Article

Underlying Security Transmission Design for Orthogonal Time Frequency Space (OTFS) Modulation

Wei Liang 1,2, Xuan Liu 2, Jia Shi 2,*, Lixin Li 1 and Junfan Hu 2

1 School of Electronics and Information, Northwestern Polytechnical University, Xi’an 710072, China
2 State Key Laboratory of Integrated Services Networks, Xidian University, Xi’an 710071, China
* Correspondence: jiashi@xidian.edu.cn

Abstract: With the aim of ensuring secure transmission in high-mobility wireless scenarios, this paper proposes a 2D permutation-aided Orthogonal Time Frequency Space (OTFS) secure transmission scheme, which uses the Gosudarstvennyi Standard (GOST) algorithm to perform disturbance control on the OTFS modulation domain. Furthermore, we develop an improved SeLective Mapping (SLM) algorithm, which can significantly improve the Peak-to-Average Power Ratio (PAPR) problem with very low complexity. In addition, we carry out the security analysis, investigating the proposed scheme’s resistance performance to a range of effective attacks. Finally, our numerical results show that our proposed transmission scheme can guarantee the underlying security property of OTFS.

Keywords: secure transmission; OTFS; security analysis

1. Introduction

As a mobile network, 6G will be a fully connected world integrating terrestrial wireless networks [1]. It is no longer a simple breakthrough in network capacity and transmission rate but the realization of the interconnection of everything [2]. As a result, many new high-mobility wireless services have emerged, such as the Low Earth Orbit (LEO) communication satellite, unmanned aerial vehicle (UAV) communications, high-speed rail communications, and Internet of Vehicles communications [3]. However, these new wireless services all have the characteristics of high mobility, which will inevitably bring a severe Doppler effect problem. Due to the additional frequency components introduced by Doppler spread, it will result in severe inter-symbol crosstalk and a huge degradation of link reliability.

Orthogonal Frequency Division Multiplexing (OFDM) technology has been widely used in 5G mobile networks due to its high spectrum utilization [4]. OFDM technology combines frequency diversity and time diversity organically, which not only can greatly improve channel capacity but also can effectively resist multipath fading and interference [5]. However, OFDM transmissions have poor reliability performance in high-mobility scenarios, in which the high Doppler frequency shift can easily destroy the orthogonality between OFDM subcarriers. Although the OFDM in the 5G system adopts a larger and more flexible subcarrier spacing design, the increase in the subcarrier spacing will shorten the Cyclic Prefix (CP) and reduce the anti-multipath capability, as well as degrade the spectrum efficiency [6]. Furthermore, the channel response in a high-mobility environment presents fast time-varying and non-stationary characteristics, which greatly increase the overhead for channel estimation under the OFDM scheme. Recently, R. Hadani et al. proposed a new modulation method, namely Orthogonal Time Frequency Space (OTFS) modulation, for combating Doppler spread in high-mobility scenarios. In particular, the OTFS modulation scheme places the data in the Delay Doppler (DD) domain, which is relatively insensitive to time changes, and spreads each symbol in the entire Time Frequency (TF) domain by the Inverse Symplectic Finite Fourier Transform (ISFFT) so that each OTFS symbol experiences almost the same channel gain.
The OTFS technique has drawn a lot of research attention, such as [7–13]. In particular, refs. [7–9] were devoted to researching the Peak-to-Average Power Ratio (PAPR) of the OTFS system, wherein [7] proposed a MuLaw companding technique to reduce the PAPR of the OTFS, and [9] proposed an effective PAPR reduction method based on an iterative limiting and filtering framework. The channel estimation methods designed for OTFS transmission were studied in [10–12]. In a little more detail, ref. [10] proposed an algorithm based on Orthogonal Matching Pursuit (OMP) and Modified Subspace Pursuit (MSP) for the DD channel estimation in OTFS multiple access (OTFS-MA) systems on the uplink. In Multiple-Input Multiple-Output (MIMO) scenarios based on the OTFS, ref. [11] proposed an iterative signal detection algorithm based on message passing and a channel estimation scheme in the DD domain. An embedded pilot-assisted channel estimation scheme was proposed in [12].

Under the OTFS scheme, especially for future high-mobility scenarios, secure transmission is particularly important and still faces huge challenges. As is known, the future 6G mobile network contains a range of high-mobility scenarios, such that UAV communications are deployed to supplement the terrestrial networks, building an integrated air–space–earth–sea network to cover a much wider area. In this case, the probability of eavesdropping on the communication links significantly increases, and thus there is a greater risk of information exposure. Nevertheless, as far as we know, very limited studies [13,14] have been devoted to the security issue of OTFS transmissions.

