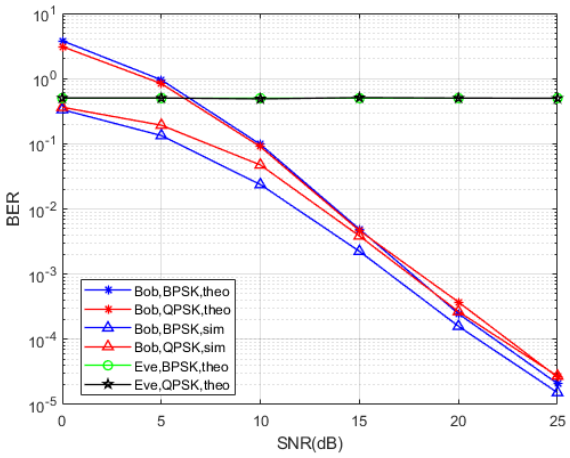

FIGURE 4. BER performance of the proposed scheme.

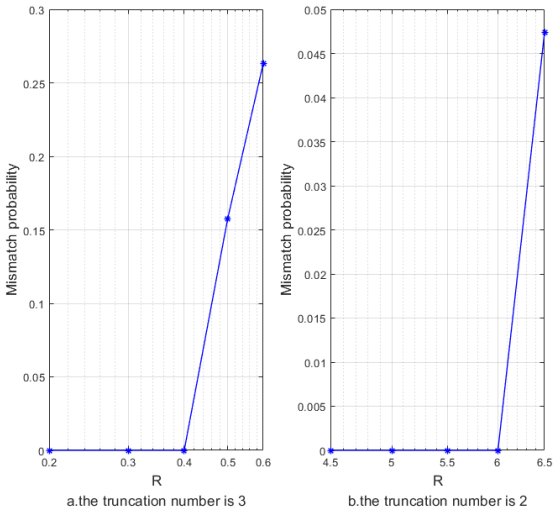

FIGURE 5. Mismatch probabilities for Alice and Bob at different truncated numbers.

$M = 4, N = 2, g = 2, k = 1$. First, we can see obviously from Fig. 4 that Eve's BER is always around 0.5 in all SNR regions, which means that she cannot do better than guessing so that the purpose of secure transmission is achieved. Then, comparing the simulation BER curves of Bob with the theoretical BER curves of Bob, we can find out that the theoretical BER of Bob approaches the simulated BER of Bob closely when SNR is larger than $10dB$. The gap between the theoretical BER and the simulated BER in the low SNR region is mainly due to the union bound in (18), while the gap in the high SNR region is mainly due to the exponential approximation of the Q-function in (17) [40], [41], [42].

When Alice and Bob estimate their angles with estimation errors, truncation operation is performed to get the same initial value. The estimation errors at Alice and Bob obey the uniform distribution. Assuming that the ideal angle is $\theta = 35$ degrees, θ_{up} of the uplink and θ_{down} of the downlink estimated at Alice and Bob satisfy that $\theta_{up} \sim U(35 - R, 35 + R)$ and $\theta_{down} \sim U(35 - R, 35 + R)$, where R is the maximum deviate angle caused by the estimation error and usually $R < 2.5$ [32]. First we check the probability of initial value mismatch at Alice and Bob by using different truncation numbers in Fig. 5. Denote the value of θ_{up} after the sigmoid function as A, and the value of θ_{down} after the sigmoid function as D. The mismatch probabilities that the initial value generated at Alice is different from that at Bob for different values of R and different truncation numbers are shown in Fig. 5. When the truncation number is 3, and $R \leq 0.4$ which means the estimation error is small, Alice and Bob can obtain the same initial value based on their estimated angles by using the truncation operation. But their initial values become mismatch when $R > 0.4$. If the truncation number decreases to 2, Alice and Bob can obtain the same initial value for most cases since from the figure we can see that the mismatch probability is 0 when $R \leq 6$ which is larger than 2.5. [32]. With this observation, we can find out that when estimation error is small, we can truncate the initial values and keep 3 digits after decimal separator. For most cases, keeping 2 digits after decimal separator of the initial values at Alice and Bob can promise a same Chaotic initial value for Alice and Bob which could guarantee the successful legitimate transmissions. In the following we will discuss the influence of truncation numbers on the BER performance of Bob and Eve.

