Research Article

ADVANCED PHOTONICS

Private communication with photonic terahertz chaos

Qiuzhuo Deng,[a] Lu Zhang,[a,*] Zhidong Lyu,[a] Xiaodan Pang,[b,c,d] Oskars Ozolins,[b,c,d] and Xianbin Yu[a,*]
[a]Zhejiang University, College of Information Science and Electronic Engineering, Hangzhou, China
[b]Royal Institute of Technology, KTH, Applied Physics Department, Stockholm, Sweden
[c]Research Institutes of Sweden, RISE, Networks Unit, Kista, Sweden
[d]Riga Technical University, Institute of Photonics, Electronics and Telecommunications, Riga, Latvia

Abstract. Terahertz (THz) communications are vulnerable to eavesdropping due to their scattering and diffraction properties, which limits their practical deployment. We propose a photonic THz chaos encryption and synchronization scheme to secure THz communications. We experimentally demonstrate the generation, encryption, and wireless transmission of a 5 Gbit/s non-return-to-zero signal at 120 GHz using flexible photonic THz chaos. In addition, we achieve high-quality chaos synchronization with a neural network, attaining a correlation coefficient of up to 90.6%. This scheme offers a viable solution for secure THz communications, showing significant potential for enhancing wireless communication privacy.

Keywords: physical layer security; private communication; THz photonics; THz chaos encryption; THz chaos synchronization.

Received Jul. 24, 2024; revised manuscript received Sep. 9, 2024; accepted for publication Oct. 12, 2024; published online Nov. 21, 2024.

[DOI: 10.1117/1.AP.6.6.066004]

1 Introduction

Terahertz (THz, 100 GHz to 10 THz) communication has garnered significant attention due to its ability to carry large amounts of data, leveraging the abundant spectrum resources within these frequency domains. Recent advancements in THz devices and systems have enabled high data rates in the THz band.[1–3] However, despite the use of highly directional narrow beams, THz signals propagating in free space remain vulnerable to security threats such as eavesdropping caused by scattering and diffraction.[4–6]

To address these security concerns, the implementation of secure systems for THz communication has become crucial. Traditional encryption methods, which rely on mathematical complexity, are commonly employed in higher layers of communication protocols to protect against signal interception.[7,8] However, the rapid growth of large-scale computing is exposing vulnerabilities in these cryptosystems. Comparatively, physical-layer-based encryption methods, which utilize inherent physical characteristics of communication systems or external random noise, offer enhanced security in key distribution and message transmission.[9,10]

As one desired candidate for key distribution, quantum key distribution technology shows great promises for unconditional security at the THz band, which has rapidly evolved in recent years.[11–14] However, quantum hardware is not technologically mature for THz frequencies.[15–18] At the same time, security strategies focusing on transmission have made their presence felt at the THz band over the past few years. Quantum noise stream ciphers[19,20] and digital chaotic ciphers,[21] which derive from mathematical complexity-based ciphers, have demonstrated their excellent integration with existing digital signal processing (DSP) lgorithms to achieve high-speed THz communications with enhanced security. However, dynamic degradation of digital ciphers, characterized by periodicity and complete predictability, may pose a threat to chaotic communication systems.[22] Meanwhile, a holistic security of communication system is still required by system design and complexity enhancement.

In this case, physical chaos, excited in electronic or photonic nonlinear systems, presents a promising approach for secure THz communications by exploiting the complex characteristics of strange attractors.[23] This method achieves privacy through the intricate fractal dimensions and the complex characteristics inherent to chaotic systems.[24,25] Electronics-based chaos sources

*Address all correspondence to Lu Zhang, zhanglu1993@zju.edu.cn; Xianbin Yu, xyu@zju.edu.cn

supported by nonlinear circuits can provide high-power chaos output, facilitating high-power encrypted THz emission. However, limited instantaneous bandwidth and spectrum impurity due to electronic components restrain system performance. These problems are further accentuated in today's speed-seeking THz systems, which require abundant spectrum resources to carry large amounts of data and information.

Since the chaos synchronization was proposed in 1990,[26] numerous photonics-based architectures for chaotic communication have been investigated, where internal or external nonlinear photonics-based cavities are excited by sufficient optical or electrical feedback to generate chaos. Chaos has proven its ability in securing fiber-optic channels and has achieved impressive private transmissions over the past few decades.[27–30] Meanwhile, efforts to secure wireless channels using physical chaos have been undertaken for many years. Direct chaotic communication in the microwave band was originally attempted with a data rate of several Mbps.[31,32] As carrier frequency is gradually increasing with the explosive demand of data throughput, chaotic free-space optical communications are of great interest and have achieved impressive transmission in recent years.[33–36] While efforts to secure wireless channels using physical chaos have begun, they have predominantly targeted the near-infrared band or higher frequencies. Improving the privacy of communication links within the THz gap remains a significant challenge.

In this paper, we propose a photonic THz chaos encryption and synchronization scheme for secure THz communications. By generating physical chaos within the optical realm and utilizing flexible photonics for THz transformation, we achieve high privacy for THz links. In a proof-of-concept experiment, we demonstrate chaotic THz communication at 120 GHz with a 5 Gbaud non-return-to-zero (NRZ) signal. The proposed neural network (NN)-based intelligent chaos synchronization scheme achieves high-quality synchronization with a correlation coefficient (C.C) of up to 90.6% for chaos decryption. This proposed photonic THz chaotic private communication system represents a significant advancement in the application of chaos at the THz band and paves the way for high-privacy wireless communications.

2 Principles and Methods

2.1 Vision of Private THz Chaotic Communications

Figure 1 shows the conceptual scenario of private THz chaotic communications involving multiple wireless end users who exchange broadband THz communication signals. In this example, a person-to-person communication system is depicted, where the legitimate transmitter, Alice, sends an encrypted THz signal to the legitimate receiver, Bob. The narrow beam of THz waves makes eavesdropping within the beam range challenging. However, due to the scattering and diffraction properties of THz waves, an eavesdropper, Eve, can intercept the signal by placing a passive object in the transmission path to scatter radiation toward him.

In this system, Alice encrypts the messages using physical chaos encryption, introducing intentional physical disturbances that can be reconstructed with shared hardware-based or software-based parameters as a private key. Bob, possessing the pre-shared key of parameters for the designed NNs from Alice, can decrypt the signal by reconstructing and eliminating the chaos, which Eve cannot do. It is important to note that this communication link is private rather than necessarily secure. Being secure implies that the system is entirely invulnerable, while being private indicates it provides a sufficient level of encryption to deter a less-determined eavesdropper.[33] This private wireless person-to-person communication system can potentially be expanded to other communication systems, such as wireless backhaul networks or satellite communication systems.