To ensure the security of wireless communications, traditional security mechanisms based on cryptography are mainly deployed on multilayer protocols above the physical layer, and the main idea is to improve the security of the wireless system by using a variety of upper layer authentication mechanisms. For example, at the Medium Access Control (MAC) layer, the MAC address is authenticated so that access is only granted to legitimate users. At the network layer, two authentication protocols for the wireless Local Area Network (LAN) security access WPA and WPA2 were adopted [15,16]. Although upper layer encryption can enhance the security of the wireless system, the corresponding techniques are completely dependent on the confidentiality of the key and the computational complexity. However, with the continuous development of quantum computing technology and breakthroughs in computing power, traditional cryptographic schemes may be easily broken, and they face great challenges. Moreover, one of the prerequisites for upper layer encryption is that the physical layer can actively provide smooth and error-free transmission, which is difficult to achieve in practical scenarios [17]. In contrast, physical layer security techniques can compensate well for the shortcomings of traditional encryption schemes and have gradually gained widespread attention in recent years. Compared with traditional encryption methods, without considering the computational power of attackers, the physical layer security technology can make full use of the instantaneity and randomness of wireless channels to achieve secure transmission without sharing the key between the legitimate transmitter and receiver. The principle of physical layer key generation technology is to use the reciprocity, time variability, and spatial uniqueness of wireless channels to generate the key. Depending on the randomness of a wireless channel, the key generation schemes are mainly divided into the following four types: Channel State Information (CSI)-based key generation technology [18], signal strength-based key generation technology [19], phase-based key generation technology [20], and eavesdropping encoding key generation technology [21]. Further, ref. [22] proposed the key generation scheme under active attack, which used random detection signals to combine the user-generated randomness and channel randomness. Ref. [23] proposed an adaptive channel detection scheme based on a proportional-integral-derivative controller, which can achieve the desired Key Generation Rate (KGR) by adjusting the detection rate.

As far as we know, the current research on OTFS secure transmission is still in its infancy. In particular, ref. [13] studied the secrecy performance of an OTFS-based uplink LEO Sat-Com system, where a cooperative UAV was employed to send jamming signals against the reconnaissance satellite. However, the study only targeted the uplink LEO
Sat-Com scenario and is not universal. Ref. [14] studied the security performance of the unicast–multicast streaming system by deriving and analyzing the maximum secrecy rate and positive secure capacity probability (PSCP) of unicast transmission. Ref. [24] proposed a novel physical layer security transmission scheme by encrypting the Discrete Fourier Transform (DFT) matrix to guarantee the underlying security property of the OFDM. It is very unfortunate that there is currently no research on physical layer security via control of the modulation matrix in the OTFS. Against the background above, we are motivated to study secure transmission by controlling the modulation matrix for the OTFS transmission in high-mobility communication scenarios. Our key contributions are summarized as follows:

- We propose a 2D permutation OTFS secure transmission scheme that uses the Gosudarstvenyi Standard (GOST) algorithm to perform disturbance control on the OTFS modulation domain so as to realize the underlying security of the OTFS transmission. By utilizing the instantaneities and uniquenesses of wireless channels, the GOST algorithm can generate a control sequence to perturb the ISFFT matrix under OTFS modulation.
- We propose a so-called Selective Mapping (SLM) algorithm, which can significantly improve the PAPR problem of our secure OTFS transmission. With very low complexity, the SLM algorithm aims to select the best transition matrix to multiply with the TF domain signal for the sake of ensuring the low PAPR characteristic.
- We conduct a security analysis for our OTFS secure transmission. We prove our scheme has a promising resistance performance to a range of effective attacks, including brutal force, chosen-plaintext, statistical attacks, etc.
- We carry out a comprehensive simulation evaluation. Our experimental results show that our proposed transmission scheme can guarantee the underlying security property of the OTFS. Furthermore, compared to the OFDM scheme, our proposed scheme can reduce the PAPR by 20% and improve the BER by at least 4 dB under the same security requirements.

The rest of this paper will be organized as follows: In Section 2, we briefly introduce the OTFS system model. In Section 3, we propose the design for a 2D permutation-aided OTFS secure transmission scheme. In Section 4, we introduce the principle of the key generation algorithm and analyze its performance. In Section 5, we conduct a security performance analysis of the proposed transport mechanism. In Section 6, the performance of the design of our 2D permutation-aided OTFS secure transmission is evaluated. Finally, Section 7 concludes the paper.

2. System Model

We assume a classic three-node secure communication model, in which the transmitter (Alice) transmits private information to the legitimate receiver (Bob) with the risk of being passively eavesdropped by an illegal eavesdropper (Eve). We assume that Alice is in a state of high mobility and that Bob and Eve are static. All nodes are equipped with a single antenna. Let us assume that each communication link has \( L \) propagation paths. The channel response of the high-mobility channels can be given by

\[
h(\tau, v) = \sum_{p=1}^{L} h_p \delta(\tau - \tau_p) \delta(v - v_p),
\]

where \( \tau_p = \frac{l_p M \Delta f}{c} \) and \( v_p = \frac{k_p N T}{c} \) denote the delay and the Doppler shift, respectively, and \( h_p \) is the Rayleigh fading.

To overcome the Doppler effect in a high-mobility scenario, Alice transmits signals to Bob based on the OTFS scheme. Specifically, the signal in the DD domain is denoted by \( x[k, l] \), where \( k \in \{0, \ldots, N - 1\} \). \( N \) represents the number of Doppler bins, \( l \in \{0, \ldots, M - 1\} \), and \( M \) represents the number of Delay bins. Firstly, the symbols \( x[k, l] \) are
preprocessed by using the Inverse Symplectic Finite Fourier Transform (ISFFT), thereby deriving the TF domain signal as

$$X[n, m] = \frac{1}{\sqrt{NM}} \sum_{k=0}^{N-1} \sum_{l=0}^{M-1} x[k, l] e^{\frac{2\pi}{N}(nk - ml)},$$

where $n \in \{0, \ldots, N - 1\}$ and $m \in \{0, \ldots, M - 1\}$. Then, by applying the Heisenberg transform, the signal $X[n, m]$ is converted into the time domain signal. Assume that the sending and receiving pulses satisfy the bi-orthogonal property. After applying the Wigner transform, the signal in the TF domain received by Bob can be expressed as

$$Y[n, m] = H[n, m]X[n, m] + W[n, m],$$

where $W[n, m]$ is the complex Gaussian distributed noise in the TF domain, and $H[n, m] = \int h(\tau, \nu) e^{2\pi i n \tau} e^{-2\pi i (\nu + m f_0) \nu} d\tau d\nu$. By using the Symplectic Finite Fourier Transform (SFFT), the signal $Y[n, m]$ in the TF domain is transformed into the signal $y[k, l]$ in the DD domain:

$$y[k, l] = \frac{1}{\sqrt{NM}} \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} Y[n, m] e^{-\frac{2\pi}{N}(nk - ml)}.$$  

