# Ultra-large Key Space Multi-dimensional Masking Encryption System for DSM-based D-band Wireless Fronthaul

**Tianqi Zheng[1], Kaihui Wang[1], Xiongwei Yang[1], Qiutong Zhang[1], Weiping Li[1], Yi Wei[1], Feng Wang[1], Xianming Zhao[2], Feng Zhao[3], and Jianjun Yu[1*]**

[1] *Fudan University, Shanghai, 200433, China * jianjun@fudan.edu.cn*

[2]. *The Institute of Future Information Technology, Harbin Institute of Technology, Harbin 150001, China*

[3]. *School of Automation Xi'an University of Posts and Telecommunications, Xi'an 710121, China*

**Abstract:** We implement a multi-dimensional masking encryption scheme with an ultra-large key space of $10^{143}$ in a photonics-aided millimeter radio-over-fiber (ROF) system. The equivalent 1.67GBaud encrypted-4096QAM signal is successfully transmitted and decrypted over a 4.6-km wireless link in the DSM-based D-band wireless fronthaul system. © 2024 The Author(s)

## 1. Introduction

Nowadays, the communication system combined with optical, electrical, and wireless hybrid links is increasingly advanced and complex, it is necessary to encrypt the physical layer to prevent eavesdropping at any link in the complex system [1]. Chaotic encryption systems have great appeal in physical layer encryption [2]. Due to their excellent unpredictability, initial sensitivity and non-periodic, chaotic encryption systems could be hard to crack with huge key space. Compared with the traditional multi-level and multi-round mathematical function operations on plaintext and keys, the chaotic encryption generation structure is simple and has more unique characteristics that can be applied to physical layer encryption in a variety of ways. Masking the chaotic signal on the orthogonal signal constellation diagram, or using the complete randomness of the chaotic sequence to perform mathematical function operations. There's already much research about employing chaotic encryption in OFDM-PON [3]. Besides this, as the mm-wave experimental verification distance increases to several kilometers, even though mm-wave transmission can achieve a minimal beam width [4], the radiation radius of its signal will exceed hundreds of meters under several kilometers' transmission [5], this greatly increases the possibility of eavesdropping. Therefore, applying and enriching physical layer encryption methods in the fiber-wireless integrated system becomes extremely necessary.

This paper proposes a multi-dimensional chaotic encryption system that combines deoxyribonucleic acid (DNA) encryption and chaotic encryption employing an orthogonal delta-sigma modulator. The encryption system simultaneously masks the signal time domain constellation diagram and the delta-sigma modulation (DSM) spectrum, realizing a time-frequency domain multi-dimensional masking encryption method. In addition, due to the introduction of digital quantization, the amplitude of the chaotic signal as a mask can be increased so that the signal cannot be forcibly attacked by blind separation communication technologies such as CMA, DDLMS, and ICA. After combining chaotic masking encryption and DNA encryption, the encryption system has an extremely large key space. Finally, we experimentally realized an equivalent of 1.67GBaud 4096QAM transmitted in the multi-dimensional making encryption system with a key space of $2.25 \times 10^{134}$.

## 2. Operation principle

Fig. 1 illustrates our proposed multi-dimensional masking encryption system. First, a third-order jerk chaos system is used to generate a chaotic signal with three varies $\{x, y, z\}$. The $x$ and $y$ are used to mask the real and imaginary parts of the modulated signal in the time domain respectively. The dimensionless state equation of the third-order jerk system is shown in Eq. 1.

$$\begin{cases} \dfrac{dx}{dt} = y - F_N(y), \dfrac{dy}{dt} = z - F_L(z) \\ \dfrac{dz}{dt} = a\left(-x - y - z + F_M(x) + F_N(y) + F_L(z)\right) \end{cases} \tag{1}$$

