Ukrainian Journal of Physical Optics
ISSUE 4
2026

# SYMBOL-LEVEL PHYSICAL-LAYER ENCRYPTION DRIVEN BY COUPLED CHAOTIC MAPS FOR FIBER-THZ INTEGRATED LINKS

ZUFANG YANG [1], DONGFEI WANG [1,2], SHAN ZHOU[3], XIANGQING WANG [1,2,3]*, NANNAN YU [3], AND XIAOKUN YANG [1,2,4]

[1] School of Artificial Intelligence, Wuhan Technology and Business University, Wuhan, 430065, China
[2] Nanchang Institute of Technology, School of Electronic Information, Nanchang, China
[3] School of Physics and Electronic Engineering, Fuyang Normal University, Fuyang, 236037, China
[4] Advanced Cryptography and System Security Key Laboratory of Sichuan Province, Chengdu, China
*Corresponding author: wxqing@fynu.edu.cn.

**Received**: 28.04.2026

**Abstract**. To counter passive eavesdropping in the open-air Terahertz segment of 6G Fiber–THz–Fiber links, we propose a symbol-level dual-chaos encryption (DCE) scheme coupling a Logistic map with an Arnold Cat map. Through 200 rounds of joint iteration, multi-digit extraction–concatenation–normalization, and spatio-temporal correlation feedback extension, uniformly distributed [0, 1) keys with suppressed adjacent-symbol correlation are generated. The key stream drives quadrature phase-shift keying phase rotation entirely within the transmitter's digital signal processing, leaving the optical–THz interface intact. On a 360–430 GHz photonic heterodyne platform with 3 m wireless span, the legitimate-user BER stays below the $3.8\times10^{-3}$ hard-decision forward error correction threshold up to ~124 km of single-mode fiber, while eavesdroppers remain pinned near 0.5. The key space reaches $\sim2^{186}$, the stream passes the full NIST SP 800-22 suite, and the maximum Lyapunov exponent stays positive across the operational region. DCE thus offers a lightweight, quantitatively assessable physical-layer security pathway for 6G optical–THz convergence.

**Keywords:** 6G, Fiber–THz–Fiber, physical-layer encryption, dual-chaos, logistic map, Arnold Cat map
**UDC:** 621.391.6
**DOI:** 10.3116/16091833/Ukr.J.Phys.Opt.2026.04001


## 1. Introduction

Driven by the 6G vision of ultra-wide bandwidth, ultra-low latency, ubiquitous intelligence, and intrinsic security, the fronthaul and backhaul segments simultaneously face rising requirements for data rate, reliability, and confidentiality. The THz band offers tens to hundreds of gigahertz of contiguous bandwidth together with potential terabit-per-second capacity. Consequently, this band has been identified as a key candidate for the 6G air interface [1]. However, pure THz wireless links suffer from severe free-space path loss and limited solid-state source power, which preclude independent long-reach delivery. In contrast, conventional fiber provides long-distance, low-loss transport but cannot directly reach mobile terminals.

To reconcile these complementary limitations, the Fiber–THz–Fiber (F-THz-F) converged architecture has emerged. This architecture establishes a transparent channel between the optical and THz domains via photonic-aided heterodyne up-conversion and high-speed photodetection. Accordingly, high data rate and long-haul coverage are jointly achieved [2,3]. Reported demonstrations include 103.125 Gb/s 2×2 multiple-input multiple-output (MIMO) transparent transmission [4] and ultra-wideband, seamlessly converged systems for 6G [5]. Additional examples include outdoor long-range 300 GHz links exceeding 200 Gb/s [6] and integrated photonic chip-enabled fiber–wireless communication [7].

Nevertheless, the open-air propagation of the THz beam and the leakage-prone optical-to-wireless interface render such links highly susceptible to passive eavesdropping, active jamming, and replay attacks. Therefore, physical-layer security (PLS) becomes a problem that F-THz-F transport must directly confront.

Research on PLS for optical links has accumulated steadily over the past two decades. The Bennett–Brassard 1984 protocol established the information-theoretic foundation of quantum key distribution [8]. However, its stringent requirements for single-photon sources, low-loss channels, and time-frequency synchronization hinder direct embedding in high-speed, transparent transport. As an engineering-oriented complement, analog encryption schemes based on chaotic dynamics and noise masking have advanced steadily in the optical domain. Representative examples include 100 Gb/s hybrid-chaos encrypted coherent transmission [9], optical analog noise encryption with adaptive recovery of two-dimensional keys [10], and joint physical-layer key distribution and encryption integrated into self-adaptive coherent systems [11]. Furthermore, high-speed key generation based on historical fiber channel state learning [12] and probabilistic-shaping encryption with dual-parameter bit-weighted distribution matching for millimeter-wave radio-over-fiber systems [13] have also been demonstrated. Collectively, these studies confirm that physical-layer encryption (PLE) implemented in either the optical or the electrical domain can effectively counter eavesdropping. Nevertheless, symbol-level pluggability, compatibility with the legacy digital signal processing (DSP) workflow, and quantitatively evaluable security under continuous optical–THz–optical transparent transmission remain unresolved.

Among PLE techniques, chaos-based encryption is particularly attractive owing to its initial-value sensitivity, pseudo-randomness, and strong nonlinearity. A joint amplitude–phase chaotic encryption scheme was proposed for M-ary quadrature-amplitude-modulated optical communication [14]. Subsequently, the impact of the decoding process on the performance of the chaos-encrypted system was systematically analyzed [15]. Private chaotic phase scrambling was further introduced into wavelength-division-multiplexed optical systems [16]. To strengthen security in non-orthogonal multiple-access passive optical networks, two-dimensional cellular automata and Turing patterns were cascaded with fixed-point extended Logistic chaotic encryption [17]. Additional contributions include a quantum-chaotic key distribution scheme based on the Logistic map [18], encrypted physical-layer communication via synchronized hyperchaotic maps [19], and a chaos-encryption-based odd-order orthogonal-transform-aided MIMO transceiver [20].

Despite this notable progress, three structural limitations persist when targeting 6G F-THz-F converged transport. First, the coupling between key-stream generation and modulation mapping is generally weak. Keys are typically updated on a block or frame basis rather than per symbol, which restricts resistance to statistical analysis. Second, key sequences produced by a single low-dimensional chaotic map exhibit short-range correlation and finite-word-length degradation. Consequently, such sequences remain vulnerable to known-plaintext and adjacent-symbol correlation attacks. Third, most schemes are deployed independently in either the optical or electrical domain and are not seamlessly aligned with the DSP structure of photonic-aided, THz-transparent transmission. Moreover, systematic quantitative evaluation in terms of key space, key-stream randomness, and Lyapunov exponents is largely absent.