3. 2D Permutation-Aided OTFS Secure Transmission

In this section, we propose a so-called 2D permutation-aided OTFS secure transmission scheme, which aims to generate control sequences by utilizing the instantaneities and uniquenesses of wireless channels. Then, the control sequence is used to perturb the OTFS modulation domain, which ensures the underlying security of the OTFS transmission. Furthermore, we develop the SLM algorithm to guarantee the low PAPR feature of the OTFS secure transmission.

3.1. Design Of 2D Permutation-Aided OTFS Secure Transmission

As shown in Figure 1, the proposed OTFS secure transmission is mainly divided into four stages: (1) security sequence generation, (2) interleaving replacement, (3) signal modulation, and (4) signal demodulation.

- security sequence generation

Alice and Bob detect the channel information through channel measurement and use the channel information as the input of the GOST method (detailed in Section 4)-based
secret key generation algorithm to generate the index sequence (secret key) that controls the permutation, denoted by $D_x, D_y, D_z, D_w$.

- **interleaving replacement**

According to the index sequence, row permutation and column permutation are performed on the IFFT matrix and the FFT matrix, respectively, as follows:

$$F_{M+M} = \frac{1}{M} e^{-j2\pi(\alpha-1)(\beta-1)/M}$$

where $\alpha$ and $\beta$ are the row index and column index of the standard FFT matrix, and $w_0^T, w_1^T, \cdots, w_{M-1}^T$ are the row vectors. The index vectors $D_x$ and $D_y$ are used to replace the rows and columns of the standard FFT matrix. The new FFT matrix can be obtained by the following two steps. During the first step, the rows of the FFT matrix are permutated by the index vectors $D_x$. The new FFT matrix can be expressed as

$$F_{M+M}' = \begin{bmatrix} w_{D_x(0)}^T, w_{D_x(1)}^T, \cdots, w_{D_x(M-1)}^T \end{bmatrix}$$

During the second step, the columns of the FFT matrix are permutated by the index vectors $D_y$. Then, the modified FFT matrix can be expressed as

$$F_{M+M}'' = \begin{bmatrix} r_{D_y(0)}^T, r_{D_y(1)}^T, \cdots, r_{D_y(M-1)}^T \end{bmatrix}$$

To describe row permutation and column permutation more clearly, an example for a $3 \times 3$ matrix is given in Figure 2. Assuming that $D_z = (3, 1, 2)$ and $D_w = (3, 1, 2)$, the entire permutation process is described as follows. Firstly, perform row permutation by using the row index sequence $D_x$. Secondly, perform column permutation by using the column index sequence $D_y$.

**Figure 2.** Flowchart of matrix permutation.

The modified IFFT matrix is obtained by repeating the above steps using the index vector $D_z, D_w$.

- **OTFS modulation**

The signal $x[k, l]$ in the DD domain is converted into the signal $X[n, m]$ in the TF domain, as follows:

$$X[n, m] = P_{ISFFT} \left( \frac{1}{\sqrt{NM}} \sum_{k=0}^{N-1} \sum_{l=0}^{M-1} x[k, l] e^{j2\pi(\frac{nk}{N} - \frac{ml}{M})} \right)$$

where $n \in \{0, \ldots, N - 1\}, m \in \{0, \ldots, M - 1\}, P_{ISFFT}(\cdot)$ denotes the ISFFT transform after the FFT matrix and IFFT matrix permutate. Then, let us multiply the TF domain signal $X[n, m]$ by a multiple $U$ group of conversion matrices $T \in \{T_1, T_2, \cdots, T_U\}$, as follows:

$$X_t[n, m] = T_t X[n, m],$$
where \( i = 1, 2, \cdots, U \), \( T_i \) is the \( i \)-th conversion matrix. Note that \( T_i = \left[ t_i, t_i^{(1)}, \cdots, t_i^{(N-1)} \right] \). 
\( t_i^{(1)} \) is obtained by cyclically shifting \( t_i \), in which \( t_i = [p_1, 0, \cdots, 0, p_2, 0, \cdots, 0, p_3, 0, \cdots, 0, p_4, 0, \cdots, 0] \) \[25\], and then generating a multiple \( U \) group of time-domain candidate signals through the Heisenberg transform. After this, it selects the group with the smallest PAPR for transmission, as follows:

\[
s_i(t) = \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} X_i[n, m] g_{tx}(t - nT)e^{j2\pi f(t-nT)},
\]

\( s(t) = \min(s_1(t), s_2(t), \cdots, s_U(t)) \),

where \( g_{tx}(t) \) is the transmission pulse shape. This can be seen as a two-dimensional extension of the OFDM modulation transform. When the input signal \( s(t) \) passes through the wireless channel, it will be affected by the channel delay and Doppler shift, as follows:

\[
r(t) = \int \int h(\tau, \nu)s(t - \tau)e^{j2\pi f(t-\tau)}d\tau dv + w(t),
\]

where \( w(t) \) denotes the white Gaussian noise, \( h(\tau, \nu) = \sum_{p=1}^{L} h_p \delta(\tau - \tau_p) \delta(\nu - \nu_p) \).