Where $x$, $y$, and $z$ are three state variables, $a$ is a constant system parameter that usually takes values in the subspace of 0 to 1. In addition, $F_M$, $F_N$, and $F_L$ are three M, N, and L-order nonlinear step equations respectively which can be expressed as $F_V(x) = \xi\left[\sum_{m=-V}^{V} \mathrm{sgn}(x - 2\xi v)\right], V = \{M, N, L\} \in \mathbb{Z}$. Proper selection of $M$, $N$, $L$, and the coefficients $\xi$ and $\alpha$ will produce different types of chaotic signals. The $\{x, y\}$ phase diagram of the generated chaotic

signal and the masked 4096QAM are shown in Fig. 1(a) and (b). $Amp_x$ and $Amp_y$ are used to control the power ratio between the chaotic signal compared to the modulated signal. In past literature [6], the power of the masking signal is often very small to ensure that the signal can be successfully restored at the receiving end, and this would create a defect that the masked signal possibly be violently cracked by blind separation algorithms like CMA, DDLMS, and ICA successfully. For the first time, we introduced delta-sigma modulation to ensure the fidelity of the signal through digital quantization, and the relative output power of the chaotic signal could be greatly increased equal to the signal power. An orthogonal delta-sigma modulator is performed on the masked signal and generates two sets of orthogonal 1-bit DSM signals. Since each orthogonal component contains only one bit of logical information, it is very suitable for performing digital encryption. DNA digital chaotic encryption works after DSM, which masks the spectrum characteristics of DSM, greatly expanding the key space and encryption form of the chaotic encryption system. DNA encryption "encodes", "operates" and "reverse-encodes" information in a biologically imitated way [7]. First, every 2 bits are mapped into the symbol represented by nucleotides {A, T, C, G}, and then a reversible logical operation is performed with the Key series and nucleotide symbol. Finally, the symbol after operation is reversely decoded back to the 1-bit form using another mapping rule. The "encodes", "operates" and "reverse-encodes" and the selection of key series for operation are all controlled by the key. The key is generated in three sets of one-dimensional Logistic chaotic sequences. Two independent keys for encoding and inverse encoding are given by $K_c = \mathrm{mod}\left(Extract(x(i), jth), 3\right)+1$, and the key to the "operation" is given by $K_{oper} = \mathrm{mod}\left(x(i)\cdot 10^{15}, 8\right)+1$. Meantime, chaotic system output $f(z) = \mathrm{mod}\left(round\left(extract(z\cdot 2^{j})\right), 2\right)$ as key series participating in "operation".

After DNA encryption, the system outputs two columns of logical signals, which become QPSK-like signals after orthogonal combination and normalization. At this time, the QPSK-like signal output by the encrypted DSM can no longer see the spectral characteristics of DSM, as shown in Fig. 1(d). In order to prevent DSM error propagation, FEC coding is placed at the end of the encryption system to obtain optimal system efficiency. Eventually, the time domain and frequency domain of the signal are simultaneously masked by the encryption system, and the information is fully confused and dispersed.

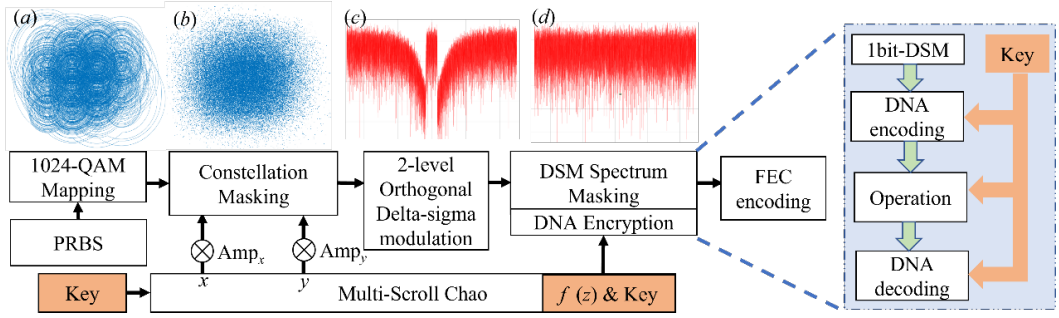


Fig. 1. Structure of the proposed encryption system. (a) x-y phase diagram of the chaotic series, (b) encrypted 4096 by time domain chaotic masking, (c)Spectrum of the DSM output, (d)Spectrum of the encrypted DSM-4096QAM.