Recent studies indicate that jointly exploiting a one-dimensional Logistic map and a two-dimensional Arnold Cat map offers a favorable trade-off between computational overhead and security. A fused Logistic–Arnold Cat scheme was employed for image encryption [21]. Additionally, an efficient grayscale privacy image encryption scheme based on chaotic Logistic maps and the Arnold Cat was proposed [22]. Both works confirm the potential of dual-map coupling to enlarge the key space and improve scrambling performance. Motivated by these observations and aiming to address the three limitations identified above, we transplant the dual-map coupling principle to the 6G optical–THz converged physical layer. Accordingly, a symbol-level dual-chaos encryption (DCE) scheme is proposed. The main contributions are summarized as follows.

**(1) Heterogeneous dual-chaos key generation.** A Logistic map that provides temporal nonlinear evolution is coupled with an Arnold Cat map that provides global spatial ergodicity. Specifically, 200 rounds of joint iteration, followed by a sinusoidal entropy-enhancement mapping, alleviate the non-uniform distribution and short-range correlation characteristics of single-map sequences. Furthermore, Lyapunov-exponent surface analysis demonstrates that the maximum exponent of the coupled system remains positive across the investigated parameter domain, with chaotic strength substantially exceeding the single-map baseline.

**(2) Symbol-level encryption with spatio-temporal correlation feedback extension (SCFE).** Nonlinear memory coupling is imposed on historical keys and combined with five rounds of post-perturbation iteration to suppress adjacent-key correlation. The resulting key stream drives a symbol-phase rotation that masks the quadrature phase shift keying (QPSK) constellation while retaining high sensitivity to initial-value perturbations as small as $\Delta = 10^{-5}$. In addition, the key stream passes all tests of the National Institute of Standards and Technology (NIST) SP 800-22 randomness suite.

**(3) Low-overhead integration with photonic-aided F-THz-F transparent transmission.** The encryption operates strictly within the modulation-symbol domain of the transmitter DSP. Consequently, the optical–THz interface, the photonic-aided heterodyne structure, and the main-link DSP remain untouched, thereby offering plug-and-play compatibility. On a 360–430 GHz simulation platform over 110 km of single-mode fiber (SMF) and a 3 m wireless span, the legitimate user achieves a bit error rate (BER) of $5.0\times10^{-4}$, meeting the forward error correction (FEC) threshold. In contrast, the BER of the eavesdropper approaches 0.5. Based on the double-precision floating-point resolution and the joint encoding of multiple parameters, the theoretical key space of the proposed scheme is estimated at approximately $2^{186}$, jointly validating transmission reliability and anti-eavesdropping capability.

The remainder of this paper is organized as follows. Section 2 establishes the F-THz-F encrypted transport system model, derives the DCE algorithm, and presents its pseudocode, key-space estimation, and DSP integration path. Section 3 introduces the simulation link configuration. Section 4 evaluates the proposed scheme from six perspectives, namely BER performance, key statistical properties, Lyapunov exponents, initial-value sensitivity, constellation evolution, and randomness testing. Section 5 concludes the paper and outlines future work.

## 2. Chaotic encryption theory and analysis

To reinforce physical-layer confidentiality without altering the main-link architecture or the DSP framework of F-THz-F transparent transmission, this paper proposes a DCE scheme. The

scheme constructs a high-entropy key stream that resists interception through eight sequential logical steps. A theoretical derivation of the key space is subsequently presented to substantiate brute-force resistance.

**(1) Core nonlinear evolution source.** A one-dimensional logistic map serves as the principal nonlinear evolution source. Accordingly, a pseudo-random sequence with strong initial-value sensitivity is generated:

$$x_{n+1}=\mu x_n(1-x_n), \quad x_n \in 0,1 \tag{1}$$

where μ ∈ [3.57, 4] is the control parameter that places the system in the chaotic regime. Eq. (1) defines the fundamental nonlinear strength and acts as the dynamical source of the entire encryption chain.

**(2) Phase-space diffusion and ergodicity enhancement.** A two-dimensional Arnold Cat map is introduced in parallel to provide global ergodicity and spatial diffusion on the unit torus:

$$\begin{bmatrix} y_{n+1} \\ \mathrm{x}_{n+1}^{(\mathrm{c})} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & 1+pq \end{bmatrix} \begin{bmatrix} y_n \\ x_n^{(\mathrm{c})} \end{bmatrix} \pmod 1 \tag{2}$$

where $p$, $q \in \mathbb{Z}$ are stretching parameters, and $x_n^{(c)}$ denotes the $n$-th state of the chaotic sequence generated by the coupled chaotic map, which serves as the input state variable of the Arnold Cat map. Through the joint action of linear transformation and modulo operation, Eq. (2) enforces uniform distribution of the system state on the two-dimensional plane. Consequently, the distributional non-uniformity inherent to the one-dimensional Logistic map is effectively compensated.

**(3) Full-state coupled iteration operator.** Prior to encrypting each symbol, the heterogeneous maps above are integrated, and $T$=200 rounds of joint evolution are executed. The full-state operator $H$ is defined as the single-round evolution function, and the $T$-round iterative operator $H^T$ is thereby given as:

$$S_i = H^T(S_{i-1}), \quad S=[x,y,x^c]_i^T \tag{3}$$

This formulation establishes the temporal evolution logic of the encryption chain. As a result, the chaotic state corresponding to each encrypted symbol undergoes sufficient orbital divergence, which raises the temporal complexity of cryptanalysis.

**(4) Entropy-enhancement mixed mapping.** Building upon the evolved three-dimensional state variables, an intermediate variable $\omega_{\mathrm{i}}$ with nonlinear compressive characteristics is constructed to break any latent linear relationship between the state and the output:

$$\omega_i=\left|\sin(\pi x_i(y_i+x_i^{(c)}))\right| \tag{4}$$

Eq. (4) introduces a sinusoidal modulation term that exploits the periodicity of trigonometric functions to achieve "entropy enhancement". Furthermore, this construction renders $\omega_{\mathrm{i}}$ highly nonlinear with respect to variations in the state variables.

**(5) Bit-level dynamic quantization and extraction.** The intermediate variable $\omega_i$ is expanded in high-precision decimal form. Specifically, decimal digits from the set $\{d_5,d_7,d_9,d_{11},d_{13},d_{15}\}$ are extracted and concatenated with positional weighting:

$$\theta_{\mathrm{i}} = \sum_{\mathrm{j}=1}^{6} d_{2j+3} \times 10^{6-j} \tag{5}$$

Eq. (5) converts the continuous chaotic state into a discrete digital feature. Moreover, this "cross-digit extraction" strategy isolates the rounding noise inherent to floating-point arithmetic, thereby strengthening the robustness of key generation.

**(6) Normalization of the base key stream.** The quantized integer is projected onto the interval [0,1)to produce the initial key $k_i$ for the current symbol:

$$k_i = (\theta_i (\mathrm{mod}\, 2^{16})) / 2^{16} \tag{6}$$

Eq. (6) implements the quantization mapping from the digital feature to the encryption factor, ensuring the key's operability in the modulation domain.