2.2 Basic Architecture of THz Chaotic Communication Transmitter and Receiver

Figure 2 shows the basic architecture of THz chaotic communication transmitter and receiver. As for optical chaos generation, a nonlinear cavity is required to excite the chaotic oscillation, where an electro-optic modulator (EOM) is used as an instance of the key optoelectronic device for nonlinear electro-optic conversion in the external cavity. The amplifier in the cavity is essential to generate optical chaos by driving

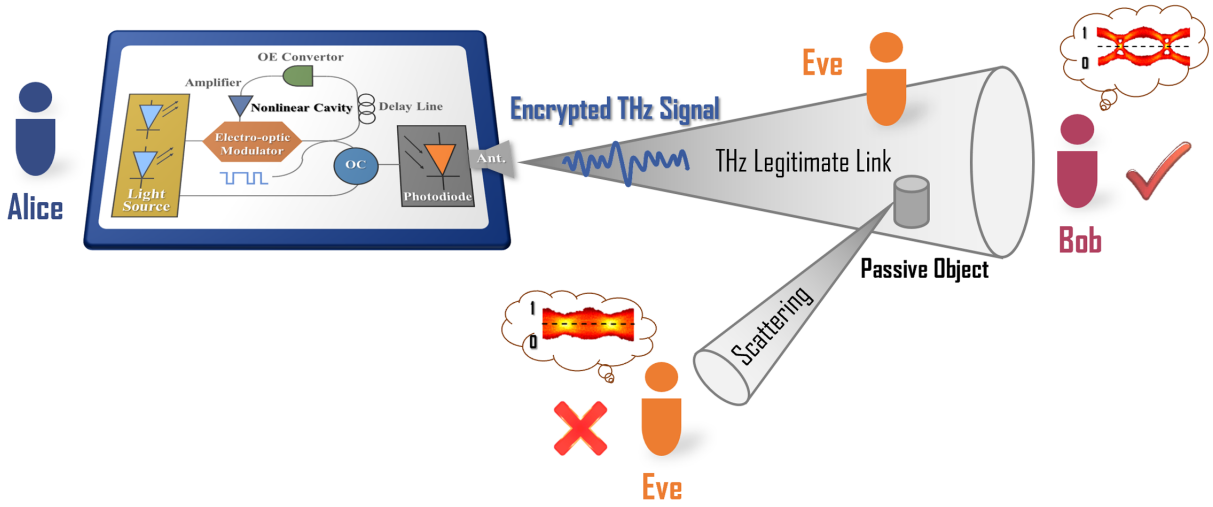

Fig. 1 Conceptual scenario of private person-to-person THz chaotic communication.

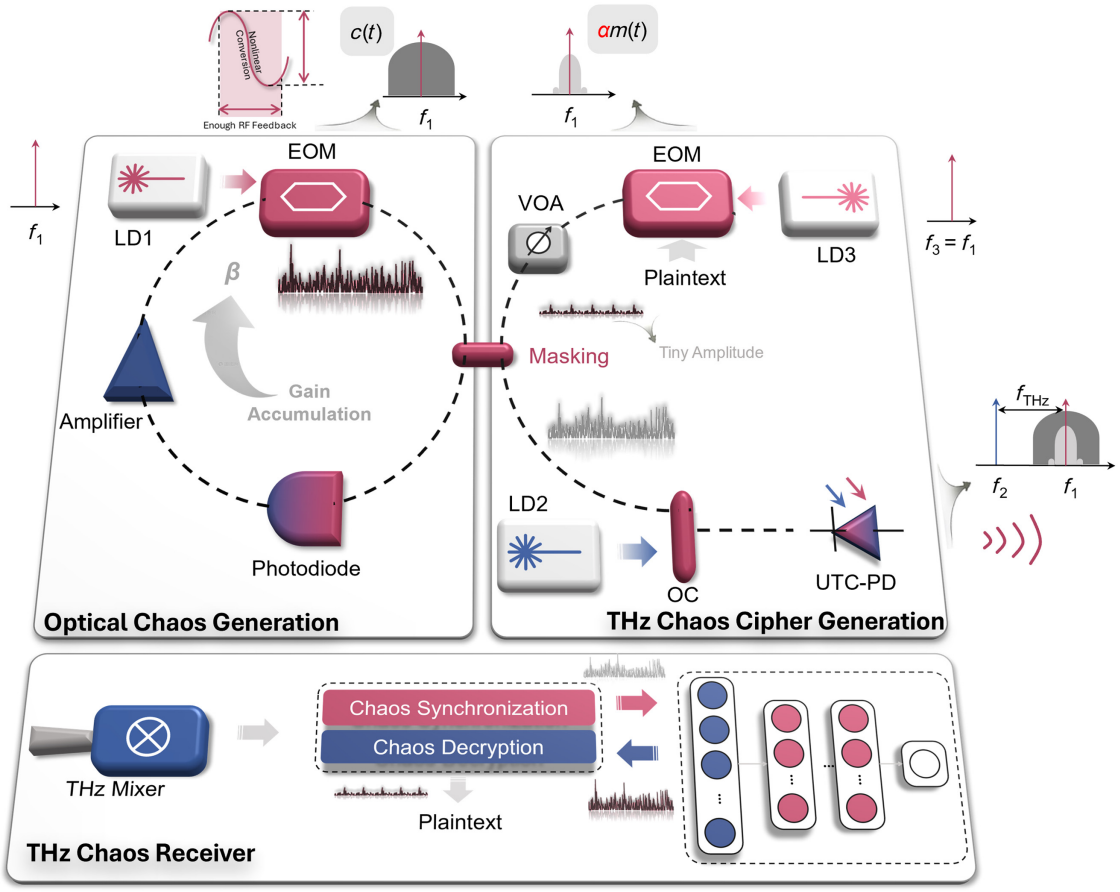

Fig. 2 Schematic of photonic heterodyne generation of encrypted THz signal with physical chaos.

the EOM to fully utilize the nonlinearity. The chaotic oscillation is reflected on the intensity or phase of the output signal.

As for THz chaos cipher generation, the output of chaos cavity is used for masking the optical plaintext in terms of intensity or phase. As shown in Fig. 2, the intensity chaos masking is, as an instance, where the plaintext-modulated optical signal with low amplitude is embedded within large intensity chaos fluctuations. In this case, messages with small amplitudes are controlled by a variable optical attenuator (VOA) and can be effectively concealed, thereby ensuring they do not interfere with larger chaotic disturbances and remain undetected by potential eavesdroppers. Concurrently, chaos introduces an expanded spectrum that overlaps with that of messages, thus making it more difficult for eavesdroppers to perform spectrum analysis. After chaos masking, optical message signal is coupled with the optical LO with the frequency of f_2 and injected to a broadband photodiode (PD) for photonic heterodyne detection. Encrypted signals with chaos masking in the THz domain can be generated in a photodiode, such as unitraveling-carrier photodiode (UTC-PD), and the frequency f_{THz} equals the difference of f_2 and f_1. To minimize the influence of phase noise induced by optical source, a coherent optical source can be applied to enhance the stability of the generated THz encrypted signal.

At the THz chaos receiver, the THz chaos-encrypted signal is received by a THz mixer and captured for further processing. After NN-based chaos synchronization and decryption, the plaintext can be obtained, which effectively simplifies the system complexity of the THz chaos receiver.