## 3. Experimental setup and results

The system for photon-assisted terahertz wireless transmission to verify the proposed multi-dimensional encryption scheme is illustrated in Fig. 2. At the transmitter, the encrypted 1-bit DSM-4096QAM/1024QAM is generated by the proposed encryption system. The oversampling rate (OSR) of the DSM is 8, and the power ratio (PR) of the transmitted signal to the chaotic signal is 5. The frequency of photogenerated millimeter waves is about 125GHz. At the receiver, the received QPSK-like signal is equalized and decoded. The BER performance is enhanced as the input power of the UTC-PD increases. It can be seen from Fig.3(a) that the optimal PD power point is about 2dBm. We transmitted 25GBaud, and 20GBaud encrypted signals respectively. When the QPSK-like signal is at 25GBaud and the received optical power (ROP) of the UTC-PD is above -1dBm, all signals meet the SD-FEC threshold of 7% redundancy. And can be accurately restored in subsequent decryption. Coherent equalization algorithms include down conversion, resampling, T/2 CMA, FFT-based FOE, ML-BPS-based CPE, and DDLMS. Fig.3(I) illustrates the QPSK-like signal recovered by coherent equalization. After recovering the encrypted QPSK-like signal, the keys shared between the transceiver are to decrypt and recover the original 1024QAM/4096QAM, as shown in Fig.3(b), the decrypted 4096QAM and 1024QAM signals respectively satisfy $2.4\times10^{-2}$ SD-FEC threshold with 20% overhead and $3.8\times10^{-3}$ HD-FEC with 7% overhead, the final recovered constellation diagram is depicted in Fig.3(II) and Fig.3(III).

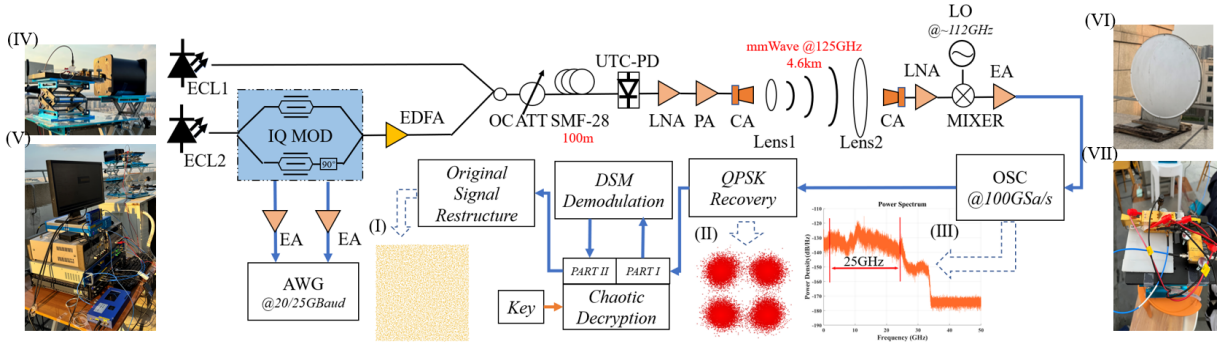


Fig. 2 Experimental setup of photonics-based millimeter wave wireless transmission system, (I) restructured 4096 QAM, (II) the recovered QPSK-like signal, (III) the Spectrum of the receiving signal. The picture of (IV) the wireless transmitting unit, (V) the transmitter, (VI) Lens2, and (VII) the wireless receiving unit.

The BER performance of the signals with correct decryption, wrong decryption, and brute force attack is depicted in Fig.3(c) while ROP is 2dBm. In the figure, the power ratio (PR) represents the relative normalized power of the modulated signal to the chaotic signal. When the chaotic signal power gradually increases, the BER of the signal after brute force cracking gradually increases. Fig.3(IV) illustrates the signal after blind cracking by CMA, DDLMS, and ICA. Benefiting from the DSM technology, even when the normalized powers of the chaotic masking signal and the modulated signal are equal, there is only minimal performance loss.