**OTFS demodulation**

By using the Wigner transform, which obtains the mutual ambiguity function and then performs sampling, the received signal \( r(t) \) in the time domain is converted into the TF domain signal, denoted by \( Y[n, m] \), as follows:

\[
Y[n, m]' = \int g_{rx}(t - \tau)e^{-j2\pi f(t-\tau)}r(t)\left| \tau=nT, \nu=m\Delta f, \right.
\]

where \( g_{rx}(t) \) is the reception pulse shape. Assuming that the transmit pulse \( g_{tx}(t) \) and the receive pulse \( g_{rx}(t) \) are ideal, we have \( \int e^{-j2\pi m\Delta f(t-nT)}g_{rx}(t-nT)g_{tx}(t)dt = \delta(m)\delta(n) \).

Since the TF domain signal is multiplied by the conversion matrix before the Heisenberg transform, the corresponding inverse transformation must be performed after the Wigner transform to obtain the correct DD domain signal \( Y[n, m] \). Then, by using the SFFT, the signal \( Y[n, m] \) in the TF domain is transformed into the signal \( y[k, l] \) in the DD domain:

\[
y[k, l] = P_{SFFT}\left( \frac{1}{\sqrt{NM}} \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} Y[n, m]e^{-j2\pi f\left(\frac{n}{N} - \frac{m}{M}\right)} \right),
\]

where \( k \in \{0, \cdots, N - 1\} \) and \( l \in \{0, \cdots, M - 1\} \). Further, \( P_{SFFT}(\cdot) \) denotes the SFFT transform after the FFT matrix and IFFT matrix de-permutate.

**3.2. SLM Algorithm for PAPR Reduction**

To realize secure OTFS transmission, we need to carefully deal with the PAPR problem to avoid eavesdropping. For this reason, we apply the SLM algorithm to our OTFS transmission. In particular, it generates multiple sets of candidate sequences by multiplying the QAM symbols with the \( U \) groups of the phase rotation vectors and selects the time-domain signal with the lowest peak-to-average power ratio as the transmission sequence, which requires \( U \) ISFFT transforms and Heisenberg transforms. To reduce the computational complexity, we generate candidate sequences by multiplying the time-frequency domain signal sequence by the transition matrices. The principle of the SLM algorithm developed is described in Figure 3:
Assuming that the OTFS system contains $M$ symbols and $N$ subcarriers, $x$ represents the input signal in the DD domain, $X$ represents the signal in the TF domain, $Q_1$ is an $N \times N$ IFFT matrix, and $Q_2$ is an $M \times M$ FFT matrix. Then, we have $X = ISFFT(x) = Q_1 x Q_2$. There are $U$ different phase rotation vectors, and the representation is as follows:

$$
\gamma_i = \begin{bmatrix}
  p^i_0 & p^i_0 & \ldots & p^i_0 \\
  p^i_1 & p^i_1 & \ldots & p^i_1 \\
  \vdots & \vdots & \ddots & \vdots \\
  p^i_{N-1} & p^i_{N-1} & \ldots & p^i_{N-1}
\end{bmatrix},
$$

where $i = 1, 2, \ldots, U$, $p^i_k = e^{j \varphi^i_k}$ follows a uniform distribution between $[0, 2\pi]$. Suppose that the ISFFT transform is used to change $X$ and $X_i$ into $S = x$ and $S_i = R_i x$, respectively, where $R_i$ is the phase transformation matrix corresponding to $\gamma_i$. Therefore, $X = ISFFT(x) = Q_1 x Q_2$, $X_i = ISFFT(x) = Q_1 R_i x Q_2$. Given that $T_i = Q_1 R_i Q_1^{-1}$, we have

$$
T_i = Q_1 R_i Q_1^{-1} = [p^{(1)}_i, p^{(2)}_i, \ldots, p^{(N-1)}_i],
$$

where $p^{(k)}_i$ is obtained by circularly shifting $p_i$ down by $k$ elements. As shown in [25], by choosing the appropriate $\gamma$, the complexity of SLM can be significantly reduced.

4. Secret Key Generation Algorithm

In our proposed secure OTFS transmission scheme, the key generation algorithm plays the core role. In this section, we propose the key generation algorithm, named GOST, as well as provide an analysis of its characteristics.

4.1. Gost Method-Based Secret Key Generation

As shown in Figure 4, the GOST-based key generation algorithm contains two parts: round function and compression–expansion.