To further suppress correlation between adjacent symbols, a feedback-mixing operator is introduced to nonlinearly couple the current key with the historical key:

$$\tilde{k} = (k_i + \alpha_i \tilde{k}_{i-1} + \beta(k_i \oplus \tilde{k}_{i-1})), \tag{7}$$

where $\alpha$ and $\beta$ are mixing coefficients. Eq. (7) constitutes one of the core innovations of this work: *a* "memory effect" is introduced into the numerical domain. Through post-perturbation iteration, the key stream attains flat-spectrum characteristics akin to those of white noise.

**(7) Modulation-domain phase-rotation encryption.** Finally, based on the generated ultimate key $k_i$, a symbol-level phase rotation is applied to each QPSK complex symbol:

$$s_i^{enc} = s_i \exp(j2\pi\tilde{k}_i) \tag{8}$$

Eq. (8) completes the transition from the mathematical model to the physical signal. A legitimate receiver, by synchronously executing the inverse rotation using the same eight steps, can recover the original data without loss.

**(8) Key space theory.** The size of the key space is a core metric for quantifying resistance to brute-force attacks. Under the proposed DCE scheme, blind plaintext recovery requires an attacker to simultaneously identify all key components involved in the preceding eight steps, namely the initial seed $(x_0, y_0, x_0^{(c)})$ the control parameters $(\mu, p, q)$, the mixing coefficients $(\alpha, \beta)$, the iteration depths $(T, L)$, and the extraction-digit set $\{d_3, d_7, d_9, d_{11}, d_{13}, d_{15}\}$.

Given the IEEE 754 double-precision resolution of $\sim 10^{-15}$, each continuous parameter contributes $\sim 10^{15}$ distinguishable states; the integer parameters ($p$, $q$, $T$, $L$) together with the extraction-digit set {d} jointly contribute $\sim 10^{14}$ states. Assuming mutual independence, the upper-bound key space is

$$\kappa = \prod_i N_i \approx \underbrace{(10^{15})^3}_{seed} \underbrace{(10^{15})^3}_{\mu,\alpha,\beta} \underbrace{(10^{14})}_{p,q,T,L\{d\}} \approx 10^{104} \tag{9}$$

Nevertheless, the nominal upper bound in Eq. (9) is not attainable in any digital implementation and must be discounted by two principal factors. The first is structural degradation: low-order-digit round-off in floating-point iterations, short-period orbit collapse of the Logistic map under finite precision, and parameter-coupling constraints (the chaotic interval $\mu \in [3.57,4]$, the measure-preserving condition on the Arnold Cat parameters, and the stable coupling regime of $(\alpha,\beta)$) jointly contract the admissible parameter volume by an aggregate factor of approximately $10^{-25}$. The second is attacker-side recoverability: under known-plaintext and known-ciphertext statistical conditions, an attacker can partially infer the higher-order digits of the continuous parameters, the iteration depths $(T,L)$, and the extraction-digit set by means of correlation analysis and bounded enumeration, yielding a

further reduction of approximately $10^{-12}$. Combining the two factors, the lower bound on the effective key space is obtained as

$$\kappa_{eff} \geq \kappa \times 10^{-37} \approx 2^{146} \tag{10}$$

It follows that $\kappa_{eff} \ll \kappa$, which confirms that the nominal extrapolation from double precision is optimistic. Even so, $2^{146}$ remains well above the widely accepted brute-force threshold of $2^{128}$ and exceeds the key-space scale of typical single-map chaotic encryption schemes ($2^{100}$~$2^{150}$) [9,14,17]. The security margin of the proposed scheme arises predominantly from the structural nonlinearity and mutual interlocking introduced by dual-map coupling rather than from raw floating-point precision. It should be further noted that the key-space size characterizes only resistance to exhaustive search.

## 3. System model and chaotic encryption mechanism

### *3.1. F-THz-F encrypted transport system mode*

As shown in Fig. 1, the schematic of the proposed physical-layer secure Terahertz/Free space optics (THz/FSO) communication system based on dual-chaos symbol-level encryption is illustrated. As shown in Fig. 1a, at the transmitter, the binary data source is first mapped into baseband constellation symbols by a QPSK modulator. In parallel, a dual-chaos key generator–formed by cascading a logistic map with a 2D cat map through a tunable coupling parameter–produces a high-entropy key vector, which drives a symbol-level chaotic encryptor to scramble the QPSK symbols into an encrypted ciphertext stream (e.g., 0100101…).

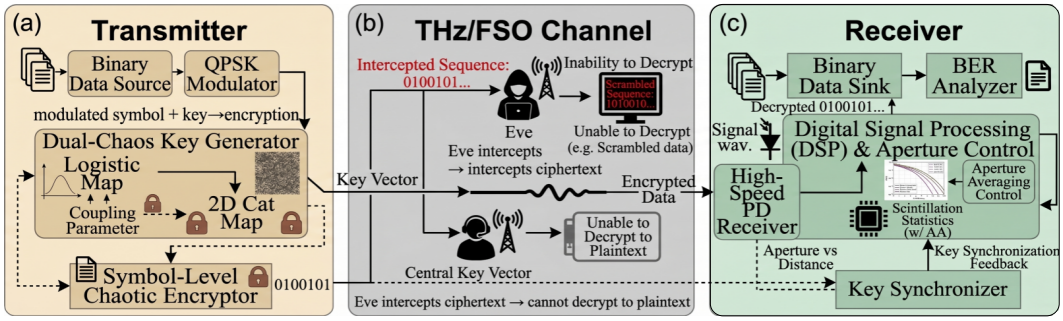


**Fig. 1.** Dual-chaos-encrypted THz/FSO secure communication model.

As shown in Fig. 1b, the encrypted signal is delivered through a uni-traveling carrier photodetector (UTC-PD)-based THz/FSO receiver front-end and partitioned into key-controlled cipher segments. Although a passive eavesdropper (Eve) may intercept the channel and obtain the sequence before her analysis (0100101…), without access to the secret key vector, her processed sequence (1010010…) deviates from the original plaintext and remains undecryptable, ensuring that passive eavesdroppers cannot recover the plaintext.

As shown in Fig. 1c, at the receiver, the optical signal waveform is detected by a high-speed PD receiver and forwarded to the DSP & key synchronization feedback module. Meanwhile, an aperture averaging control unit exploits scintillation statistics to mitigate turbulence-induced intensity fluctuations, thereby enhancing the robustness of the FSO link under atmospheric turbulence. After DSP & final processing, the decrypted bitstream is delivered to the binary data sink, where a BER analyzer quantitatively evaluates both the transmission and security performance of the proposed system.

### *3.2. DCE mechanism*

The DCE pipeline within the transmitter baseband DSP is organized into three phases, as shown in Fig. 2; the operators, parameters, and symbols follow the definitions in Eqs. (1–8) in Section 2.