Assuming that Eve uses the same angle estimation algorithm as Alice and Bob, that is, the estimated angle of Alice-Eve link at Eve satisfy $\theta_{Eve} \sim U(\theta' - R, \theta' + R)$, where θ' is the ideal angle of Alice-Eve link. In Fig. 6, the BERs of Bob and Eve are discussed for different estimation errors and different angles of Alice-Eve link, which indicate different positions of Eve. First, we discuss the BER in the case of more accurate estimations with $R = 0.4$ and choose the number of truncated decimal places as 3. The BER curves of Eve with $\theta' = \theta + \delta$ are shown as dashed lines in the figure, where δ represents the deviation of θ' from θ.

First we can see from Fig. 6 that by performing truncation, Bob can always decode the information successfully although Alice and Bob may estimate the angles differently. We first check the case that the estimation error is small and $R = 0.4$. As for Eve, when $\delta = 0.7$, its BER decreases as SNR increases at low SNR region, but shows a platform at higher SNR region. When δ increases to 1.5, Eve's BER stays around 0.5, which indicates that the eavesdropper cannot decode correctly. When the estimation is inaccurate and $R = 2.5$, the truncation number is chosen as 2. When the angle deviation

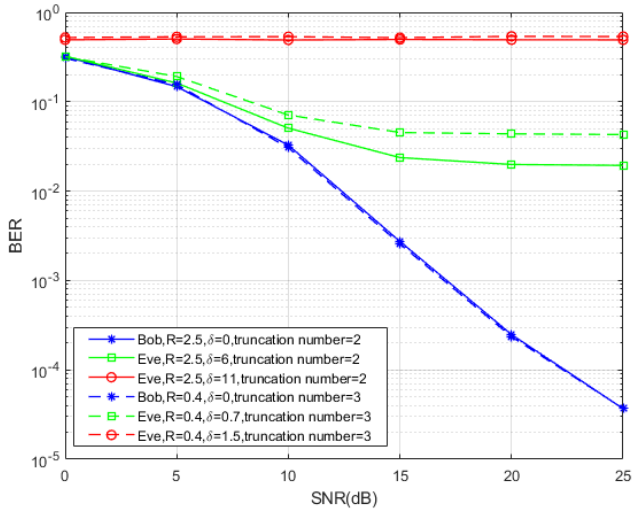

FIGURE 6. BER performance of different estimation errors and angle deviations.

of Eve is $\delta = 6$, Eve's BER decreases first but becomes flat around 2.5×10^{-2} after SNR$\geq$ 15dB.When δ increases to 11, Eve's BER stays around 0.5. Based on the above observations we can conclude that when the angle estimation is more accurate, Alice and Bob can get the same initial value to three decimal places. In this case, the secrecy can not be guaranteed if Eve's angle deviation δ is smaller than 1.5 degrees. When the angle estimation error increases, Alice and Bob have to decrease the truncation number to obtain the same initial value. In this case, Alice and Bob get the same initial value to two decimal places, and the secrecy can not be guaranteed if Eve's angle deviation δ is smaller than 11 degrees, which means the secure transmission region decreases due to the decrease of the truncation number.