The detailed Gost algorithm is detailed in Algorithm 1. Since our algorithm uses 64-bit grouping on the input data, we must first change the input data to a multiple of 64. That is, if the length of the data to be encrypted is less than 64 bits, it must be padded to 64 bits; if the length of the data to be encrypted exceeds 64 bits, it must first be padded to a multiple of 64. Then, the data that need to be encrypted are divided into two parts, each containing 32 bits. Because the round function is iterated for 64 rounds, we use a 2048-bit key and perform the addition of the (mod2$^{32}$) operation with the right part of the data to obtain the new right part, denoted by itmp. Then, the itmp passes through the S box. That is, the 32-bit itmp is equally divided into eight blocks; each block has four bits, and the value of each block does not exceed Oxf. The S box of the secret key generation algorithm has a total of eight groups that correspond to these eight blocks one-to-one. For example, if the value of the third block is eight, then replace the original value of the third block with the value at the eighth column of the third group of the S box. Repeat the above steps eight times to obtain a new itmp. Subsequently, the new itmp and the left part perform the XOR

![Figure 3. Flowchart of SLM.](image)

This is a flowchart of SLM.
operation to obtain the right part of the next round. Additionally, the left part of the next round is obtained from the right part of the previous round, as follows:

\[
R_{i+1}^{j+4} = Sbox_j(R_{i+1}^{j+4} \otimes K_i) \oplus R_i^j,
\]

\[
R_{i+1}^j = R_{i+1}^{j+4},
\]

where \( i = 1, 2, \cdots, 64 \) represents the \( i \)-th iteration, \( j = 1, 2, 3, 4 \) represents the \( j \)-th S box, \( \otimes \) and \( \oplus \), respectively, represent the addition of \((\text{mod} 2^{32})\) and the binary operation of XOR. At this point, one round of non-linear transformation is complete. Repeat the above steps. The output ciphertext composed of eight parts can be obtained after 64 iterations. Then, by applying the rotate left operator, the final ciphertext can be obtained, as shown in Equation (19).

\[
C = \left( \left( R_1^{64} \oplus R_2^{64} \right) \oplus \left( R_3^{64} \oplus R_4^{64} \right) \right) \oplus \left( \left( R_5^{64} \oplus R_6^{64} \right) \oplus \left( R_7^{64} \oplus R_8^{64} \right) \right).
\]

Figure 4. Flowchart for the GOST method-based secret key generation.

In this article, since we use the detected channel state information as the input of this secret key generation algorithm, we can obtain multiple corresponding output ciphertexts. Using \( N = 128 \) as an example, in order to control the permutation of the IFFT matrix of the ISFFT transformation, we obtain 128 ciphertext outputs. Sort the output ciphertext in ascending order and then obtain the index sequence \((D_z, D_w)\) that con-
controls the row permutation and column permutation, respectively, as shown in Figure 5.

**Algorithm 1: GOST Method-Based Secret Key Generation.**

**Input:** Channel state information \( H \).

**Initialize:** \( R = \text{zeros}(8,8); \) \( \text{tod} = \text{d2b}(H,64); \)

```plaintext
for \( n = 1 \rightarrow \text{size}(R,1); \)
    \( \text{todex}(n,:) = \text{tod}((n-1)*8+1:(n-1)*8+8); \)
end for;
for \( i = 0 \rightarrow 63; \)
    First, \( R_{\text{right}} \) performs \( \text{mod2}^n \) with key;
    second, \( R_{\text{right}} \) passes through the S box;
    Third, \( R_{\text{right}} \) and \( R_{\text{left}} \) perform XOR operation;
    Fourth, update \( R_{\text{right}} \) and \( R_{\text{left}} \) following function (17) and function (18), respectively;
end for;
Apply the rotate left operator following function (19).
```

![Flowchart of obtaining permutation index vector.](image-url)

**Figure 5.** Flowchart of obtaining permutation index vector.

### 4.2. Characteristic Analysis for Secret Key

The performance of the key can directly determine the security performance of the OTFS transmission. In this section, the main performance tests are for randomness and complexity. Let us first clarify the testing conditions as follows. The length of the sequence is \( L = 10,000 \). In each test, we select five sets of data streams for the GOST algorithm, the DES algorithm, and the chaotic mapping algorithm, ref. [26] respectively.

#### 4.2.1. Lempel–Ziv Complexity

The Lempel–Ziv (LZ) complexity is a simple algorithm for calculating sequence complexity by calculating the rate at which new patterns appear in a sequence. It was first proposed by Lempel and Ziv. Since this method is applicable to symbol sequences, the data sequence must be quantized in advance. That is, the average value of all data must be calculated. Data larger than the average value are set to one, and data smaller than the average value are set to zero. The brief idea of LZ complexity is as follows: \( c(n) \) is defined as the complexity count of a given symbol sequence \( S = (s_1,s_2,\cdots,s_n) \). \( b(n) \) is the progressive behavior of a random sequence. \( b(n) = \lim_{n \to \infty} c(n) = n / \log_2 n \), and \( C_{\text{LZ}}(n) = c(n) / b(n) \). As we all know, the complexity of completely random sequences tends toward one, while the regular sequence tends toward zero [27]. That is, the larger the \( C_{\text{LZ}} \) is, the weaker the periodicity of the symbol sequence. The more new patterns there are, the higher the complexity becomes. As can be seen in Figure 6, the complexity of the sequence generated by the GOST algorithm we used is the highest.
4.2.2. Randomness