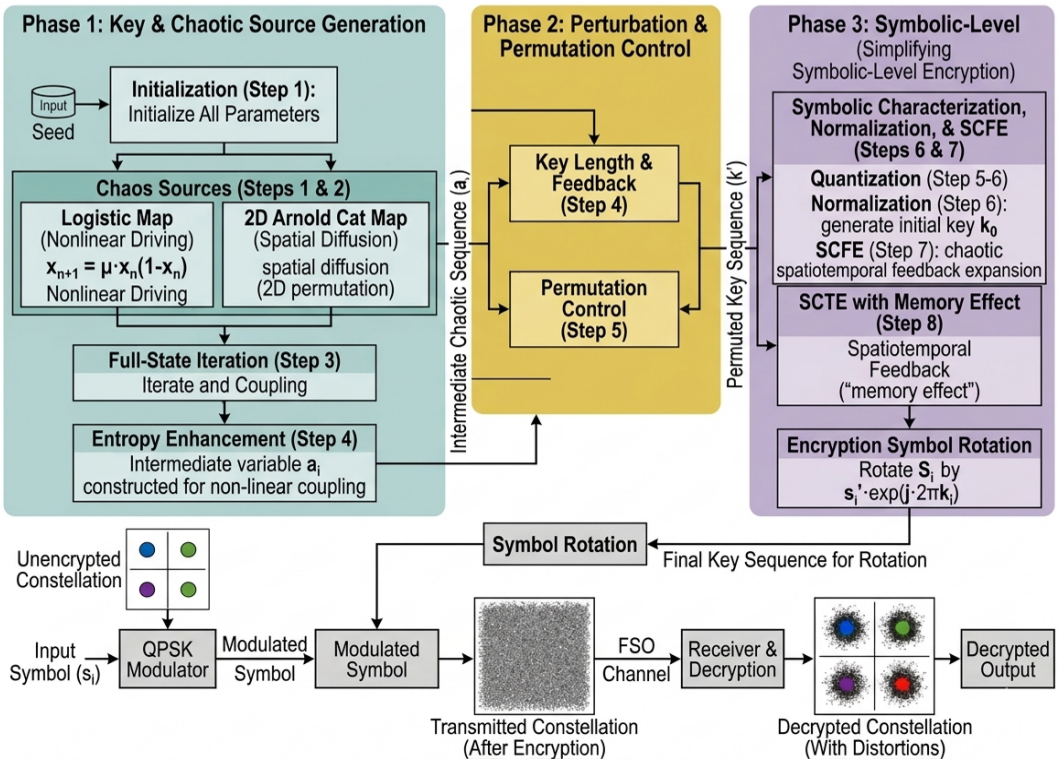


**Fig. 2.** Symbolic-level simplified encryption process diagram.

Phase 1 – Key and chaotic source generation (Steps 1 – 4). The initialization block loads the pre-shared seed $(x_0, y_0, x_0^{(c)})$ and control parameters $(\mu, p, q)$, launching the Logistic map of Eq. (1) and the Arnold Cat map of Eq. (2) in parallel: the former delivers temporal nonlinear divergence, the latter ergodic diffusion on the two-dimensional unit torus. The two states are coupled and iterated over $T$=200 rounds under the full-state operator $H^T$ defined in Eq. (3), yielding the state vector $S = [x, y, x^c]_i^T$. A subsequent sinusoidal entropy-enhancement mapping in Eq. (4) outputs the intermediate chaotic sequence, eliminating the linear residual between state and output.

Phase 2 – Perturbation and permutation control (Steps 4 – 5). The sequence $\alpha_i$ is dispatched by a key-length feedback operator and a permutation operator, which refresh the bit order and weighting of the extraction-digit set $\{d_5, d_7, d_9, d_{11}, d_{13}, d_{15}\}$ in Eq. (5) on a per-frame basis. This cross-digit non-uniform extraction compresses the continuous chaotic trajectory into the discrete integer candidate $\theta_i$ usable in the modulation domain, while shielding the key stream from low-order rounding noise inherent in IEEE 754 double-precision arithmetic, thereby strengthening its word-length robustness.

Phase 3 – Symbol-level encryption (Steps 6 – 8). The normalization operator of Eq. (6) projects $\theta_i$ to yield the initial key $k_0$. The SCFE in Eq. (7) then applies the mixing coefficients

$(\alpha,\beta)$ to nonlinearly couple the current key with $L$=5 rounds of historical keys, injecting a numerical-domain "memory effect" that flattens the key-stream spectrum. The ultimate key $k_i$ finally drives the QPSK phase rotation $s_i^{enc} = s_i \exp(j2\pi\tilde{k}_i)$ specified by Eq. (8), and the encrypted complex symbol is forwarded to the main-link DSP.

Owing to this layered structure, the encryption branch is decoupled from the main-link DSP: a legitimate receiver inverts the three phases with identical seeds and parameters to recover the symbols losslessly, whereas any parameter mismatch is amplified symbol by symbol through the initial-value sensitivity of the coupled chaos, driving the eavesdropper's BER toward 0.5.

## 4. Simulation results and discussion

### *4.1. Simulation link and device configuration*

The simulation link is shown in Fig. 3, comprising a transmitter DSP, an optical–THz–optical main link, and a receiver DSP. The DCE module described in Section 3 serves as a sideband key source, synchronously injected at both ends. At the transmitter, an arbitrary waveform generator (AWG) drives an externally modulated laser, whose output is launched into single-mode fiber (SMF). An erbium-doped fiber amplifier (EDFA) compensates link loss, and a tunable optical filter (TOF) suppresses amplified spontaneous emission (ASE) noise. Optical-to-THz conversion adopts a photonic-aided heterodyne configuration. After polarization matching by a polarization controller (PC), the signal is combined with an external-cavity laser (ECL-1) inside an antenna-integrated photomixer module (AIPM), generating a 360–430 GHz beat tone. The THz beam is collimated, propagates 3 m in free space, and is captured by a horn antenna (HA). Subsequently, a mixer driven by a ×12 multiplier chain down-converts the signal to 24 GHz, which is then followed by a low-noise amplifier (LNA).