VII. CONCLUSION

In this paper, a physical layer anti-eavesdropping scheme is proposed for the FDD IM-OTFS system. By exploiting the initial-value sensitivity and the aperiodicity property of Chaos sequences, a Chaos sequences based secure mapping scheme is designed, which introduces the time-variant activation rule and modulation rule for the IM-OTFS system, and the secure mapping rules cannot be obtained by Eve. To avoid secret sharing of the Chaos initial value, the angular reciprocity in FDD systems is used to generate the same initial value for Alice and Bob. A truncation method is proposed to provide robust secure transmission when angle estimation error exists. Numerical results show that the simulated BER fits the theoretical BER well in medium and high SNR regions, and the closed-form approximated secrecy rate fits the ergodic secrecy rate well in low and high SNR regions. The BER of Bob is not influenced by the proposed scheme even there are angle estimation errors. The BER of Eve is always around 0.5 for perfect angle estimations, but the secure transmission region decreases due to the increase of angle estimation errors and the decrease of the truncation number.

APPENDIX A

Considering the activation status matrix $\boldsymbol{E}$, we can rewrite the received signal as,

$$\boldsymbol{y}_b = \boldsymbol{H}_{eff}\boldsymbol{E}\boldsymbol{x} + \boldsymbol{w}. \tag{29}$$

Let

$$\boldsymbol{r}_b = \boldsymbol{y}_b - \boldsymbol{H}_{eff}\boldsymbol{E}_d\boldsymbol{x}_k, \tag{30}$$

then the received signal at the legitimate receiver follows the distribution that,

$$\mathbb{P}_b = \frac{1}{F_1F_2}\sum_{d=1}^{F_1}\sum_{k=1}^{F_2}\frac{1}{\pi\sigma^2}exp(-\frac{\|\boldsymbol{r}_b\|^2}{\sigma^2}). \tag{31}$$

So, the mutual information can be expressed as (21) where,

$$\boldsymbol{d}_{d,k}^{d_2,k_2} = \boldsymbol{H}_{eff}\boldsymbol{E}_d\boldsymbol{x}_k - \boldsymbol{H}_{eff}\boldsymbol{E}_{d_2}\boldsymbol{x}_{k_2}. \tag{32}$$

APPENDIX B

For the illegitimate receiver, we divide the mutual information into two parts. The first partof the mutual information between $\boldsymbol{y}_e$ and $\boldsymbol{x}$ expresses as (35), shown at the top of the next page, where,

$$\boldsymbol{\delta}_{t,k}^{t_2,k_2} = \boldsymbol{G}_{eff}\boldsymbol{E}_t\boldsymbol{x}_k - \boldsymbol{G}_{eff}\boldsymbol{E}_{t_2}\boldsymbol{x}_{t_2}, \tag{33}$$

$$\boldsymbol{\delta}_t^{t_2} = \boldsymbol{G}_{eff}(\boldsymbol{E}_t - \boldsymbol{E}_{t_2})\boldsymbol{x}_k. \tag{34}$$

And then, the mutual information between $\boldsymbol{y}_e$ and $\boldsymbol{E}$ when $\boldsymbol{x} = \boldsymbol{x}_k$ is shown as (36), at the top of the next page. Therefore, according to the chain rule for the mutual information, we can obtain the data rate of the illegitimate receiver as (22)

APPENDIX C

By means of the Jensen's inequality, the lower bound of R_b is,

$$\begin{aligned}
R_{bl} &= log_2(F_1F_2) - \frac{1}{F_1F_2}\sum_{d=1}^{F_1}\sum_{k=1}^{F_2} log_2 \sum_{d_2=1}^{F_1}\sum_{k_2=1}^{F_2} \\
&\quad \times \mathbb{E}_{\boldsymbol{H}_{eff},\boldsymbol{w}_b}\left\{exp(-\frac{\left\|\boldsymbol{d}_{d,k}^{d_2,k_2} + \boldsymbol{w}_b\right\|^2 - \|\boldsymbol{w}_b\|^2}{\sigma^2})\right\} \\
&= log_2(F_1F_2) - \frac{1}{ln2} - \frac{1}{F_1F_2}\sum_{d=1}^{F_1}\sum_{k=1}^{F_2} log_2 \sum_{d_2=1}^{F_1}\sum_{k_2=1}^{F_2} \\
&\quad \times \mathbb{E}_{\boldsymbol{H}_{eff},\boldsymbol{w}_b}\left\{exp(-\frac{\left\|\boldsymbol{d}_{d,k}^{d_2,k_2} + \boldsymbol{w}_b\right\|^2}{\sigma^2})\right\} \\
&= log_2(F_1F_2) - (\frac{1}{ln2} - 1) - \frac{1}{F_1F_2}\sum_{d=1}^{F_1}\sum_{k=1}^{F_2} \\
&\quad \times log_2 \sum_{d_2=1}^{F_1}\sum_{k_2=1}^{F_2} \mathbb{E}_{\boldsymbol{H}_{eff}}\left\{exp(-\frac{\left\|\boldsymbol{d}_{d,k}^{d_2,k_2}\right\|^2}{2\sigma^2})\right\}
\end{aligned}$$