In practical applications, for keys, good randomness is essential for secure transmission. Therefore, we use the randomness test suite developed by the National Institute of Standards and Technology (NIST) to evaluate the randomness of the generated keys, referred to as the NIST test. The NIST test uses 16 test methods for randomness testing. The significance level $\alpha$ is used to characterize the randomness of the key, and it is set as 0.01. Furthermore, the $p$-value is the probability that a sequence has better randomness than a true random sequence. If the $p$-value $\geq \alpha$, it means that the sequence has passed the randomness test. We use the software stst-2.1.2 to test the randomness of the generated sequence and compare it with the randomness of the sequence generated by the chaotic algorithm and the block cipher algorithm DES. It can be seen from Figure 7 that more than half of the sequences generated by the chaotic algorithm cannot exceed 0.01, so it did not pass the randomness test. Even the sequence generated by the GOST algorithm exceeds 0.05. Moreover, more than half of the $p$-value of the sequence generated by the GOST algorithm exceeds the $p$-value of the sequence generated by the DES algorithm. In summary, the key sequence generated by the proposed method has strong randomness.

| Test Specification                  | $p$-value (GOST) | $p$-value (DES) | $p$-value (Chaotic) |
|-------------------------------------|-----------------|----------------|--------------------|
| Frequency Test                      | 0.510538        | 0.445904       | 0.780797           |
| Block Frequency Test                | 0.712821        | 0.798806       | 0.000000           |
| Cumulative Sums Test(Forward)       | 0.384284        | 0.725238       | 0.210855           |
| Cumulative Sums Test(Reverse)       | 0.661509        | 0.754394       | 0.359852           |
| Runs Test                           | 0.238969        | 0.024416       | 0.130706           |
| Longest Run Test                    | 0.346482        | 0.296694       | 0.000000           |
| Rank Test                           | 0.689899        | 0.799782       | 0.034088           |
| FFT Test                            | 0.152271        | 0.185594       | 0.000000           |
| Non Overlapping Template Test       | 0.979779        | 0.973244       | 0.544944           |
| Overlapping Template Test           | 0.338457        | 0.53974        | 0.000102           |
| Universal Test                      | 0.705048        | 0.600986       | 0.000000           |
| Approximate Entropy Test            | 0.203306        | 0.051002       | 0.000000           |
| Random Excursions Test              | 0.902665        | 0.933855       | 0.000000           |
| Random Excursions Variant Test      | 0.962649        | 0.960599       | 0.000000           |
| Serial Test                         | 0.772202        | 0.401258       | 0.000000           |
| Linear Complexity Test              | 0.616689        | 0.590102       | 0.205106           |

Figure 6. LZ complexity simulation results.

Figure 7. NIST test.
5. Security Performance Analysis

To evaluate the security of the proposed secure OTFS scheme, we consider its resistance to some effective attacks (including brutal force, chosen-plaintext, and statistical attacks). Here, we make the following assumptions about the eavesdropper, Eve. First, for all data packets exchanged by Alice and Bob, Eve can completely overhear. Second, Eve completely understands the secret key generation algorithm. Third, Eve will not interfere with Alice and Bob.

5.1. Brutal Force Attacks

Brutal force attacks are also exhaustive search attacks. In this attack mode, the attacker Eve insists on trying all possible secret keys in the secret key space until the correct secret key is successfully found. In fact, when the key space is large enough, it will cause the exhaustive search to fail, thereby resisting brutal force attacks. In other words, whether an encryption system can resist brutal force attacks depends on the size of the key space. Because our key is extracted based on channel state information, the slightest change in the channel will result in a completely different key. Take the OTFS system with $N = 256$ and $M = 16$ as an example, the size of the IFFT matrix is $256 \times 256$, so its key space size is $256!$; the size of the FFT matrix is $16 \times 16$, so its key space size is $16!$. Therefore, the total key space of our proposed transmission mechanism is $10^{578}$. Assuming that the fastest computer, whose calculation speed is $2.5 \times 10^{13}/s$ that, is used to obtain the correct secret key, the illegal eavesdropper Eve will spend $10^{556}$ years. This will cause the exhaustive search to fail, so the transmission mechanism we propose is sufficient to resist brutal force attacks.

5.2. Chosen-Plaintext Attacks

Assuming that the attacker, Eve, has access to the encryption machine, it can construct a ciphertext corresponding to any plaintext. Because the wireless channel has the characteristics of instantaneity and uniqueness, the encryption sequence $(D_x, D_y, D_z, D_w)$, generated according to the wireless channel, is completely dynamic. That is, the IFFT matrix and the FFT matrix controlled by $D_x, D_y, D_z, D_w$ are also completely dynamic. The input OTFS symbols are encrypted into dynamic ciphertext through the IFFT matrix and the FFT matrix. The eavesdropper, Eve, must have real-time channel state information between the legitimate users, Alice and Bob, in order to process the fully dynamic ciphertext. However, Eve cannot know the channel state information between Alice and Bob, so the chosen-plaintext attack is invalid. In other words, the transmission mechanism we propose is sufficient to resist selective plaintext attacks.

5.3. Statistical Attacks

A statistical attack refers to the method by which the attacker, Eve, deciphers the password according to the statistical law of plaintext, ciphertext, and key. Being able to resist statistical analysis has become a basic requirement of modern cryptography. In practical applications, due to the number of encrypted OTFS symbols, the illegal eavesdropper, Eve, cannot launch statistical attacks through statistical changes in OTFS symbols. Therefore, the transmission mechanism we propose is sufficient to resist statistical attacks.