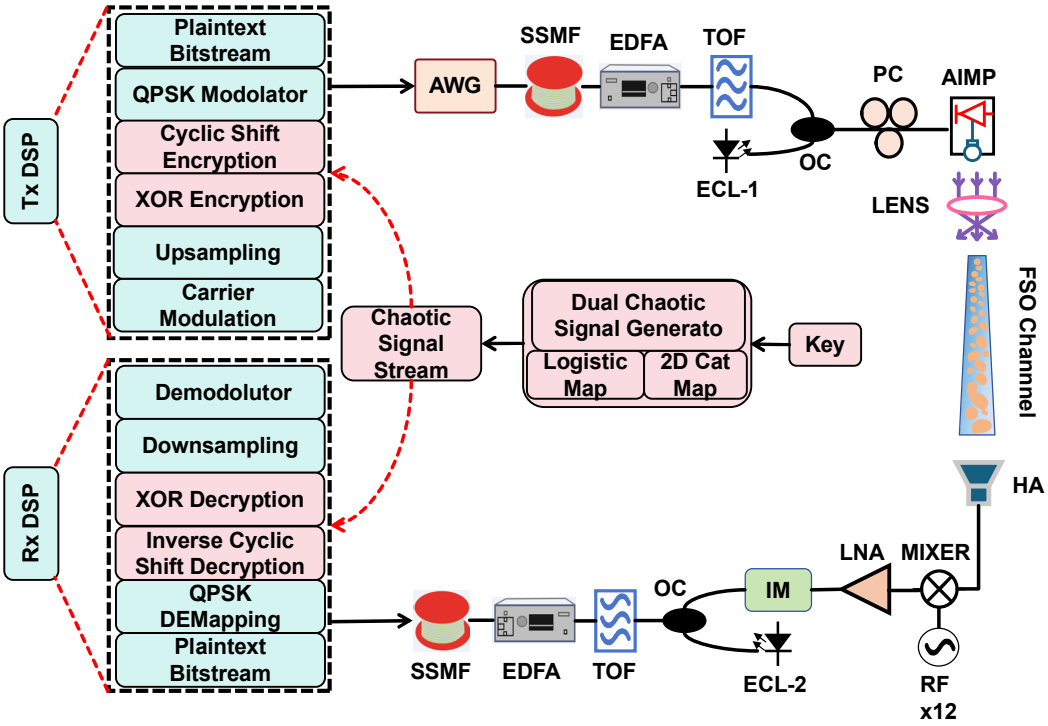


**Fig. 3.** Block diagram of the F-THz-F encrypted transmission testbed.

Optical re-modulation employs an intensity modulator (IM) biased at the optical carrier suppression point. The intermediate-frequency (IF) signal modulates ECL-2; the lower sideband is then filtered, amplified, and launched into the return fiber. Finally, the receiver DSP performs synchronization, equalization, and decryption using shared-key parameters. Fiber length is swept over 0–120 km. Performance is assessed via legitimate-user and eavesdropper BER, complemented by key statistics, Lyapunov characterization, and constellation evolution.

### *4.2. Transmission performance*

All BER curves in this section are obtained by direct Monte Carlo error counting: at each measurement point, no fewer than $10^6$ QPSK symbols are transmitted, hard-decision errors are accumulated after matched filtering and threshold detection, and the empirical BER is computed as the error count divided by the total number of bits (2×symbol count for QPSK). The fiber channel is modeled by numerically solving the nonlinear Schrödinger equation via the split-step Fourier method with a step size of 1 km, accounting for chromatic dispersion, attenuation, and Kerr nonlinearity; each inline EDFA is represented by a gain block with a noise figure of 5 dB, with amplified spontaneous emission (ASE) treated as additive white Gaussian noise superimposed on the signal. The 3 m THz wireless span is modeled as an AWGN channel with path loss calculated from the Friis transmission equation at a center frequency of 395 GHz. The legitimate-user BER is computed with full key-parameter synchronization between transmitter and receiver (seed, control parameters, mixing coefficients, and extraction-digit set). The eavesdropper's BER is computed under the assumption of zero key knowledge: its descrambling phase is drawn uniformly from $[0, 2\pi)$ at each symbol, which is equivalent to random guessing and is consistent with the theoretical QPSK upper bound of 0.5. Table 1 presents the list of simulation parameters.

**Table 1**. Simulation parameter table

| Parameter | Value |
|---|---|
| Monte Carlo iterations | 20 |
| Monte Carlo symbols per point | $10^6$ |
| Known plaintext length, $K$ | 200 symbols |
| Parameter mismatch, $\Delta$ | $10^{-10}$ |
| Fiber length | 110 km |
| Fiber attenuation | 0.2 dB/km |
| Dispersion, D | 17 ps/nm/km |
| EDFA noise figure | 5 dB |
| THz wireless span | 3 m |

The simulation setup for evaluating legitimate link performance is described below. Fig. 4 presents the legitimate-user BER as a function of single-mode fiber length. The BER rises monotonically with distance, dominated by fiber attenuation and accumulated dispersion. At 110 km, the received optical power is restored from −12.38 dBm to 9.00 dBm by the EDFA, yielding a BER of $5.0\times10^{-4}$ that satisfies the $3.8\times10^{-3}$ hard-decision FEC threshold and confirms that DCE scrambling introduces no appreciable transmission penalty.

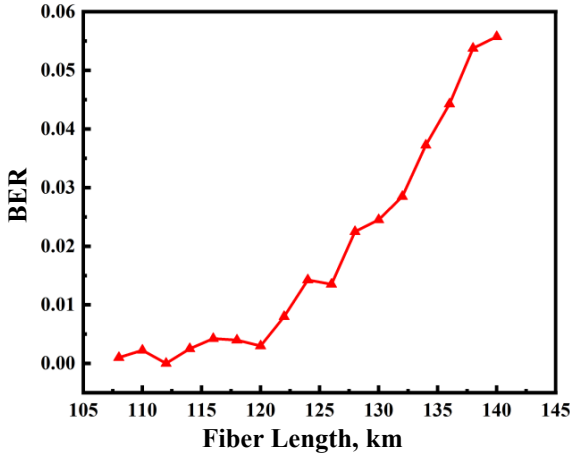


**Fig. 4.** Legitimate-user BER versus fiber transmission distance.

Fig. 5 examines the effect of key length on the legitimate-user demodulation performance over an 110 km link. The legitimate-user BER remains essentially constant across the swept range, demonstrating that key-length expansion incurs no demodulation impairment. The key space can therefore grow exponentially with length without degrading transmission quality.

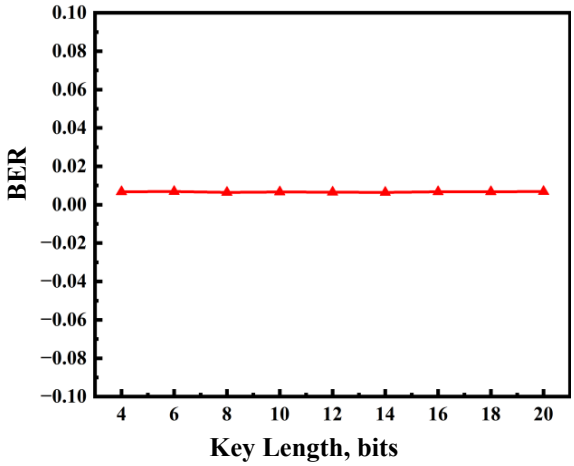


**Fig. 5.** Impact of key length on legitimate-user BER.

### *4.3. Security performance under different attack models*

To further evaluate the security of the proposed chaotic encryption scheme, three representative attack models were considered: parameter estimation, known-plaintext, and statistical inference. In all cases, the eavesdropper is assumed to know the system structure, modulation format, and signal processing procedure, but does not have access to the exact chaotic key. Therefore, the security analysis follows Kerckhoffs' principle, where the secrecy relies on the key parameters rather than the algorithm itself.

