OEA | Opto-Electronic
Advances

Partially coherent optical chip enables physical-layer public-key encryption

Bo Wu, Wenkai Zhang, Hailong Zhou*, Jianji Dong*, Yilun Wang, Xinliang Zhang

https://doi.org/10.29026/oea.2025.250098

Opto-Electronic
Advances

CN 51–1781/TN ISSN 2096–4579 (Print) ISSN 2097–3993 (Online)

Partially coherent optical chip enables physical-layer public-key encryption

Bo Wu, Wenkai Zhang, Hailong Zhou, Jianji Dong, Yilun Wang and Xinliang Zhang

Citation: Wu B, Zhang WK, Zhou HL, et al. Partially coherent optical chip enables physical-layer public-key encryption. *Opto-Electron Adv* **8**, 250098(2025).

https://doi.org/10.29026/oea.2025.250098

Received: 6 May 2025; Accepted: 10 September 2025; Published online: 21 November 2025

Related articles

Research advances of partially coherent beams with novel coherence structures: engineering and applications
Liu Yonglei, Dong Zhen, Chen Yahong, Cai Yangjian
Opto-Electronic Engineering 2022 **49**, 220178 doi: 10.12086/oee.2022.220178

Physics-informed deep learning transport-of-intensity quantitative phase imaging: accurate phase retrieval under partially coherent illumination
Linpeng Lu, Shun Zhou, Yanbo Jin, Xingyu Huang, Habib Ullah, Piotr Zdankowski, Maciej Trusiak, Malgorzata Kujawinska, Qian Chen, Chao Zuo
Intelligent Opto-Electronics 2025 **1**, 250005 doi: 10.29026/ioe.2025.250005

Robust measurement of orbital angular momentum of a partially coherent vortex beam under amplitude and phase perturbations
Zhao Zhang, Gaoyuan Li, Yonglei Liu, Haiyun Wang, Bernhard J. Hoenders, Chunhao Liang, Yangjian Cai, Jun Zeng
Opto-Electronic Science 2024 **3**, 240001 doi: 10.29026/oes.2024.240001

Full-dimensional complex coherence properties tomography for multi-cipher information security
Yonglei Liu, Siting Dai, Yimeng Zhu, Yahong Chen, Peipei Peng, Yangjian Cai, Fei Wang
Opto-Electronic Advances 2025 **8**, 240278 doi: 10.29026/oea.2025.240278

More related article in Opto-Electronic Journals Group website

OEA Opto-Electronic Advances

http://www.oejournal.org/oea

OE_Journal @OptoElectronAdv

Opto-Electronic Advances

Article

November 2025, Vol. 8, No. 11

DOI: 10.29026/oea.2025.250098 CSTR: 32247.14.oea.2025.250098

Partially coherent optical chip enables physical-layer public-key encryption

Bo Wu[1], Wenkai Zhang[1], Hailong Zhou[1]*, Jianji Dong[1]*, Yilun Wang[2] and Xinliang Zhang[1]

Public-key encryption is essential for secure communications, eliminating the need for pre-shared keys. However, traditional schemes such as RSA (Rivest-Shamir-Adleman) and elliptic curve cryptography rely on computational complexity, making them increasingly susceptible to advances in computing power and algorithms. Physical-layer encryption, which leverages the intrinsic properties of physical systems, offers a promising alternative with security rooted in physics. Despite progress in this field, public-key encryption at the optical layer remains largely unexplored. Here, we propose a novel optical public-key encryption scheme based on partially coherent light sources. The cryptographic keys are encoded in the incoherent optical transmission matrix of an on-chip Mach-Zehnder interferometer mesh, providing high complexity and resilience to computational attacks. We experimentally demonstrate encrypted image transmission over 40 km of optical fiber with high decryption fidelity and achieve a 10 Gbit/s optical encryption rate using a lithium niobate photonic chip. This represents the first implementation of public-key encryption at the physical optical layer. The approach offers key advantages in security, cost, energy efficiency, and compatibility with commercial optical communication systems. By integrating public-key encryption into photonic hardware, this work opens a new direction for secure and high-speed optical communications in next-generation networks.

Keywords: public key encryption; partially coherent source; optical incoherent matrix

Wu B, Zhang WK, Zhou HL et al. Partially coherent optical chip enables physical-layer public-key encryption. *Opto-Electron Adv* **8**, 250098 (2025).