The chaotic encryption is achieved by chaos masking in terms of intensity with an optical coupler (OC) or phase with a phase modulator (PM). The general process of encryption can be expressed as

$$c(t+\Delta T) = f_{\mathrm{NLF}}(\beta(c(t)+\alpha\cdot m(t)) * h(t)), \tag{1}$$

where $f_{\mathrm{NLF}}(\cdot)$ is the nonlinear function of EOM, which is mathematically modeled by the NN to reconstruct the chaotic time series. $c(t)$ and $m(t)$ refer to the normalized intensity or phase of chaos or plaintext signal, respectively. β stands for the total gain of cavity, and the total impulse response of photodiode and amplifier in the cavity is represented by $h(t)$. Symbol $(*)$ indicates the convolution operation. The mask coefficient α is defined as the ratio of the peak-to-peak (PtP) value of optical message to the PtP value of optical chaos. Therefore, the privacy introduced by chaos masking is enhanced by combining the chaos $c(t)$ and message $m(t)$ in an appropriate ratio, which is adjusted by a VOA.

For a specific Mach–Zehnder modulator (MZM)-based chaos cavity, the numerical model is expressed by the Ikeda equation,[37] shown as

$$c(t)+\frac{1}{\Delta\omega}\cdot\frac{\mathrm{d}c(t)}{\mathrm{d}t}+\frac{\omega_0^2}{\Delta\omega}\cdot\int_0^t c(\zeta)\mathrm{d}\zeta = \beta\cdot\cos^2((c(t-\Delta T)+\alpha\cdot m(t-\Delta T))+\varphi_0). \tag{2}$$

The left items of the equation refer to the output of an equivalent bandpass filter, which is characterized by the bandwidth $\Delta\omega$ and the central frequency ω_0. Especially, $c(t)$ in the equation is a dimensionless voltage, given as

$$c(t) = \frac{\pi V(t)}{2V_{\pi\mathrm{RF}}}, \tag{3}$$

where $V_{\pi\mathrm{RF}}$ represents the radio-frequency (RF) half-wave voltage and $V(t)$ is denoted as the RF input of MZM. $\varphi_0 = \pi V_{\mathrm{Bias}}/(2V_{\pi\mathrm{DC}})$ refers to the initial phase, determined by the MZM's direct current (DC) bias voltage V_{Bias} and DC half-wave voltage $V_{\pi\mathrm{DC}}$. The cosine-squared nonlinearity is induced by the transfer function of the MZM.

2.3 Neural Network Training and THz Chaos Synchronization

Figure 3 shows the principle of NN training and THz chaos synchronization for private THz chaotic communication. At the transmitter side (Alice), digital samples captured by the analog digital converter (ADC) from two PDs are used to train the NN, where the encrypted signal is used as the input matrix **X** and the generated chaotic signal is used as the desired output vector **Y**. A digital lowpass filter and a least mean square filter are applied for PD and ADC channel prematching. The well-trained NN is considered as the private key that is preshared between Alice and Bob. At the legal receiver side (Bob), the encrypted THz signal needs to be downconverted to the intermediate frequency (IF) to be captured by the ADC. The received IF digital samples are then processed offline and the baseband samples are input to the NN to reconstruct the chaotic time series. The NN is applied to synchronize the chaos, which means NN reconstructs the chaotic signal $c(t)$ using the received signal $c(t) + m(t)$. The process of decryption is subtraction, where $m(t)$ can be obtained from the known $c(t) + m(t)$ and reconstructed $c(t)$.

3 Results and Discussions

3.1 Experimental Setup of Photonic THz Chaotic Communication

Figure 4 shows the experimental setup of the private THz chaotic communication system. Here, in the experiment, the coherent optical source is realized by generating an optical frequency comb (OFC), which is excited by a 1550-mm continuous-wave (CW) laser. A PM is employed as the core device driven by a 30 GHz single-tone RF signal in the OFC generator. The upper inset of Fig. 4 depicts the optical spectrum of the OFC, where the comb space equals the driving frequency of 30 GHz. With a programmable wavelength selective switch, only two tones of the OFC remain, and the frequency difference is set to match the desired frequency of the desired THz carrier. The optical carrier at 193.461 THz is regarded as the optical LO, whereas the other with the frequency of 193.341 THz is amplified by an erbium-doped fiber amplifier (EDFA) and used for chaos cavity excitation. In the cavity, an EDFA and an RF amplifier (RFA) are used for optical and electrical amplification to obtain enough gain driving the MZM, respectively. The MZM is the key device for nonlinear electro-optical conversion to excite chaotic oscillations in the external cavity, whose DC bias point is affected by the experimental conditions and has a great impact on the dynamic characteristics and nonlinearities of the cavity.[38] In our experiment, the stability of the chaotic oscillation operating point is practically enough for several minutes of transmission and data capture after the DC bias is set. If longer stability is desired, active control of the operating point is needed.[39,40] There is an extra branch leading out of the cavity, where a PD is applied to capture the chaos as vector **X** only for training an NN.

As for message loading, the optical carrier is modulated by a 5 Gbaud NRZ signal, and the frequency of the optical carrier needs to be the same as the central frequency of the generated optical chaos. A VOA is set after the MZM to adjust the mixing ratio of chaos to messages to be masked. After coupling, the encrypted signal needs to be captured as vector **Y** only for

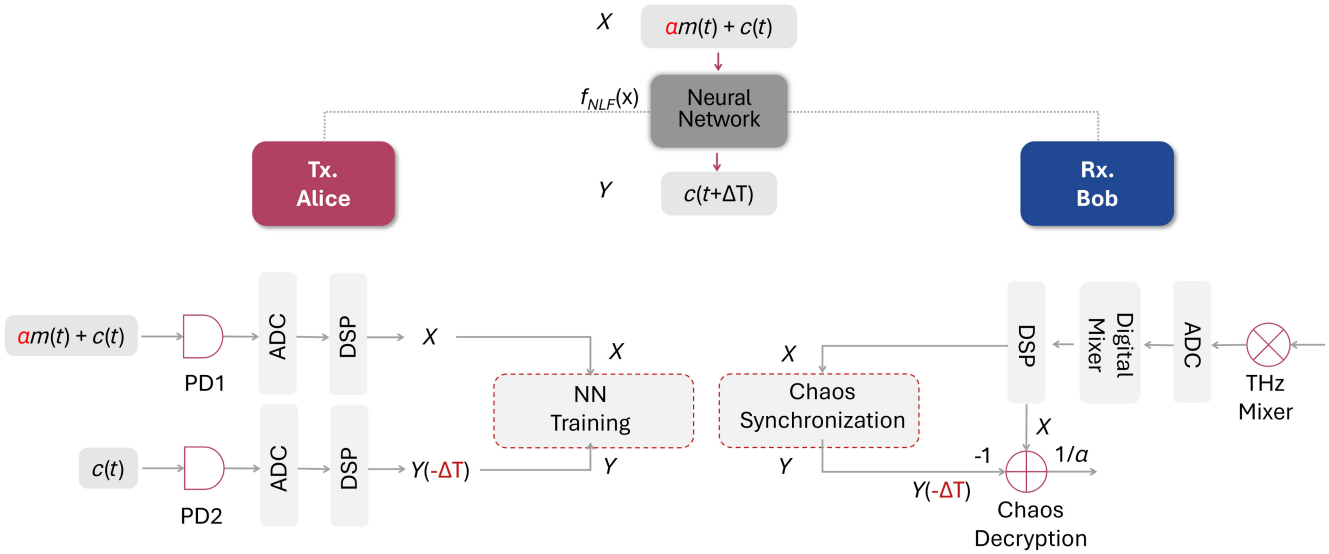

Fig. 3 Principle of NN training and THz chaos synchronization.