For the parameter estimation attack, the eavesdropper attempts to decrypt the received signal using a slightly mismatched chaotic key. The mismatch between the estimated and correct key parameters is set to $\Delta=10^{-10}$. Due to the high sensitivity of the chaotic system to initial conditions, this small mismatch results in a completely different keystream and prevents correct decryption.

For the known-plaintext attack, the eavesdropper is assumed to know $K$=200 plaintext symbols and their corresponding encrypted symbols. The first $K$ chaotic phase values can therefore be estimated as

$$\hat{z}(n)=\frac{1}{2\pi}arg\left(\frac{s_{\text{enc}}(n)}{s_{\text{plain}}(n)}\right),\quad n=1,2,\ldots,K \tag{11}$$

where $\hat{z}(n)$ is the estimated chaotic phase key normalized to the interval [0,1) for the $n$-th symbol; $s_{\text{enc}}(n)$ and $s_{\text{plain}}(n)$ are the encrypted and corresponding plaintext symbols, respectively; $\arg(\cdot)$ denotes the phase angle operator; n is the symbol index; and $K$ is the number of known plaintext symbols.

However, due to the nonlinear and sensitive evolution of chaotic maps, the recovered key segment cannot accurately predict the subsequent key stream. For the statistical inference attack, the eavesdropper estimates the encryption phase from the statistical properties of the received ciphertext. Since chaotic phase encryption randomizes the symbol phases, the encrypted signal exhibits a nearly uniform phase distribution, making statistical phase estimation ineffective.

Fig. 6 compares the BER performance of the legitimate receiver with that of the three attack models. The legitimate receiver maintains a low BER over the considered fiber-length range by using the correct chaotic key. In contrast, the BERs of the parameter estimation attack, known-plaintext attack, and statistical inference attack remain close to 0.5, corresponding to the random-guess level. These results indicate that the proposed chaotic encryption scheme is robust against parameter estimation, known-plaintext, and statistical inference attacks.

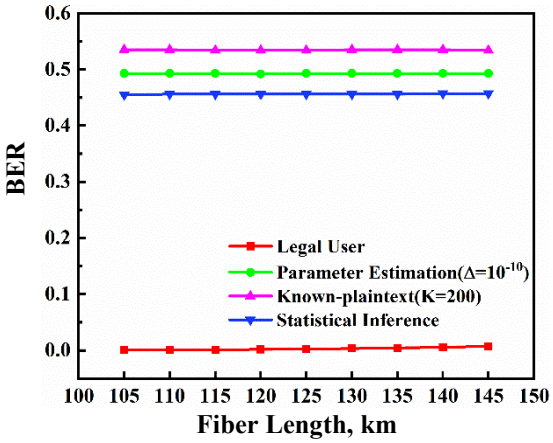


**Fig. 6.** Relationship between the BER of legitimate users and different attackers versus fiber length.

### *4.4. Key statistical properties and chaotic strength*

Fig. 7 characterizes the DCE key stream from four perspectives. As illustrated in Fig. 7a, the 3-D phase-space scatter uniformly fills the unit cube without folds or bands, evidencing strong ergodicity. In Fig. 7b, the temporal trace over $10^4$ iterations densely covers [0, 1) with no detectable periodicity. In Fig. 7c, the amplitude histogram exhibits per-bin probabilities of ~0.02, deviating from uniform by less than 5%. In Fig. 7d, the ($x$, $y$) projection shows no striations or clusters, confirming negligible inter-dimensional correlation. Furthermore, the key stream passes all fifteen NIST SP 800-22 tests.

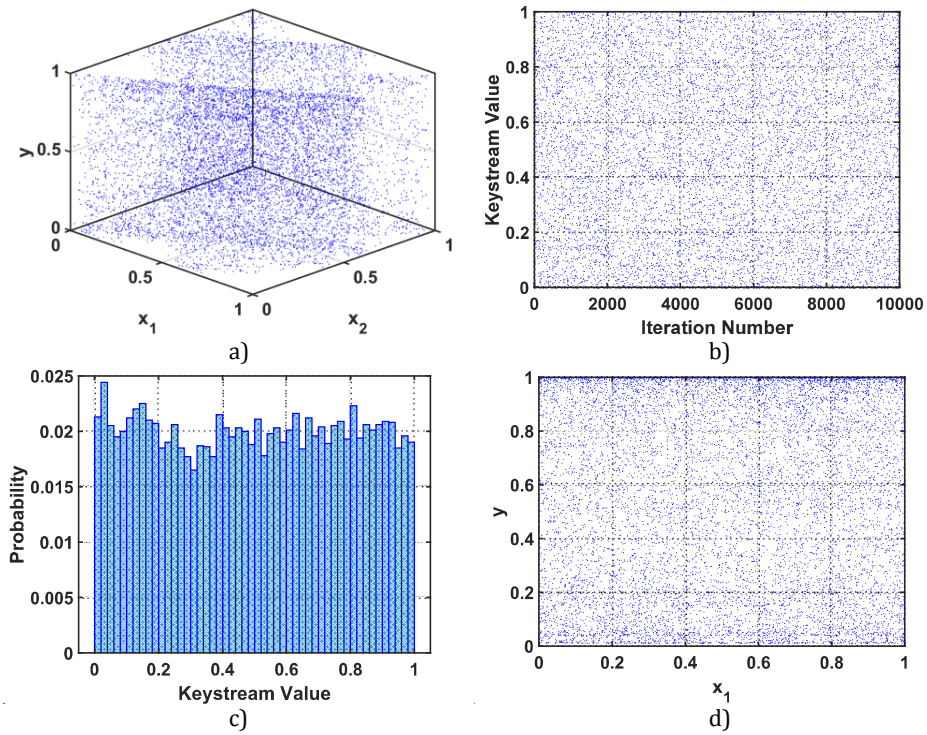


**Fig. 7.** Randomness and ergodicity of the DCE key stream. (a) Dual chaos attractor in the 3D space $(x_1, x_2, y)$; (b) Dual chaos keystream sequence; (c) Probability distribution of the dual chaos keystream; (d) Projection of the dual chaos attractor onto the $(x_1, y)$ plane.

Fig. 8 compares the frequency distributions of two ciphertexts produced from initial seeds differing by $\Delta = 10^{-5}$ (where $\Delta$ denotes the initial key perturbation magnitude). Ciphertext 1 displays localized spikes in multiple bins with large variance, whereas Ciphertext 2 trends toward near-uniformity but with peak positions entirely distinct from those of Ciphertext 1; the two histograms share no common structure. A perturbation as small as $\Delta = 10^{-5}$ is therefore exponentially amplified through $T$=200 rounds of full-state coupled iteration, fully decorrelating the key streams–and consequently the ciphertexts–and constituting the fundamental mechanism by which DCE resists known-plaintext and differential attacks.