$$I(\boldsymbol{x};\boldsymbol{y}_e) = log_2(F_2) - \frac{1}{F_1F_2}\sum_{t=1}^{F_1}\sum_{k=1}^{F_2}\mathbb{E}_{\boldsymbol{G}_{eff},\boldsymbol{w}_e}\left\{log_2\frac{\sum_{t_2=1}^{F_1}\sum_{k_2=1}^{F_2}exp(-\frac{\left\|\boldsymbol{\delta}_{t,k}^{t_2,k_2}+\boldsymbol{w}_e\right\|^2}{\sigma^2})}{\sum_{t_2=1}^{F_1}exp(-\frac{\left\|\boldsymbol{\delta}_t^{t_2}+\boldsymbol{w}_e\right\|^2}{\sigma^2})}\right\}. \tag{35}$$

$$I(\boldsymbol{E};\boldsymbol{y}_e|\boldsymbol{x}) = log_2(F_1) - \frac{1}{F_1F_2}\sum_{t=1}^{F_1}\sum_{k=1}^{F_2}\mathbb{E}_{\boldsymbol{G}_{eff},\boldsymbol{w}_e}\left\{log_2\sum_{t_2=1}^{F_1}exp(-\frac{\left\|\boldsymbol{\delta}_t^{t_2}+\boldsymbol{w}_e\right\|^2-\|\boldsymbol{w}_e\|^2}{\sigma^2})\right\}. \tag{36}$$

$$= log_2(F_1F_2) - (\frac{1}{ln2}-1) - \frac{1}{F_1F_2}\sum_{d=1}^{F_1}\sum_{k=1}^{F_2} \times log_2\sum_{d_2=1}^{F_1}\sum_{k_2=1}^{F_2}(1+\frac{\sigma_h^2\alpha_b}{2\sigma^2})^{-1}, \tag{37}$$

where

$$\alpha_b = \left\|\boldsymbol{E}_d\boldsymbol{x}_k - \boldsymbol{E}_{d_2}\boldsymbol{x}_{k_2}\right\|^2. \tag{38}$$

APPENDIX D

For the illegitimate receiver, the approximated $I(\boldsymbol{x};\boldsymbol{y}_e)$ can be expressed as,

$$I_{app}(\boldsymbol{x};\boldsymbol{y}_e) = log_2(F_2) - \frac{1}{F_1F_2}\sum_{t=1}^{F_1}\sum_{k=1}^{F_2} \times log_2\frac{\sum_{t_2=1}^{F_1}\sum_{k_2=1}^{F_2}(1+\frac{\sigma_g^2\alpha_e}{2\sigma^2})^{-1}}{\sum_{t_2=1}^{F_1}(1+\frac{\sigma_g^2\alpha_x}{2\sigma^2})^{-1}}, \tag{39}$$

where

$$\alpha_e = \left\|\boldsymbol{E}_t\boldsymbol{x}_k - \boldsymbol{E}_{t_2}\boldsymbol{x}_{k_2}\right\|^2, \tag{40}$$

$$\alpha_x = \left\|(\boldsymbol{E}_t - \boldsymbol{E}_{t_2})\boldsymbol{x}_k\right\|^2. \tag{41}$$