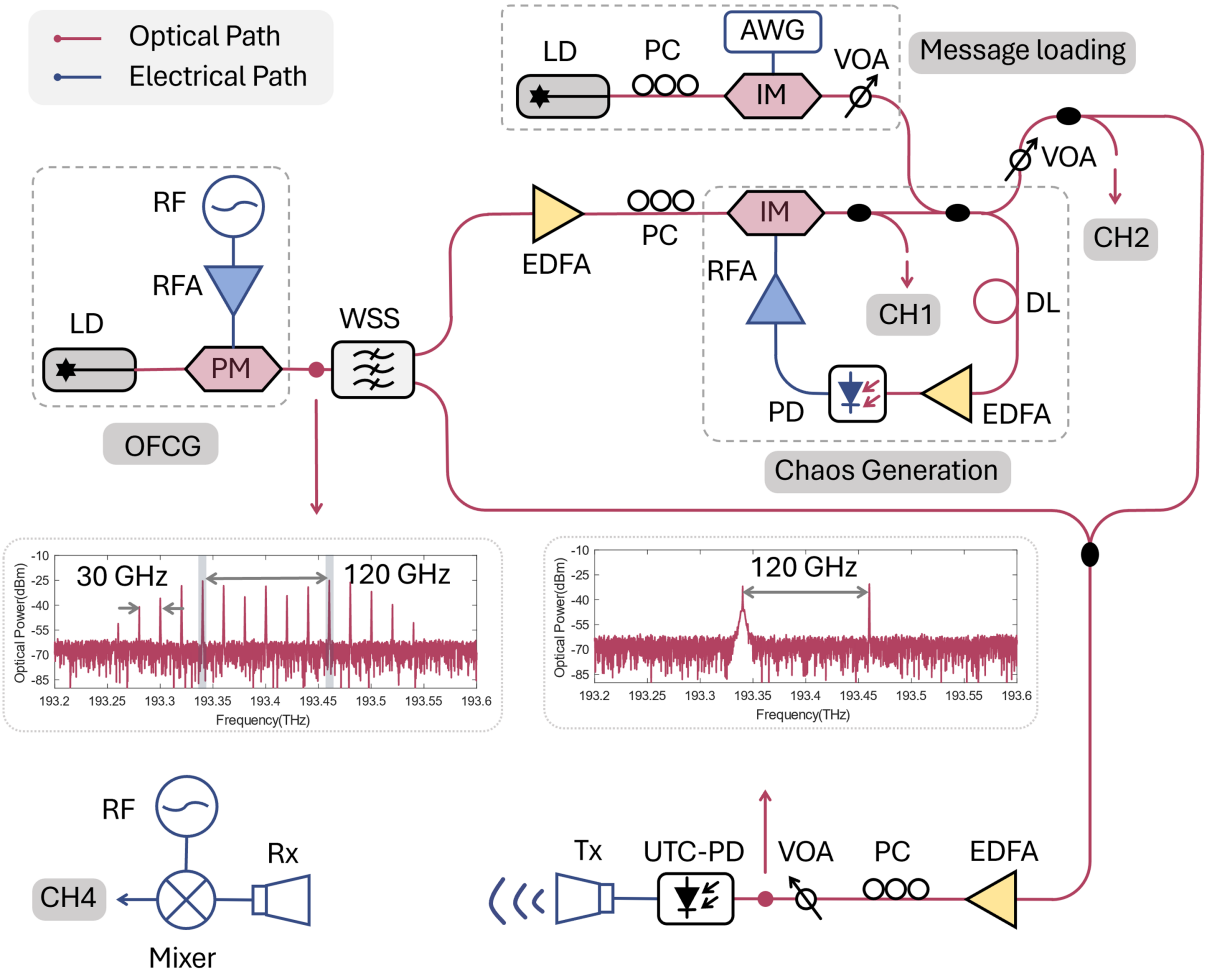

Fig. 4 Experimental setup of private THz chaotic communication.

NN training outside the cavity. To achieve the photonic heterodyne detection, the encrypted signal needs to be coupled with the optical LO. The coupled optical spectrum of the chaos-masked signal and the optical LO is shown in the lower inset of Fig. 4; the frequency difference between two signals is 120 GHz. To optimize the photo-mixing efficiency of the UTC-PD, the optical power of the chaos-masked signal is adjusted to make it balanced with that of the optical LO. After being amplified by the EDFA, the coupled signal is adjusted in polarization and injected into the UTC-PD to generate the THz signal at 120 GHz. A polarization-maintaining VOA is employed to regulate the input optical power, consequently controlling the photocurrent of the UTC-PD. It should be mentioned that the heterodyne detection scheme benefits the flexible THz chaos-encrypted signal generation, which will facilitate the practical deployment of THz chaotic communication systems at a proper THz carrier frequency.

Influences induced by atmospheric factors[34,41–45] need to be considered for THz communications. In the experiment, the transmission distance is set as 0.5 m, which will be extended longer for practical deployments in the future. In this case, influences induced by atmospheric factors can be ignored in the experiment. After the wireless transmission, the electrical coherent manner is applied to receive the THz encrypted signal with a THz subharmonic mixer. The RF source offers a single-tone signal with the frequency of 10.833 GHz and drives the mixer with an electrical LO at 130 GHz after 12 times up-conversion. The IF signal with the frequency of 10 GHz is then sampled by a DSO (digital storage oscilloscope, i.e., ADC) with a sampling rate of 80 GSa/s, and the digital samples are stored for offline processing.

3.2 Synchronization Performance for Photonic THz Chaotic Communication

Modeling of the optical wireless transmission link is essential to achieve high-quality chaotic synchronization. In the experiment, a full-connected NN is trained to reconstruct the nonlinear chaos cavity. The digital samples are divided into two parts for model establishment, where 80% of samples were used as the training subset, and the remaining 20% were used as the validation subset. The input dimension is set to 5000, and the NN features eight hidden layers, each with 770 neurons and an output layer with a single neuron. The network is trained using backpropagation (BP) and the Adam optimizer with a learning rate of 0.008. Rectified linear unit (ReLU) [max(0, x)] acts as the activation function. Mean squared error loss between the original chaos and the NN output is used for parameter updates, with training conducted over 60 epochs. Hyperparameters of the NN may need minor adjustments for optimal performance in the experiment.