Introduction

The rapid development of digital communication and data transfer technologies has underscored the critical importance of secure encryption systems. Public-key cryptography, a cornerstone of modern security protocols, plays an indispensable role in enabling secure communication over untrusted networks. Unlike traditional symmetric-key encryption schemes, which rely on shared secret keys and suffer from limitations in key distribution and scalability, public-key encryption eliminates the need for pre-shared secrets, offering a more practical solution for many real-world applications[1].

Conventional public-key encryption algorithms, such as RSA and elliptic curve cryptography, are grounded in the computational complexity of solving certain mathematical problems, such as integer factorization or discrete logarithms[2,3]. While these schemes have been robust against traditional attacks, advances in computing power and algorithmic breakthroughs present significant risks to their long-term security[4]. This vulnerability has motivated the search for alternative encryption paradigms that are intrinsically secure and resistant to

[1]Wuhan National Laboratory for Optoelectronics, School of Optical and Electronic Information, Huazhong University of Science and Technology, Wuhan 430074, China; [2]College of Science, National University of Defense Technology, Changsha 410073, China.

*Correspondence: HL Zhou, E-mail: hailongzhou@hust.edu.cn; JJ Dong, E-mail: jjdong@hust.edu.cn

Received: 6 May 2025; Accepted: 10 September 2025; Published online: 21 November 2025

such emerging threats.

Physical-layer cryptographic schemes have emerged as an innovative response to this challenge. These approaches leverage the intrinsic properties of physical systems to achieve secure communication without solely relying on computational assumptions. Among these, optical encryption has garnered significant attention due to its ability to exploit the multiple degrees of freedom inherent in photons for encoding information. Additionally, optical encryption benefits from the advantages of large bandwidth and low power consumption, particularly over long transmission distances. Over recent decades, various optical encryption methods have been developed, including those based on metasurfaces, complex scattering media, and chaotic systems, which enhance the complexity of secret keys[5–14]. However, these methods often assume pre-shared keys, a limitation that restricts their practical application scenarios. Quantum key distribution (QKD) exploits the principles of quantum mechanics to ensure provably secure key exchange[15,16], offering a fundamentally different approach compared to classical cryptographic protocols. While QKD offers unparalleled security, it also introduces challenges related to implementation complexity and cost, limiting its widespread adoption. Despite these advances, public-key encryption schemes that exploit the unique characteristics of optical systems remain underexplored.

Partially coherent optical sources have recently attracted growing attention in information transmission, optical encryption, and optical computing due to their unique statistical properties[17–20]. Compared with fully coherent light, partially coherent beams exhibit reduced spatial coherence and inherent randomness, which can effectively suppress speckle effects and enhance robustness against environmental disturbances[21,22]. Recent studies have demonstrated their advantages in physical-layer encryption leveraging their tunable coherence and complex interference behaviors[23,24]. However, these schemes also rely on pre-shared keys, which introduces additional security requirements for key management.

Here we introduce a novel public-key encryption scheme based on partially coherent light sources. The optical incoherent transmission matrix exhibits complex, hard-to-reproduce physical characteristics and inherently conceals plaintext information, making it an ideal candidate for secure encryption. Leveraging the reciprocity of optical linear systems, we demonstrate encrypted image transmission over a 40 km optical fiber with high fidelity and an optical encryption rate of 10 Gbit/s using a lithium niobate (LN) photonic chip. To the best of our knowledge, this work represents the first implementation of a public-key encryption scheme utilizing partially coherent light, offering advantages in security, cost, energy efficiency, and operating speed while unlocking new possibilities for optical communication technologies.

Results

Principle of the optical public key encryption

The principles of public-key encryption are illustrated in Fig. 1(a). In this scheme, Alice distributes a public key through a public channel, enabling users to encrypt their plaintext (e.g., x_1, x_2…). However, the corresponding ciphertext can only be decrypted using Alice's private key. We implement this protocol at the optical layer using partially coherent sources. By leveraging the reciprocity of incoherent optical matrices, we have achieved secure key distribution in our previous work, demonstrating the system's robustness against detection attacks[25]. Here, we extend this concept to public key encryption, as depicted in Fig. 1(b). In our implementation, a partially coherent optical source, such as an amplified spontaneous emission (ASE) source, is equally divided into two orthogonal polarizations, which remain mutually incoherent. These polarizations are coupled into two separate channels of an on-chip 2×2 Mach-Zehnder interferometer (MZI) mesh via a polarization-splitting grating coupler. After undergoing matrix transformation, the optical signals are recombined using a polarization-splitting grating coupler and transmitted through a public single-mode fiber channel. The resulting optical signal in the public channel constitutes the public key. Upon reaching the recipient (Bob), the signal is processed by Bob's on-chip optical matrix. To decode the public key, Bob must train his optical matrix to equalize the intensities of the two output channels. The entire public key distribution process can be mathematically expressed as:

$$\boldsymbol{E}_{\mathrm{P}} = k\begin{pmatrix}1\\1\end{pmatrix} = |\boldsymbol{M}_2\boldsymbol{S}\boldsymbol{M}_1|^2\begin{pmatrix}1\\1\end{pmatrix}, \tag{1}$$

where $\boldsymbol{M}_1$, $\boldsymbol{S}$, and $\boldsymbol{M}_2$ represent the forward transmission matrices of Alice's MZI mesh, the public channel, and Bob's MZI mesh, respectively, and k denotes the attenuation coefficient due to link loss. Here $|\boldsymbol{M}|^2$ denotes a matrix constituted by the modulus square of each element of a matrix $\boldsymbol{M}$. For information encryption, plaintext is

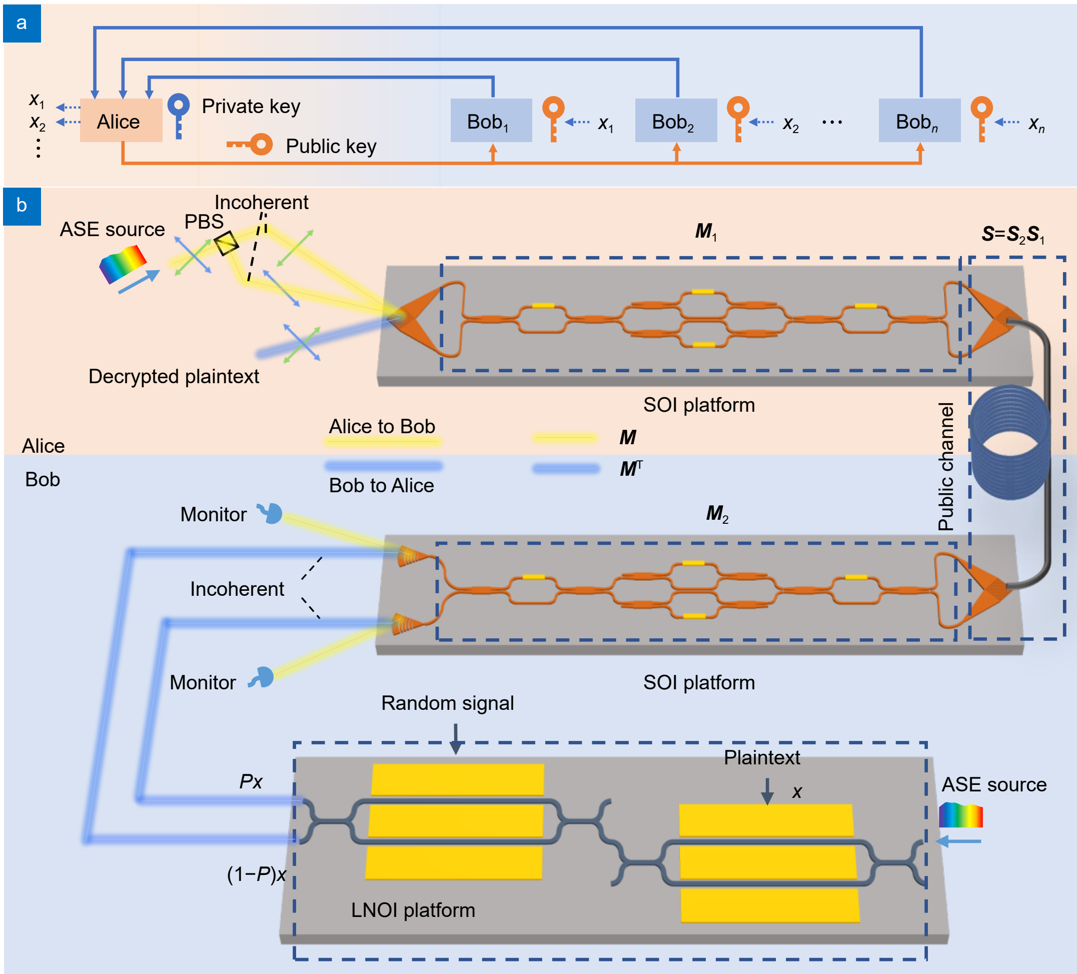

Fig. 1 | The principle of optical public-key encryption based on the incoherent reciprocal optical matrix. (**a**) An overview of the public key encryption process, where Alice distributes the public key to all users, enabling them to encrypt their plaintexts (x_1, x_2…x_n). Only Alice, who retains the private key, can decrypt the resulting ciphertext. (**b**) The practical implementation of the proposed public-key encryption scheme. Alice randomly generates an optical matrix (M_1) as her private key and transmits the public key by inputting an optical vector. Bob trains his optical matrix to produce a specific output vector and subsequently uses it to encrypt plaintext. The plaintext is encoded onto one lithium niobate on insulator modulator, while a second modulator randomly splits the input signal before it enters Bob's optical matrix. Alice detects the correct plaintext at the transmitting side using her private key. To ensure encryption security, the input optical signal to the on-chip matrix is partially coherent.

encoded onto the intensity of the partially coherent source, which is then randomly split into two mutually incoherent components. These signals propagate backward through Bob's MZI mesh, the public channel, and Alice's MZI mesh. The intensity of the backward signal output from the polarization-splitting coupler corresponds to the decrypted information. Combined with Eq. (1), the decryption can be always expressed as the scaled plaintext, given by:

$$\begin{aligned} E_{\mathrm{D}} &= \begin{pmatrix} 1 & 1 \end{pmatrix} \left| \boldsymbol{M}_1^{\mathrm{T}} \boldsymbol{S}^{\mathrm{T}} \boldsymbol{M}_2^{\mathrm{T}} \right|^2 \begin{pmatrix} P \\ 1-P \end{pmatrix} x \\ &= k \begin{pmatrix} 1 & 1 \end{pmatrix} \begin{pmatrix} P \\ 1-P \end{pmatrix} x \\ &\equiv kx, \end{aligned} \tag{2}$$

where x is the plaintext, P is the random splitting ratio, and the transposition of the transmission matrices reflects the reciprocity of the optical linear system[26]. The obtained result deviates from the plaintext information by a constant multiple, which generally does not impact the decryption process. In this case, Alice's private key (her MZI mesh) is essential for ensuring accurate decryption. The plaintext is encoded using a lithium niobate on insulator (LNOI) Mach-Zehnder modulator (MZM), with a secondary MZM cascaded as a random splitter. Due to their large bandwidth, low loss, and high linearity[27,28], LNOI modulators are ideal for information encoding in this encryption system. The random splitting signal must operate at a rate of at least the same level as the plaintext to ensure effective encryption and protect against direct detection attacks. If an eavesdropper attempts to tap into the forward and backward optical signals, they will acquire two incoherent vectors:

$$\boldsymbol{E}_{\mathrm{F}} = |\boldsymbol{S}_1\boldsymbol{M}_1|^2 \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$
$$\boldsymbol{E}_{\mathrm{B}} = \left|\boldsymbol{S}_2^{\mathrm{T}}\boldsymbol{M}_2^{\mathrm{T}}\right|^2 \begin{pmatrix} P \\ 1-P \end{pmatrix} x, \tag{3}$$

here, the transmission matrix of public channel is divided into two components ($\boldsymbol{S}_1$ and $\boldsymbol{S}_2$, where $\boldsymbol{S}$=$\boldsymbol{S}_1\boldsymbol{S}_2$) according to the eavesdropping point. The inability to derive Eq. (2) from these incoherent vectors prevents successful decryption. Fundamentally, the incoherent nature of the partially coherent source obscures the phase information of the original coherent optical matrix, which is critical for accurate decryption (see Supplementary information Section 1 for more analysis on security).