And then, the approximated $I(\boldsymbol{E};\boldsymbol{y}_e|\boldsymbol{x})$ can be expressed as,

$$I_{app}(\boldsymbol{E};\boldsymbol{y}_e|\boldsymbol{x}) = log_2(F_1) - \frac{1}{F_1F_2}\sum_{t=1}^{F_1}\sum_{k=1}^{F_2} \times log_2\sum_{t_2=1}^{F_1}(1+\frac{\sigma_g^2\alpha_x}{2\sigma^2})^{-1}. \tag{42}$$

REFERENCES

[1] V. W. Wong, R. Schober, D. W. K. Ng, and L.-C. Wang, *Key Technologies for 5G Wireless Systems*. Cambridge, U.K.: Cambridge Univ. Press, 2017.

[2] R. Hadani, S. Rakib, M. Tsatsanis, A. Monk, A. J. Goldsmith, A. F. Molisch, and R. Calderbank, "Orthogonal Time Frequency Space modulation," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2017, pp. 1–6.

[3] Z. Wei, W. Yuan, S. Li, J. Yuan, G. Bharatula, R. Hadani, and L. Hanzo, "Orthogonal time-frequency space modulation: A promising next-generation waveform," *IEEE Wireless Commun.*, vol. 28, no. 4, pp. 136–144, Aug. 2021.

[4] E. Basar, M. Wen, R. Mesleh, M. D. Renzo, Y. Xiao, and H. Haas, "Index modulation techniques for next-generation wireless networks," *IEEE Access*, vol. 5, pp. 16693–16746, 2017.

[5] T. Mao, Q. Wang, Z. Wang, and S. Chen, "Novel index modulation techniques: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 315–348, 1st Quart., 2019.

[6] X. Cheng, M. Zhang, M. Wen, and L. Yang, "Index modulation for 5G: Striving to do more with less," *IEEE Wireless Commun.*, vol. 25, no. 2, pp. 126–132, Apr. 2018.

[7] A. B. Saleem and S. A. Hassan, "On the performance of spatial modulation schemes in large-scale MIMO under correlated Nakagami fading," in *Proc. IEEE 91st Veh. Technol. Conf. (VTC-Spring)*, May 2020, pp. 1–5.

[8] H. Bitra and P. Ponnusamy, "Performance analysis of adaptive generalized spatial modulation," in *Proc. Int. Conf. Artif. Intell. Signal Process. (AISP)*, Jan. 2020, pp. 1–6.

[9] E. K. Hidir, E. Basar, and H. A. Cirpan, "On practical RIS-aided OFDM with index modulation," *IEEE Access*, vol. 11, pp. 13113–13120, 2023.

[10] J. Li, S. Dang, Y. Huang, P. Chen, X. Qi, M. Wen, and H. Arslan, "Composite multiple-mode orthogonal frequency division multiplexing with index modulation," *IEEE Trans. Wireless Commun.*, vol. 22, no. 6, pp. 3748–3761, Jun. 2023.

[11] E. Basar, Ü. Aygölü, E. Panayirci, and H. V. Poor, "Orthogonal frequency division multiplexing with index modulation," *IEEE Trans. Signal Process.*, vol. 61, no. 22, pp. 5536–5549, Nov. 2013.

[12] Y. Liang, L. Li, P. Fan, and Y. Guan, "Doppler resilient orthogonal time-frequency space (OTFS) systems based on index modulation," in *Proc. IEEE 91st Veh. Technol. Conf. (VTC-Spring)*, May 2020, pp. 1–5.

[13] H. Zhao, D. He, Z. Kang, and H. Wang, "Orthogonal time frequency space (OTFS) with dual-mode index modulation," *IEEE Wireless Commun. Lett.*, vol. 10, no. 5, pp. 991–995, May 2021.