Figure 5(a) shows the NN training performance in terms of C.C of up to 97.3% at Alice's side, which indicates the nonlinear chaos cavity is excellently mathematically modeled. As is shown in Fig. 5(b), the temporal fluctuation of NN output behaves similarly to the original chaos. The well-trained NN is first self-tested using the encrypted signal at Alice's side and the C.C results (red triangles) with seven different mask coefficients (α) are shown in Fig. 5(c), where α is defined as, $V_{\text{ppMessage}}/V_{\text{ppSignal}}$, and the V_{pp} denotes the PtP value of the optical message to optical chaos. All C.Cs are over 93%, and the mean value reaches 94.6%, showing the excellent potential of trained NN for chaos synchronization. For the synchronization performance of Bob, the C.C deteriorates and the mean value decreases to 90.6%, which is shown by the blue pentagrams in Fig. 5(c). In general, a C.C above 90% indicates the chaos decryption can be achieved to support the chaotic communication. Device mismatch mainly causes the C.C's degradation induced by different PDs and different channels of DSO. In the proposed scheme, the NN is trained on a specific nonlinear chaos cavity designed for a particular THz private communication system.[22,46–49] The nonlinearity inherent in the system acts as a hidden private physical key, enhancing the privacy of THz communication with chaos encryption.

3.3 Photonic THz Chaotic Communication Performance

Figure 6 shows the BER performance with different α in four different decryption situations. Considering the device mismatch at Alice's side, there exists an optimal BER limit in the experiment, shown by the red line with a square. The optimal BER is tested in back-to-back transmission; the C.C is assumed to be 100%. It means that all experimental BERs will never be smaller than the optimal BER when α is fixed. The yellow line with a triangle is the BER performance of Alice, where the well-trained NN is self-tested for chaos synchronization. The result is obtained in back-to-back transmission, but unlike the test for an optimal BER line, the chaos synchronization is realized with a trained NN and is definitely not 100%, resulting in a BER penalty between Alice's result and optimal BER limit.

The blue line with a hexagon is the BER performance of Bob, where Bob can decrypt the chaos-masked signal with the pre-shared NN with clear eyes. The BER of Bob can reach under the SD-FEC[50] limit @ 2.0×10^{-2} when α is larger than 0.75 and under HD-FEC[51] limit @ 3.8×10^{-3} when α is larger than 0.90. As for Eve without the shared NN, the BER performance deteriorates with indistinguishable eyes by direct cracking of the encrypted signal, as shown by the gray line with a solid circle. The obvious BER penalty between Bob and Eve suggests chaos encryption has brought enough privacy to legal receivers.

The photocurrent of the UTC-PD at the transmitter is maximized to achieve the highest possible THz signal output power. The BER performance of the THz communication system without encryption is evaluated under these same conditions. The BER results were obtained below 3.6×10^{-7}. The comparison reveals a penalty for encrypted transmission compared to

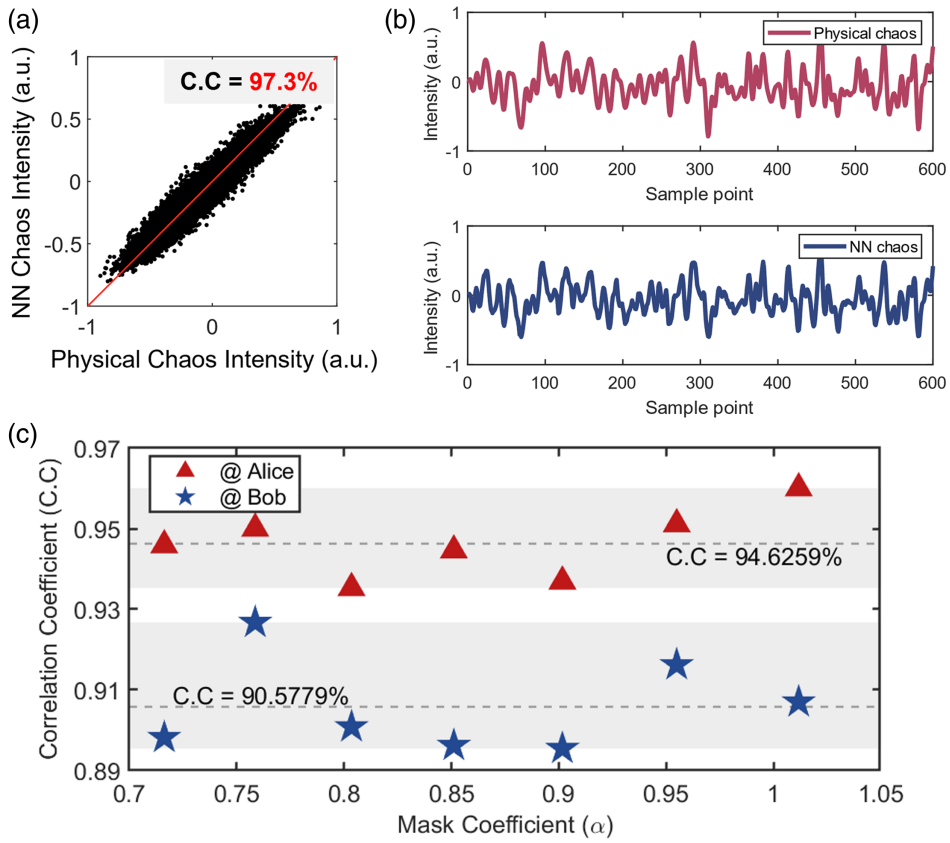

Fig. 5 Photonic THz chaos synchronization performance. (a) NN training performance between physical chaos and chaos from NN with 45-deg line; (b) temporal waveform comparison between physical chaos and chaos from NN; (c) C.C results at Alice's and Bob's sides.

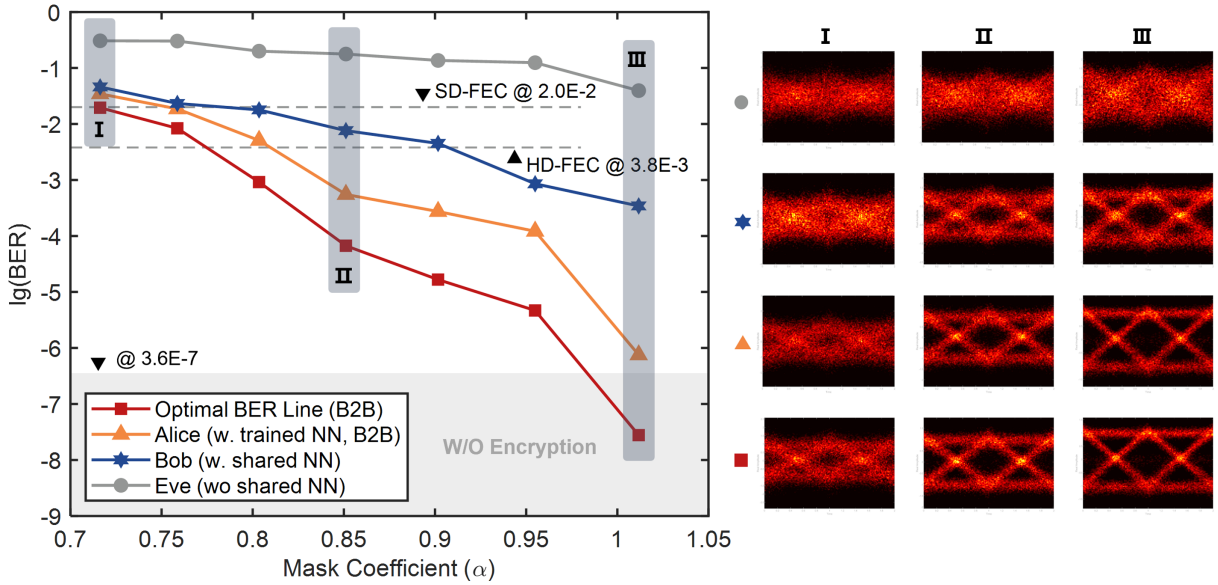

Fig. 6 Transmission performance in terms of BER and eye diagram with different mask coefficient (α).

unencrypted transmission, primarily due to errors in chaotic synchronization on the receiver side. However, the enhanced privacy provided by chaos will offer greater benefits to the communication link than the trade-off between encrypted and unencrypted transmission.