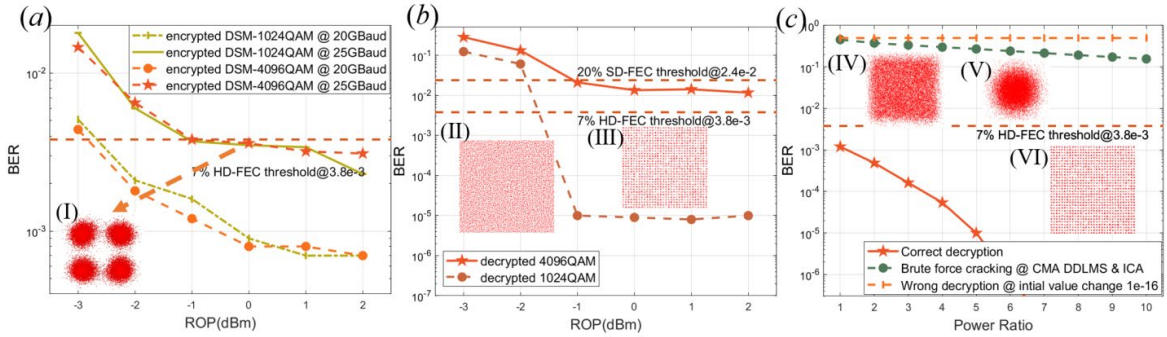


Fig. 3(a) BER performance of Encrypted QPSK-like DSM-high order QAM and (b) Decrypted 4096QAM/1024QAM (c) Performance of different power ratio of the chaotic masking signal (I)recovered QPSK-like signal (II) Scatterplot of decrypted 4096QAM (III) and 1024QAM (IV) Cracking by CMA, DDLMS, and ICA (V) Decrypted by wrong key with a $10^{-16}$ error. (VI) Correct decrypted signal

Besides, even under a small initial perturbation of $1\times10^{-16}$, as shown in Fig. 3(V), the signal is still completely unable to be decrypted. Only with the correct key, the encrypted signals can be correctly recovered. Fig.3(VI) illustrates the recovered 1024QAM after correct decryption while the PR=5. Above all, in a double-precision number system, the key space of our proposed multidimensional masking encryption system is up to $(10^{16})^3\times(10^{16})^4 \times 0.45 \times 10^{16} \times 0.5 \times 10^{16}=2.25 \times 10^{143}$, which is much larger than the conventional chaotic encryption scheme.

## 4. Conclusions

In this paper, an improved physical layer multi-dimensional masking encryption scheme based on DSM, multi-scroll chaotic, and DNA encryption system is implemented to enhance the security of physical layer communication, this system overcomes the limitations of chaotic signal power and significantly expands the key space. Eventually, we experimentally demonstrated the encrypted 4096QAM signal successfully transmitted over a 100m SMF-28 and 4.6 km wireless link at 125 GHz. The experiment results indicate that the proposed encryption system can successfully protect against eavesdroppers for the DSM-based D-band wireless fronthaul, which can resist brute force cracking and has an ultra-large key space of $10^{143}$. *This work was supported by the National Natural Science Foundation of China (No. 62305067, No. 61935005, and No. 61835002, No. 62375219, No. 62331004).*

## 5. References

[1] F. Wang, et al., OFC 2022, M3C.4.
[2] K. Yamauchi, et al., OECC 2020.
[3] X. Liang, et al., J. Lightwave Technol., 2023,41(6): 1619-1625.
[4] W. Zhou, et al., OFC 2023, W2B.25.
[5] W. Li et al., IEEE T MICROW THEORY.
[6] B. Zhu, et al., IEEE PHOTONIC TECH L., 2021, 33(8): 383-386.
[7] C. Zhang, et al., J. Lightwave Technol.,2018, 36(19): 1706-1712.