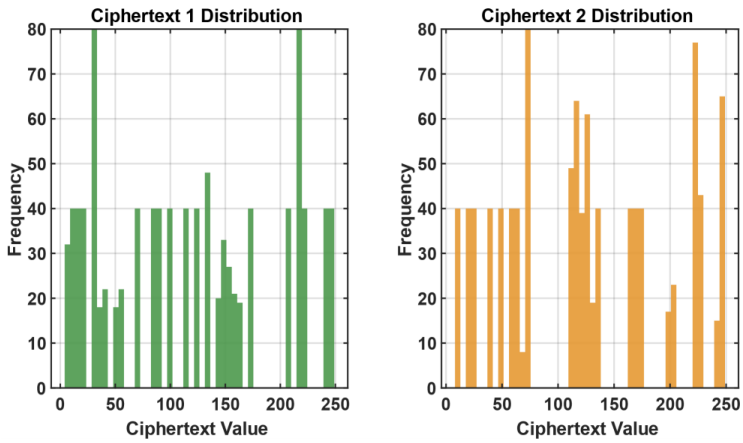


**Fig. 8.** Comparison of frequency distributions of two ciphertexts generated from initial seeds differing by $\Delta = 10^{-5}$.

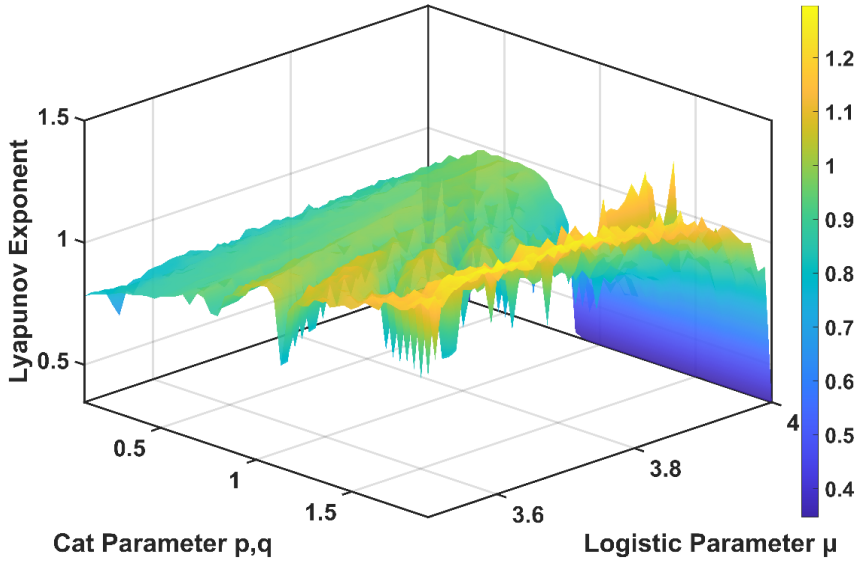


**Fig. 9.** MLE surface of the logistic–Cat coupled system.

Fig. 9 plots the maximum Lyapunov exponent (MLE) of the Logistic–Cat coupled system against the Logistic nonlinearity μ and the Cat stretching parameter. The MLE stays positive throughout, ranging from ∼0.4 to ∼1.25, confirming sustained chaos. It rises along the μ-axis and peaks near the upper bound, while only narrow depressions to ∼0.5 appear near the Cat measure-preserving condition. In contrast, a stand-alone Logistic map is chaotic only for $\mu \geq 3.57$. Dual-map coupling therefore broadens the usable chaotic domain and supplies the dynamical foundation for the $\sim 2^{186}$ key space derived in Section 2.

## 5. Conclusions

This paper proposes a symbol-level DCE scheme tailored to the open-propagation THz segment of 6G F-THz-F links. Logistic–Arnold Cat coupling generates high-dimensional key streams that drive symbol-level QPSK phase rotation, while leaving the DSP framework and photonic heterodyne architecture fully intact. Simulation results confirm that the legitimate-user BER stays below the $3.8 \times 10^{-3}$ HD-FEC threshold up to ∼110 km, whereas the eavesdropper's BER remains pinned near 0.5. The generated key stream further passes the full NIST SP 800-22 suite and exhibits a positive MLE across the operational region, jointly verifying its strong randomness and chaotic behavior. Compared with prior schemes, the proposed DCE achieves three salient benefits: its symbol-level granularity suppresses intra-block correlation typical of block-based encryption; the resulting $\sim 2^{186}$ key space substantially exceeds the $\sim 2^{100}$ ceiling of single-map alternatives, offering a stronger margin against brute-force attacks; and its DSP-only deployment is fully compatible with photonic-aided F-THz-F transport, requiring no hardware modification. Future work will extend the DCE framework to higher-order formats such as 16-QAM and probabilistic-shaping signaling, and pursue an FPGA (Field-Programmable Gate Array)- based implementation for real-time experimental validation.

**Funding.** This research work was supported by the Special Fund of Advantageous and Characteristic disciplines (Group) of Hubei Province. This work is supported by the Hubei Provincial Natural Science Foundation of China (Grant No. 2023AFB474, Grant No. 2024AFB881),

the Anhui Provincial Special Project for Special Needs in Humanities and Social Sciences (Grant No. 2025AHGXSK50067), and the Postgraduate Quality Engineering Project of Anhui Province (Grant No. 2024jyjxggyjY232). Supported in part by Scientific Research Project of Fuyang Normal University (Grant No. 2022KYQD0004). Supported by Special Project for Talent Development in Machinery Industry (Grant No. Cmitc2025087, Grant No. Cmitc2025066, Grant No. Cmitc2025090). This work is supported by Jiangxi Provincial Natural Science Foundation (20232BAB212006) and Open Fund of Advanced Cryptography and System Security Key Laboratory of Sichuan Province (Grant No. SKLACSS-202306) & (Grant No. SKLACSS-202303). Supported by the 2025 E-Commerce Research Project (No. CCPITCBEC-20251167) and the 2025 Annual Project of the 14th Five-Year Plan for National Business Education Research (No. SKJYKT-2505186).

**Conflict of interest.** Authors declare no conflict of interest.

**Authors' contribution.** Dongfei Wang: Conceptualization, methodology, validation, and manuscript writing; Zufang Yang: Funding acquisition and project administration; Shan Zhou: Software implementation and simulation; Xiangqing Wang: Investigation and visualization; Nannan Yu: Resource support; Xiaokun Yang: Manuscript review and editing.