The masking ratio between optical message and chaos significantly impacts both the privacy and reliability of the THz chaotic communication system.[35,46,49] In general, a larger α results in weaker privacy because the chaotic signals, being a smaller fraction of the combined signal, may be perceived as random noise that disrupts THz communications. Conversely, a smaller α enhances privacy but complicates decryption for legitimate receivers, as the plaintext signal is perceived as low-amplitude noise relative to chaotic signals. Since chaotic synchronization in legitimate receivers is always imperfect, errors in synchronization affect the accuracy of decrypting low-amplitude plaintext signals. Thus, there is an inherent trade-off between privacy and transmission performance for a given α, which is experimentally determined for each specific THz chaos system. In the experiment, when α is adjusted to smaller than 0.75, optimal BER limit is larger than the SD-FEC limit with the deteriorated performance of legal decryption at both transmitter side (Alice) and legal receiver side (Bob). High interference introduced by chaos degrades the BER performance of Alice and Bob, even though Eve's BER deteriorates more severely. Conversely, setting α to greater than 1 introduces significant security risks, with Eve's BER dropping below 0.1, even though Alice and Bob achieve optimal BER performance, which is not acceptable. Therefore, proper masking coefficient ($0.8 \leq \alpha \leq 0.95$) for THz chaotic system enables information to be effectively hidden and recovered by legal receivers and resist eavesdropping.

3.4 Privacy Analysis of Photonic THz Chaotic Communication

To further quantitatively evaluate the transmission performance and privacy enhancement brought by chaotic encryption for THz communications, the data capacities of the legitimate channel and illegitimate channel are first calculated, which are defined as C_{Bob} and C_{Eve}, respectively.[52] The data capacity means the maximum average mutual information in the transmission channel and the value of C_x closer to 1 refers to a better transmission performance in this channel:

$$C_{\mathrm{Bob}} = 1 - (-\mathrm{BER}_{\mathrm{Bob}} \log_2(\mathrm{BER}_{\mathrm{Bob}}) - (1 - \mathrm{BER}_{\mathrm{Bob}}) \log_2(1 - \mathrm{BER}_{\mathrm{Bob}})), \tag{4}$$

$$C_{\mathrm{Eve}} = 1 - (-\mathrm{BER}_{\mathrm{Eve}} \log_2(\mathrm{BER}_{\mathrm{Eve}}) - (1 - \mathrm{BER}_{\mathrm{Eve}}) \log_2(1 - \mathrm{BER}_{\mathrm{Eve}})). \tag{5}$$

The C_{Bob} and C_{Eve} versus the mask coefficient are shown in Fig. 7, which characterize both transmission and privacy performance. Here, Eve conducts brute-force attacks to the THz chaotic communication system, which means Eve does not obtain the chaotic time series but demodulates the signal directly. It should be mentioned that larger C_{Eve} means lower privacy. It is clearly shown that the transmission performance makes obvious progress characterized by C_{Bob} with the increasing α, while C_{Eve} also has an increasing trend with α increasing, indicating the deteriorating privacy performance. Moreover, the penalty between Bob and Eve in terms of $C_{\mathrm{Bob}} - C_{\mathrm{Eve}}$ can be used for comprehensive assessment of the privacy and transmission performance, where larger value indicates a better comprehensive performance of privacy and transmission. As is shown in the inset of Fig. 7, the penalty has a stable and slight decrease when α is set at a proper interval from 0.75 to 1, while it declines dramatically when α is larger than 1. It also shows when α is set to smaller than 0.75, the penalty declines, indicating the start of deteriorating performance.

Brute force attack to the NN also needs to be considered for privacy analysis. In a full-connected NN, weight, bias, and activation function of each neuron layer present an infinite array

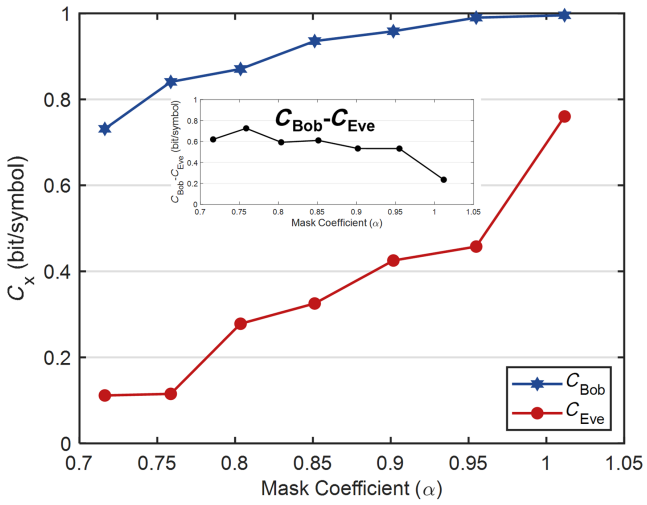

Fig. 7 Data capacities C_{Bob} (blue line with hexagon) and C_{Eve} (red line with dot) versus the mask coefficient (α).

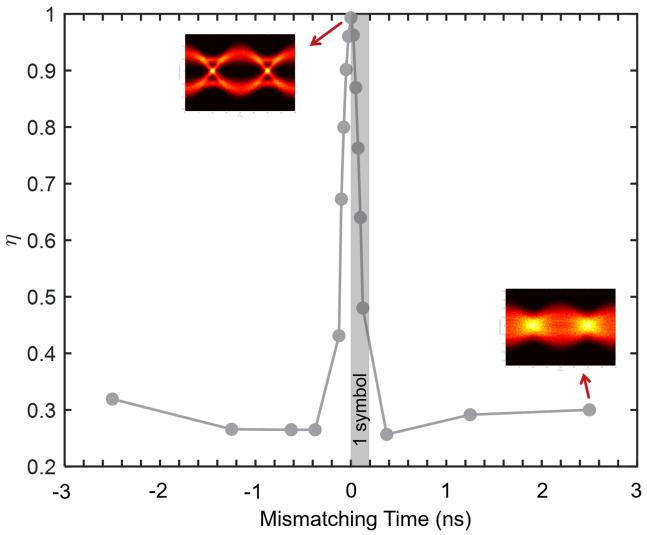

Fig. 8 Information interception probability (η) of Eve with chaos mismatching time.

of possibilities. The system with the parameter space larger than 2^{100} can exhibit enough sensitivity to prevent brute force attacks.[22,53] In the experiment, the NN contain more than 11,000 parameters. Assuming each parameter can take k discrete values, parameter combinations exceed more than k^{11000}, making it difficult to brute force the network by parameter enumeration, thus demonstrating the privacy of NN.