[14] H. Ren, W. Xu, and L. Wang, "Orthogonal time-frequency space with improved index modulation," in *Proc. 15th Int. Conf. Signal Process. Commun. Syst. (ICSPCS)*, Dec. 2021, pp. 1–6.

[15] D. Feng, J. Zheng, B. Bai, J. Jiang, and L. Zheng, "In-phase and quadrature index modulation aided OTFS transmission," *IEEE Commun. Lett.*, vol. 26, no. 6, pp. 1318–1322, Jun. 2022.

[16] A. Tusha, S. Dogan-Tusha, S. Althunibat, E. Basar, K. Qaraqe, and H. Arslan, "Index modulation-aided IQ imbalance compensator for OTFS communications systems," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2022, pp. 2178–2183.

[17] J. Sun, Z. Wang, and Q. Huang, "Secure precoded orthogonal time frequency space modulation," in *Proc. 13th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2021, pp. 1–5.

[18] J. Hu, J. Shi, S. Ma, and Z. Li, "Secrecy analysis for orthogonal time frequency space scheme based uplink LEO satellite communication," *IEEE Wireless Commun. Lett.*, vol. 10, no. 8, pp. 1623–1627, Aug. 2021.

[19] K. Jo, *Satellite Communications Network Design and Analysis*. Boston, MA, USA: Artech House, 2011.

[20] M. Ashok Raj and G. Ananthi, "Performance analysis of OTFS modulation in vehicular networks," in *Proc. 2nd Int. Conf. Secure Cyber Comput. Commun. (ICSCCC)*, May 2021, pp. 198–201.

[21] Y. Gu, Z. Wu, Z. Yin, and X. Zhang, "The secrecy capacity optimization artificial noise: A new type of artificial noise for secure communication in MIMO system," *IEEE Access*, vol. 7, pp. 58353–58360, 2019.

[22] N. Nandan, S. Majhi, and H.-C. Wu, "Beamforming and power optimization for physical layer security of MIMO-NOMA based CRN over imperfect CSI," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 5990–6001, Jun. 2021.

[23] Z. Gao, S. Bai, X. Liao, and M. Liu, "Anti-eavesdropping scheme based on random mapping for GSM-MBM systems," *IEEE Access*, vol. 8, pp. 48416–48427, 2020.