6. Simulation Results Discussion

In this section, we use MATLAB software for the performance simulation. To prove the overall performance of the entire system, under the mechanism of our proposed transmission scheme, we perform PAPR and Bit-Error Ratio (BER) simulations, as well as independence tests, at the same time. In this section, the simulation sets the carrier spacing to $\Delta f = 15$ kHz and the carrier frequency to $f_c = 35$ GHz, and the channel fading follows the Rayleigh variables’ distribution. The number of propagation paths is two, and a 16-QAM symbol modulation is used.
6.1. Independence Performance

The independence is the bit difference between the encrypted and original OTFS symbols. In order to ensure a secure OTFS encryption technique, it should be close to 50% [4]. It is assumed that QPSK modulation and 256QAM modulation are adopted, respectively. The vertical axis of the graph represents the percentage of the bit change between the encrypted and original OTFS symbols. It can be seen from Figure 8 that when QPSK modulation is used, the ordinate is close to 50%. When 256QAM modulation is used, the percentage of the bit change decreases slightly but remains around 40%. These results demonstrate that our scheme ensures a good cryptographic performance in terms of the difference properties. Therefore, our scheme can ensure the underlying security of the OTFS transmission.

![Figure 8. Independence test results.](image)

6.2. PAPR Performance

As shown in Figure 9, traditional OFDM symbols will cause a high PAPR, thereby reducing the system transmission performance. Although the conventional OTFS symbol reduces the PAPR to a certain extent, the PAPR of the transmission system is still very high. The proposed improved selective mapping algorithm can significantly reduce the PAPR of OTFS symbols with lower complexity. It can be seen from the figure that when the Complementary Cumulative Distribution Function (CCDF) is $10^{-3}$, compared with the traditional OFDM system, our proposed scheme can obtain a 2.5-dB PAPR reduction; compared with the conventional OTFS system, our proposed scheme can obtain a 1.0-dB PAPR reduction.

![Figure 9. CCDF of PAPR for different schemes.](image)
6.3. BER Performance

As shown in Figure 10, compared with the conventional OTFS system, our proposed transmission mechanism will not reduce the bit-error rate of the legal receiver, Bob. Compared with the traditional OFDM system, under the same signal-to-noise ratio, the proposed transmission mechanism can significantly increase the bit-error rate difference between Bob and Eve. With the increase in the signal-to-noise ratio, the more obvious the bit-error rate difference becomes, and the more obvious the superiority of our proposed transmission mechanism becomes.

As shown in Figure 11, because the illegal eavesdropper, Eve, cannot extract the channel information between Alice and Bob, it cannot extract the correct secret key and thus cannot crack the matrix replacement process and cannot perform correct demodulation, so the bit-error rate is close to 0.5. However, due to the reciprocity of the channel, the legitimate receiver, Bob, can extract the correct secret key and demodulate correctly, so the transmission mechanism we propose will not affect Bob’s bit-error rate. For the traditional OTFS system, since the eavesdropper, Eve, knows the modulation matrix, the bit-error rate is much lower than 0.5 through correct demodulation. In the scheme using the chaotic algorithm as the key generation algorithm, there is only one source of the initial value, so the key is not sensitive enough to the channel change; though the bit-error rate is still high, it is less than 0.5. To sum up, our proposed transport mechanism has superior security performance.

Figure 10. BER for different schemes.

Figure 11. BER for legal receiver and illegal eavesdropper.
7. Conclusions

In this paper, we have proposed a 2D permutation-aided OTFS secure transmission scheme that uses the GOST algorithm to perform disturbance control on the OTFS modulation domain. Furthermore, we have proposed an improved SLM algorithm, which can significantly improve the PAPR problem with very low complexity. We have carried out a comprehensive security analysis and simulation evaluation. Our results have shown that the transmission scheme can obtain a promising independence performance, ensuring the underlying security property of the OTFS. Furthermore, compared to the OFDM scheme, our proposed scheme can reduce the PAPR by 20% and significantly improve the BER. To facilitate practical implementation, future studies may consider the design of the OTFS secure scheme in non-reciprocal channel scenarios.

Author Contributions: Conceptualization, J.S. and X.L.; methodology, W.L.; validation, J.S., W.L. and J.H.; investigation, L.L.; writing—original draft preparation, W.L.; writing—review and editing, W.L.; funding acquisition, J.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation of China under Grant 61901327, Grant 61941105, Gants 62101450, in part by the National Natural Science Foundation for Distinguished Young Scholar 61825104, in part by the Fundamental Research Funds for the Central Universities under Grant JB210109, in part by the Shenzhen Science and Technology program under Grant JCYJ20210324121006017, in part by the Foundation of State Key Laboratory of Integrated Services Networks of Xidian University under Grant ISN22-03.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Khiaadani, N. Vision, Requirements and Challenges of Sixth Generation (6G) Networks. In Proceedings of the 2020 6th Iranian Conference on Signal Processing and Intelligent Systems (ICSPIS), Mashhad, Iran, 23–24 December 2020; pp. 1–4. [CrossRef]

2. Zong, B.; Duan, X.; Fan, C.; Guan, K. 6G Technologies—Opportunities and Challenges. In Proceedings of the 2020 IEEE International Conference on Integrated Circuits, Technologies and Applications (ICTA), Nanjing, China, 23–25 November 2020; pp. 171–173. [CrossRef]

3. Chen, S.; Sun, S.; Kang, S. System integration of terrestrial mobile communication and satellite communication—The trends, challenges and key technologies in B5G and 6G. China Commun. 2020, 17, 156–171. [CrossRef]

4. Melki, R.; Noura, H.N.; Mansour, M.M.; Chehab, A. An Efficient OFDM-Based Encryption Scheme Using a Dynamic Key Approach. IEEE Internet Things J. 2019, 6, 361–378. [CrossRef]