In addition, assuming that Eve has the ability to fully reconstruct the same chaotic signal as Alice's, the privacy of chaotic communication is analyzed by chaos mismatch, which is characterized by the mismatch time, with α is fixed at 0.85. The information interception probability η of Eve can be used for the evaluation of privacy and is defined as the ratio of the illegitimate channel capacity in the source entropy:[52]

$$\eta = \frac{C_{\mathrm{Eve}}}{H(X)} \times 100\%, \tag{6}$$

where $H(\cdot)$ is denoted as the source entropy and is defined as

$$H(X) = -\sum_{x=0}^{1} P(x)\log_2 P(x). \tag{7}$$

The η of Eve is shown in Fig. 8. The value of η that is closer to 1 means worse privacy of the THz chaotic communication system. It can be clearly seen that only if the chaos of Eve matches Alice's exactly can Eve decrypt the encrypted signal with clear eyes and η of 0.993 and tiny time mismatch (only 1 symbol) makes it hard to crack for Eve, thus ensuring the high privacy of transmission between Alice and Bob.

Considering the free ciphertext attack, it is assumed that Eve can reconstruct the chaotic time series without messages and can train an NN. The attack performance of Eve with the trained NN in terms of BER is stable with above 0.1 as α changes, which is shown in Fig. 9. The result demonstrates that optical messages play a crucial role in nonlinear opto-electro conversion within the chaos cavity. Even if Eve successfully reconstructs the chaotic time series with a C.C of up to 96.0%, Eve cannot retrieve the messages.

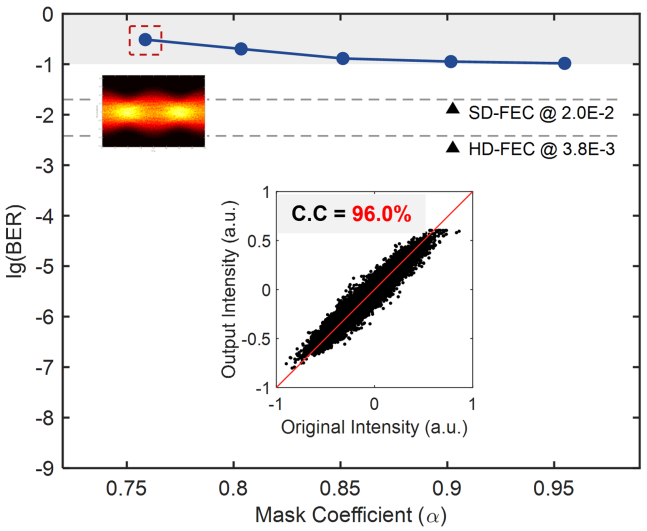

Fig. 9 BER performance of Eve with the free ciphertext attack.

4 Conclusion

We propose and experimentally demonstrate private THz communication using the wireless transmission of a 5 Gbit/s NRZ signal at 120 GHz, employing flexible photonics-based chaos encryption and intelligent chaotic synchronization. The NN facilitates high-quality chaos synchronization with a C.C of up to 90.6%, simplifying the physical complexity of the THz chaos receiver. This approach represents a valuable addition to the application of physical chaos within the THz realm and shows great promise in enabling high-privacy wireless communications.

Disclosures

The authors declare no conflicts of interest.

Code and Data Availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Acknowledgments

We thank Lilin Yi, Junxiang Ke, and Yunhao Xie from Shanghai Jiao Tong University for helpful discussions. This work was supported by the National Key R&D Program of China (Grant No. 2020YFB1805700), the National Natural Science Foundation of China (Grant No. 62471433), the LZP FLPP project 'MIR FAST' lzp-2023-1-0503, the Swedish Research Council (VR) projects 2019-05197 and 2022-04798, and the strategic innovation program Smarter Electronic Systems - a joint venture by Vinnova, Formas and the Swedish Energy Agency A-FRONTAHUL project (2023-00659).