[24] J. Liu, A. Ren, R. Sun, X. Du, and M. Guizani, "A novel chaos-based physical layer security transmission scheme for Internet of Things," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.
[25] Z. Liu, L. Zhang, Z. Wu, and J. Bian, "A secure and robust frequency and time diversity aided OFDM–DCSK modulation system not requiring channel state information," *IEEE Trans. Commun.*, vol. 68, no. 3, pp. 1684–1697, Mar. 2020.
[26] H. Zhang, L. Zhang, Y. Jiang, and Z. Wu, "Reliable and secure deep learning-based OFDM-DCSK transceiver design without delivery of reference chaotic sequences," *IEEE Trans. Veh. Technol.*, vol. 71, no. 8, pp. 8059–8074, Aug. 2022.
[27] Y. Yang and M. Guizani, "Mapping-varied spatial modulation for physical layer security: Transmission strategy and secrecy rate," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 877–889, Apr. 2018.
[28] H. Zhou, M. L. Honig, J. Liu, and W. Xiao, "Bi-directional training methods with frequency-division duplexing," *IEEE Trans. Wireless Commun.*, vol. 20, no. 10, pp. 6493–6505, Oct. 2021.
[29] Z. Zhong, L. Fan, and S. Ge, "FDD massive MIMO uplink and downlink channel reciprocity properties: Full or partial reciprocity?" in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2020, pp. 1–5.
[30] U. Ugurlu, R. Wichman, C. B. Ribeiro, and C. Wijting, "A multipath extraction-based CSI acquisition method for FDD cellular networks with massive antenna arrays," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2940–2953, Apr. 2016.
[31] Y. Han, T.-H. Hsu, C.-K. Wen, K.-K. Wong, and S. Jin, "Efficient downlink channel reconstruction for FDD multi-antenna systems," *IEEE Trans. Wireless Commun.*, vol. 18, no. 6, pp. 3161–3176, Jun. 2019.
[32] K. Hugl, K. Kalliola, and J. Laurila, "Spatial reciprocity of uplink and downlink radio channels in FDD systems," in *Proc. COST TD*, May 2002, vol. 273, no. 2, pp. 66–77.
[33] W. Yan, Z. Jiang, X. Huang, and D. Qun, "Generalized 2D polynomial chaotic map and its application in secure communication," *J. Commun.*, vol. 43, no. 9, 2022, pp. 1684–1697.
[34] L. R. Tang, Q. Zuo, and W. X. Cui, "Synchronization scheme using four-dimensional chaotic system for OFDM," *J. Commun.*, vol. 31, no. 1, pp. 73–84, 2010.
[35] G. D. Surabhi, R. M. Augustine, and A. Chockalingam, "On the diversity of uncoded OTFS modulation in doubly-dispersive channels," *IEEE Trans. Wireless Commun.*, vol. 18, no. 6, pp. 3049–3063, Jun. 2019.
[36] M. Chiani and D. Dardari, "Improved exponential bounds and approximation for the Q-function with application to average error probability computation," in *Proc. Global Telecommun. Conf. (GLOBECOM)*, vol. 2, Nov. 2002, pp. 1399–1402.
[37] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 1985.
[38] F. Wu, W. Wang, C. Dong, and L.-L. Yang, "Performance analysis of secret precoding-aided spatial modulation with finite-alphabet signaling," *IEEE Access*, vol. 6, pp. 29366–29381, 2018.
[39] X. Yu, Y. Hu, Q. Pan, X. Dang, N. Li, and M. H. Shan, "Secrecy performance analysis of artificial-noise-aided spatial modulation in the presence of imperfect CSI," *IEEE Access*, vol. 6, pp. 41060–41067, 2018.
[40] H. Jafarkhani, *Space-Time Coding: Theory and Practice*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[41] S. Dang, G. Ma, B. Shihada, and M.-S. Alouini, "A novel error performance analysis methodology for OFDM-IM," *IEEE Wireless Commun. Lett.*, vol. 8, no. 3, pp. 897–900, Jun. 2019.
[42] S. Dang, S. Guo, J. P. Coon, B. Shihada, and M.-S. Alouini, "Enhanced Huffman coded OFDM with index modulation," *IEEE Trans. Wireless Commun.*, vol. 19, no. 4, pp. 2489–2503, Apr. 2020.

KEJIA MA received the B.E. degree in information engineering from Xi'an Jiaotong University, Xi'an, China, in 2023, where she is currently pursuing the master's degree in information and communications engineering. Her research interests include physical layer security and index modulation.

ZHENZHEN GAO received the B.S. degree in communication engineering from Lanzhou University, Lanzhou, China, in 2005, and the Ph.D. degree from Xi'an Jiaotong University, Xi'an, China, in 2011. From August 2009 to September 2011, she was a Visiting Student with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD, USA. Since 2012, she has been with the School of Information and Communication Engineering, Xi'an Jiaotong University, where she is currently an Associate Professor. Her current research interests include physical-layer security, index modulation, and advanced techniques in 5/6G wireless communication networks.

JINCHI WANG received the B.E. degree in information engineering from Xi'an Jiaotong University, Xi'an, China, in 2023, where he is currently pursuing the master's degree in information and communications engineering. His current research interests include anti-jamming techniques and intelligent transmission techniques in wireless communication systems.

LINLING CHENG received the B.E. degree in information engineering and the M.E. degree in information and communication engineering from Xi'an Jiaotong University, Xi'an, China, in 2020 and 2023, respectively. Her research interests include physical layer security, index modulation, and OTFS systems.