5. Liang, Y.; Li, L.; Fan, P.; Guan, Y. Doppler Resilient Orthogonal Time-Frequency Space (OTFS) Systems Based on Index Modulation. In Proceedings of the 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 25–28 May 2020; pp. 1–5. [CrossRef]

6. Vahidi, V.; Saberinia, E. OFDM high speed train communication systems in 5G cellular networks. In Proceedings of the 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 12–15 January 2018; pp. 1–6. [CrossRef]

7. Naveen, C.; Sudha, V. Peak-to-Average Power Ratio reduction in OTFS modulation using companding technique. In Proceedings of the 2020 5th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, 5–6 March 2020; pp. 140–143. [CrossRef]

8. Surabhi, G.D.; Augustine, R.M.; Chockalingam, A. Peak-to-Average Power Ratio of OTFS Modulation. IEEE Commun. Lett. 2019, 23, 999–1002. [CrossRef]

9. Gao, S.; Zheng, J. Peak-to-Average Power Ratio Reduction in Pilot-Embedded OTFS Modulation Through Iterative Clipping and Filtering. IEEE Commun. Lett. 2020, 24, 2055–2059. [CrossRef]

10. Rasheed, O.K.; Surabhi, G.D.; Chockalingam, A. Sparse Delay-Doppler Channel Estimation in Rapidly Time-Varying Channels for Multiuser OTFS on the Uplink. In Proceedings of the 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 25–28 May 2020; pp. 1–5. [CrossRef]

11. Ramachandran, M.K.; Chockalingam, A. MIMO-OTFS in High-Doppler Fading Channels: Signal Detection and Channel Estimation. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 206–212. [CrossRef]
12. Raviteja, P.; Phan, K.T.; Hong, Y. Embedded Pilot-Aided Channel Estimation for OTFS in Delay–Doppler Channels. IEEE Trans. Veh. Technol. 2019, 68, 4906–4917. [CrossRef]

13. Hu, J.; Shi, J.; Ma, S.; Li, Z. Secrecy Analysis for Orthogonal Time Frequency Space Scheme Based Uplink LEO Satellite Communication. IEEE Wirel. Commun. Lett. 2021, 10, 1623–1627. [CrossRef]

14. Tie, Z.; Shi, J.; Li, Z.; Li, S.; Liang, W. Security Performance Analysis for An OTFS-based Joint Unicast-Multicast Streaming System. IEEE Trans. Commun. 2022. [CrossRef]

15. Lashkari, A.H.; Mansoor, M.; Danesh, A.S. Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA). In Proceedings of the 2009 International Conference on Signal Processing Systems, Singapore, 15–17 May 2009; pp. 445–449. [CrossRef]

16. Hole, K.J.; Dyrnes, E.; Thorsheim, P. Securing Wi-Fi networks. Computer 2005, 38, 28–34. [CrossRef]

17. Hu, X.; Yang, X.; Shen, Z.; He, H.; Hu, W.; Bai, C. Chaos-Based Partial Transmit Sequence Technique for Physical Layer Security in OFDM-PON. IEEE Photonics Technol. Lett. 2015, 27, 2429–2432. [CrossRef]

18. Liu, Y.; Draper, S.C.; Sayeed, A.M. Exploiting Channel Diversity in Secret Key Generation From Multipath Fading Randomness. IEEE Trans. Inf. Forensics Secur. 2012, 7, 1484–1497. [CrossRef]

19. Aono, T.; Higuchi, K.; Taromaru, M.; Ohira, T.; Sasaoka, H. Wireless secret key generation exploiting the reactance-domain scalar response of multipath fading channels: RSSI interleaving scheme. In Proceedings of the European Conference on Wireless Technology, Paris, France, 3–4 October 2005; pp. 173–176. [CrossRef]

20. Ren, K.; Su, H.; Wang, Q. Secret key generation exploiting channel characteristics in wireless communications. IEEE Wireless Commun. 2011, 18, 6–12. [CrossRef]

21. Bloch, M.; Barros, J.; Rodrigues, M.R.D.; McLaughlin, S.W. Wireless Information-Theoretic Security. IEEE Trans. Inf. Theory 2008, 54, 2515–2534. [CrossRef]

22. Zeng, K. Physical layer key generation in wireless networks: Challenges and opportunities. IEEE Commun. Mag. 2015, 53, 33–39. [CrossRef]

23. Wei, Y.; Zeng, K.; Mohapatra, P. Adaptive Wireless Channel Probing for Shared Key Generation Based on PID Controller. IEEE Trans. Mob. Comput. 2013, 12, 1842–1852. [CrossRef]

24. Liu, J.; Ren, A.; Sun, R.; Du, X.; Guizani, M. A Novel Chaos-Based Physical Layer Security Transmission Scheme for Internet of Things. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6. [CrossRef]

25. Wang, C.-L.; Ouyang, Y. Low-complexity selected mapping schemes for peak-to-average power ratio reduction in OFDM systems. IEEE Trans. Signal Process. 2005, 53, 4652–4660. [CrossRef]

26. Holmes, P. Chaotic Dynamics. IEEE Power Eng. Rev. 1985, PER-5, 6–8. [CrossRef]

27. Lempel, A.; Ziv, J. On the Complexity of Finite Sequences. IEEE Trans. Inf. Theory 1976, 22, 75–81. [CrossRef]