References

1. T. Harter et al., "Generalized Kramers–Kronig receiver for coherent terahertz communications," *Nat. Photonics* **14**(10), 601–606 (2020).
2. L. Zhang et al., "Toward terabit digital radio over fiber systems: architecture and key technologies," *IEEE Commun. Mag.* **57**(4), 131–137 (2019).
3. T. Harter et al., "Wireless THz link with optoelectronic transmitter and receiver," *Optica* **6**(8), 1063–1070 (2019).
4. J. M. Jornet, E. W. Knightly, and D. M. Mittleman, "Wireless communications sensing and security above 100 GHz," *Nat. Commun.* **14**(1), 841 (2023).
5. T. Doeker et al., "Eavesdropping measurements for applications in office environments at low THz frequencies," *IEEE Trans. Microwave Theory Technol.* **71**(6), 2748–2757 (2023).
6. J. Ma et al., "Security and eavesdropping in terahertz wireless links," *Nature* **563**(7729), 89–93 (2018).
7. Y. Zou et al., "A survey on wireless security: technical challenges, recent advances, and future trends," *Proc. IEEE* **104**(9), 1727–1765 (2016).
8. Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: theories, technologies, and challenges," *IEEE Commun. Surv. Tutorials* **19**(1), 347–376 (2016).
9. Y.-S. Shiu et al., "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Commun.* **18**(2), 66–74 (2011).
10. N. Yang et al., "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.* **53**(4), 20–27 (2015).
11. C. H. Bennett and G. Brassard, "Quantum cryptography," in *Proc. IEEE Int. Conf. on Comput. Sys. Signal Process.*, Bangalore, India, pp. 175–179 (1984).
12. H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nat. Photonics* **8**(8), 595–604 (2014).
13. M. Lucamarini et al., "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature* **557**(7705), 400–403 (2018).
14. J.-P. Chen et al., "Quantum key distribution over 658 km fiber with distributed vibration sensing," *Phys. Rev. Lett.* **128**(18), 180502 (2022).
15. E. Diamanti et al., "Practical challenges in quantum key distribution," *npj Quantum Inf.* **2**(1), 16025 (2016).
16. N. K. Kundu et al., "MIMO terahertz quantum key distribution under restricted eavesdropping," *IEEE Trans. Quantum Eng.* **4**, 4100315 (2023).
17. H. Liu et al., "Continuous-variable measurement-device-independent quantum key distribution in the terahertz band," *Photonics* **11**(4), 367 (2024).
18. N. K. Kundu, M. R. McKay, and R. K. Mallik, "Wireless quantum key distribution at terahertz frequencies: opportunities and challenges," *IET Quantum Commun.* 1–12 (2024).
19. R. Nair et al., "Quantum-noise randomized ciphers," *Phys. Rev. A* **74**(5), 052309 (2006).
20. L. Zhang et al., "Quantum noise secured terahertz communications," *IEEE J. Select. Top. Quantum Electron.* **29**(5), 8400110 (2023).
21. F. Wang et al., "Implementation of digital chaotic encryption in THz wireless communication," in *Optical Fiber Commun. Conf.*, pp. M3C–4 (2022).
22. J. Feng et al., "256 Gbit/s chaotic optical communication over 1600 km using an AI-based optoelectronic oscillator model," *J. Lightwave Technol.* **42**(8), 2774–2783 (2024).
23. Q. Deng et al., "Experimental demonstration of photonics millimeter-wave chaotic signal generation," in *2023 Photonics Global Conf. (PGC)*, pp. 32–36 (2023).
24. A. Abel and W. Schwarz, "Chaos communications-principles, schemes, and system analysis," *Proc. IEEE* **90**(5), 691–710 (2002).
25. F. T. Arecchi et al., "Deterministic chaos in laser with injected signal," *Opt. Commun.* **51**(5), 308–314 (1984).
26. L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.* **64**(8), 821–824 (1990).
27. A. Argyris et al., "Chaos-based communications at high bit rates using commercial fibre-optic links," *Nature* **438**(7066), 343–346 (2005).
28. G. D. VanWiggeren and R. Roy, "Communication with chaotic lasers," *Science* **279**(5354), 1198–1200 (1998).
29. J. Ke et al., "Chaotic optical communications over 100-km fiber transmission at 30-Gb/s bit rate," *Opt. Lett.* **43**(6), 1323–1326 (2018).
30. Z. Yang et al., "Chaotic optical communication over 1000 km transmission by coherent detection," *J. Lightwave Technol.* **38**(17), 4648–4655 (2020).
31. A. S. Dmitriev et al., "Ultrawideband direct chaotic data transmission in the microwave range," *Tech. Phys. Lett.* **29**(1), 72–74 (2003).
32. A. S. Dmitriev et al., "Experiments on direct chaotic communications in microwave band," *Int. J. Bifurcation Chaos* **13**(6), 1495–1570 (2011).
33. O. Spitz et al., "Private communication with quantum cascade laser photonic chaos," *Nat. Commun.* **12**(1), 3327 (2021).
34. N. F. Rulkov, M. A. Vorontsov, and L. Illing, "Chaotic free-space laser communication over a turbulent channel," *Phys. Rev. Lett.* **89**(27), 277905 (2002).
35. Y. Zhang et al., "Experimental demonstration of an 8-Gbit/s free-space secure optical communication link using all-optical chaos modulation," *Opt. Lett.* **48**(6), 1470–1473 (2023).
36. Y. Zhang et al., "Simultaneously enhancing capacity and security in free-space optical chaotic communication utilizing orbital angular momentum," *Photon. Res.* **11**(12), 2185–2193 (2023).
37. K. Ikeda, "Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system," *Opt. Commun.* **30**(2), 257–261 (1979).
38. Q. Deng et al., "Generation and Intelligent synchronization of photonic millimeter-wave chaos," *J. Lightwave Technol.*, 1–11 (2024).
39. Y. Fu et al., "Mach-Zehnder: a review of bias control techniques for Mach-Zehnder modulators in photonic analog links," *IEEE Microwave Mag.* **14**(7), 102–107 (2013).
40. M. Zhang et al., "Review of bias point stabilization methods for MZ modulator," *Commun. Signal Process. Sys.* **878**, 751–757 (2022).
41. A. Niaz et al., "Performance analysis of chaotic FSO communication system under different weather conditions," *Trans. Emerging Telecommun. Technol.* **30**(2), e3486 (2019).
42. E. E. Elsayed et al., "Investigations on wavelength-division multiplexed fibre/FSO PON system employing DPPM scheme," *Opt. Quant. Electron.* **54**(6), 358 (2022).

43. E. E. Elsayed and B. B. Yousif, "Performance evaluation and enhancement of the modified OOK based IM/DD techniques for hybrid fiber/FSO communication over WDM-PON systems," *Opt. Quant. Electron.* **52**(9), 385 (2020).
44. Y. Qiao et al., "Security performance of THz links in atmospheric weathers due to absorption," in *2022 Cross Strait Radio Sci. Wireless Technol. Conf. (CSRSWTC)*, pp. 1–3 (2022).
45. Z. Fang et al., "Secure communication channels using atmosphere-limited line-of-sight terahertz links," *IEEE Trans. Terahertz Sci. Technol.* **12**(4), 363–369 (2022).
46. J. Ke et al., "32 Gb/s chaotic optical communications by deep-learning-based chaos synchronization," *Opt. Lett.* **44**(23), 5776–5779 (2019).
47. Z. Yang et al., "Coherent chaotic optical communication of 30 Gb/s over 340-km fiber transmission via deep learning," *Opt. Lett.* **47**(11), 2650–2653 (2022).
48. L. Jiang et al., "Chaotic optical communications at 56 Gbit/s over 100-km fiber transmission based on a chaos generation model driven by long short-term memory networks," *Opt. Lett.* **47**(10), 2382–2385 (2022).
49. J. Liu, J. Zhang, and Y. Wang, "Secure communication via chaotic synchronization based on reservoir computing," *IEEE Trans. Neural Networks Learn. Syst.* **35**(1), 285–299 (2024).
50. D. Chang et al., "LDPC convolutional codes using layered decoding algorithm for high speed coherent optical transmission," in *Opt. Fiber Commun. Conf.*, p. OW1H.4 (2012).
51. F. Chang, K. Onohara, and T. Mizuochi, "Forward error correction for 100 G transport networks," *IEEE Commun. Mag.* **48**(3), S48–S55 (2010).
52. H. Jiao et al., "Physical-layer security analysis of PSK quantum-noise randomized cipher in optically amplified links," *Quantum Inf. Process.* **16**(8), 189 (2017).
53. G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos* **16**(08), 2129–2151 (2006).

Qiuzhuo Deng is currently a PhD candidate with the College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou, China. He received the bachelor's degree from China Agricultural University in Beijing, China, in 2022. His research interests include terahertz photonics and chaos dynamics in systems.

Lu Zhang is currently a research professor with the College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou, China. He received the bachelor's degree from Southeast University, Nanjing, China, in 2014, and the PhD degree from Shanghai Jiao Tong University, Shanghai, China, in 2019. From 2016 to 2017, he was a visiting doctoral student with the KTH Royal Institute of Technology, Stockholm, Sweden, sponsored by the China Scholarship Council. Since 2018, he has been a visiting research engineer with the KTH Royal Institute of Technology and the Kista High-Speed Transmission Laboratory, RISE Research Institutes of Sweden, Stockholm. His research interests include photonics terahertz communications, fiber-optic communications, and digital signal processing algorithms for optical and THz transmission systems.

Xianbin Yu is currently a professor with the College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou, China. He received the PhD degree from Zhejiang University, Hangzhou, China, in 2005. From 2005 to 2007, he was a postdoctoral researcher with Tsinghua University, Beijing, China. Since November 2007, he has been with DTU Fotonik, Technical University of Denmark, Kongens Lyngby, Denmark, where he became an assistant professor in 2009 and was promoted to senior researcher in 2013. He has coauthored more than 200 peer-reviewed international journals and conference papers within the fields of microwave photonics and optical fiber communications. His research interests include mm-wave/THz photonics and its applications, THz communications, ultrafast photonic RF signal processing, and high-speed photonic wireless access technologies.

Biographies of the other authors are not available.