## References

1. Akyildiz, I. F., Han, C., & Nie, S. (2018). Combating the distance problem in the millimeter wave and terahertz frequency bands. *IEEE Communications Magazine*, *56*(6), 102-108.
2. Zhang, J., Zhu, M., Hua, B., Lei, M., Cai, Y., Zou, Y., , Tong, W., Ding, J., Tian, L., Ma, L., Xiao, J., Huang Y., Yu, J. & You, X. (2022). Real-time demonstration of 100 GbE THz-wireless and fiber seamless integration networks. *Journal of Lightwave Technology*, *41*(4), 1129-1138.
3. Nagatsuma, T., Horiguchi, S., Minamikata, Y., Yoshimizu, Y., Hisatake, S., Kuwano, S., Yoshimoto, N., Terada, J. & Takahashi, H. (2013). Terahertz wireless communications based on photonics technologies. *Optics Express*, *21*(20), 23736-23747.
4. Zhang, J., Zhu, M., Lei, M., Hua, B., Cai, Y., Zou, Y., ... & You, X. (2022). Real-time demonstration of 103.125-Gbps fiber–THz–fiber 2× 2 MIMO transparent transmission at 360–430 GHz based on photonics. *Optics Letters*, *47*(5), 1214-1217.
5. Zhu, M., Zhang, J., Hua, B., Lei, M., Cai, Y., Tian, L., ... & You, X. (2023). Ultra-wideband fiber-THz-fiber seamless integration communication system toward 6G: architecture, key techniques, and testbed implementation. *Science China Information Sciences*, *66*(1), 113301.
6. Cai, Y., Yang, X., Zhu, M., Hua, B., Xie, Z., Tong, W., ... & You, X. (2024). Photonics-aided exceeding 200-Gb/s wireless data transmission over outdoor long-range 2× 2 MIMO THz links at 300 GHz. *Optics Express*, *32*(19), 33587-33602.
7. Zhang, Y., Shu, H., Guo, Y., Zhou, P., Wang, L., Cai, J., ... & Wang, X. (2026). Integrated photonics enabling ultra-wideband fibre–wireless communication. *Nature*, 1-8.
8. Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, *560*, 7-11.
9. Wu, Y., Zhang, Z., Luo, H., Deng, L., Yang, Q., Dai, X., ... & Cheng, M. (2023). 100Gb/s coherent optical secure communication over 1000 km based on analog-digital hybrid chaos. *Optics Express*, *31*(20), 33200-33211.
10. Zheng, L., Zhang, Z., Fok, M. P., Liu, Z., & Xiao, S. (2021). Optical analog noise encryption with adaptive recovery of two-dimensional keys. *IEEE Photonics Technology Letters*, *33*(21), 1185-1188.
11. Lei, C., Lin, R., Li, Y., Wang, B., Zhang, M., Zhao, Y., & Zhang, J. (2023). Integration of self-adaptive physical-layer key distribution and encryption in optical coherent communication. *Journal of Lightwave Technology*, *41*(17), 5599-5606.
12. Wang, D., Wang, H., & Ji, Y. (2024). Secure key generation and distribution scheme based on historical fiber channel state information with LSTM. *Optics Express*, *32*(2), 1391-1405.
13. Xiao, Y., An, Z., Jiang, L., Zhou, C., Li, Y., & Wang, S. (2024). Probabilistic shaping encryption scheme based on dual-parameter bit-weighted distribution matching in MMW-RoF system. *Journal of Lightwave Technology*, *43*(2), 539-546.
14. Hao, N., Jiang, L., Feng, J., Sun, J., Yi, A., Pan, W., & Yan, L. (2024). Numerical investigations of M-QAM chaotic optical communication with amplitude and phase encryption. *Journal of Lightwave Technology*, *42*(15), 5141-5147.
15. Kanakidis, D., Argyris, A., Bogris, A., & Syvridis, D. (2006). Influence of the decoding process on the performance of chaos encrypted optical communication systems. *Journal of Lightwave Technology*, *24*(1), 335.

16. Zhao, A., Jiang, N., Liu, S., Zhang, Y., & Qiu, K. (2021). Physical layer encryption for WDM optical communication systems using private chaotic phase scrambling. *Journal of Lightwave Technology*, *39*(8), 2288-2295.
17. Wang, Y., Zhang, Q., Xin, X., Sun, M., Gao, R., Yao, H., ... & Li, Z. (2024). Security enhancement for NOMA-PON with 2D cellular automata and Turing pattern cascading scramble aided fixed-point extended logistic chaotic encryption. *Journal of Optical Communications and Networking*, *16*(12), 1204-1217.
18. do Nascimento, J. C., Damasceno, R. L. C., de Oliveira, G. L., & Ramos, R. V. (2018). Quantum-chaotic key distribution in optical networks: from secrecy to implementation with logistic map: JC do Nascimento et al. *Quantum Information Processing*, *17*(12), 329.
19. Tang, X., & Mandal, S. (2021). Encrypted physical layer communications using synchronized hyperchaotic maps. *IEEE Access*, *9*, 13286-13303.
20. Chang, X. Y., Deng, T., Zhang, L. (2025). Design of an odd order orthogonal transform assisted MIMO transceiver based on chaotic encryption. *Optical Communication Technology*, *49*(2), 57-63.
21. Akraam, M., Rashid, T., & Zafar, S. (2024). A novel and secure image encryption scheme based on two-dimensional logistic and Arnold Cat map. *Cluster Computing*, *27*(2), 2029-2048.
22. Zareai, D., Balafar, M., & FeiziDerakhshi, M. (2023). EGPIECLMAC: efficient grayscale privacy image encryption with chaos logistics maps and Arnold Cat. *Evolving Systems*, *14*(6), 993-1023.

Yang, Z., Wang, D., Zhou, S., Wang, X., Yu, N., and Yang, X. (2026). Symbol-Level Physical-Layer Encryption Driven by Coupled Chaotic Maps for Fiber-THz Integrated Links. *Ukrainian Journal of Physical Optics*, *27*(4), 04001 – 04015.
doi: 0.3116/16091833/Ukr.J.Phys.Opt.2026.04001

***Анотація.*** *Для протидії пасивному прослуховуванню у відкритому терагерцовому (THz) сегменті 6G оптоволоконних з'єднань ми пропонуємо схему символьного шифрування з подвійним хаосом (DCE), що поєднує логістичну карту з картою кота Арнольда. Шляхом 200 раундів спільної ітерації, багатоцифрового вилучення-конкатенації-нормалізації та розширення просторово-часового кореляційного зворотного зв'язку генеруються рівномірно розподілені ключі [0, 1) з пригніченою кореляцією між сусідніми символами. Потік ключів повністю керує фазовим обертанням квадратурної фазової маніпуляції в межах цифрової обробки сигналів передавача, залишаючи оптично-терагерцевий інтерфейс недоторканим. На фотонній гетеродинній платформі 360–430 ГГц з бездротовою протяжністю 3 м BER легітимного користувача залишається нижче порогу жорсткої корекції помилок прямого рішення $3{,}8\times10^{-3}$ до ~124 км одномодового волокна, тоді як підслуховувачі залишаються заблокованими поблизу 0,5. Ключовий простір досягає $\sim 2^{186}$, потік проходить повний набір NIST SP 800-22, а максимальний показник Ляпунова залишається додатним на всій операційній області. Таким чином, DCE пропонує легкий, кількісно оцінюваний шлях безпеки на фізичному рівні для конвергенції оптичного та ТГц-зв'язку 6G.*

***Ключові слова:*** *6G, оптоволокно-ТГц-оптоволокно, шифрування фізичного рівня, подвійний хаос, логістична карта, карта Кота Арнольда*