Chip fabrication and characterization

The encryption and decryption components are integrated on the same silicon photonic chip, as illustrated in Fig. 2(a). The 2×2 MZI mesh adopts a singular value decomposition-based architecture[29]. To increase encryption flexibility, two additional MZIs are placed before Bob's MZI mesh. Figure 2(b) displays the packaged chip, where the grating coupler and polarization-splitting grating coupler exhibit insertion losses of 3.69 dB and 6.7 dB, respectively. The thermal phase shifter requires 22.43 mW of power for a phase shift of π, as shown in Fig. 2(c). The plaintext encoding chip is fabricated on an LNOI platform, as depicted in Fig. 2(d). The modulator has a length of 1.1 cm, with an edge coupler insertion loss of 2 dB and a waveguide loss of 0.6 dB/cm. The packaged chip is shown in Fig. 2(e). The half-wave voltage was tested using a 50 kHz triangular-wave signal, with Fig. 2(f) presenting the measured optical transmission as a function of the applied voltage. The half-wave voltage was measured to be just 2.4 V. The bandwidth of the modulator was also characterized, as shown in Fig. 2(g). The S21 parameter demonstrates a 3 dB bandwidth of 45.5 GHz, underscoring its potential for high-speed encryption applications.

Image encryption results

Although we have demonstrated that direct detection

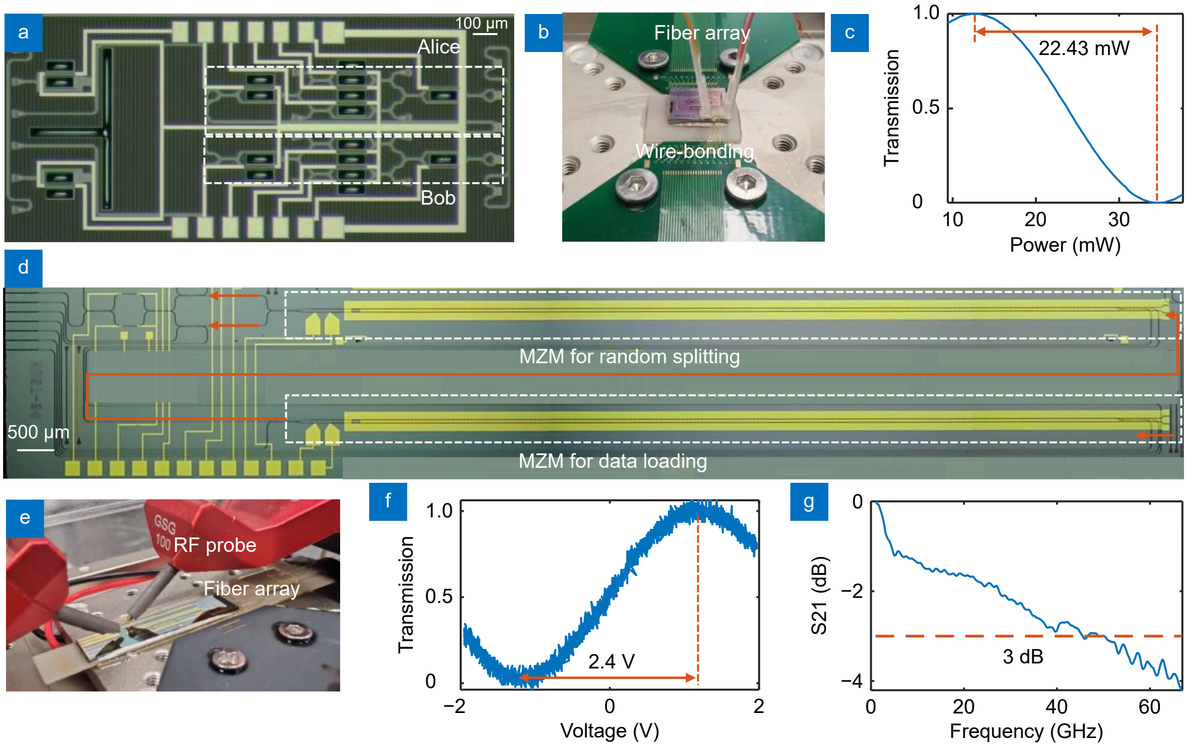

Fig. 2 | Fabrication and characterization of the chip. (**a**) The fabricated encryption and decryption chip based on silicon photonic 2×2 MZI mesh. (**b**) The encryption and decryption chip with optical and electrical package. (**c**) The transmission of thermally tuned MZI with different heating power. (**d**) The fabricated plaintext encoding chip based on LNOI MZMs. The orange arrows denote the propagation paths of the optical signals within the chip. (**e**) The plaintext encoding chip with optical and electrical package. (**f**) The intensity of output light as a function of applied voltage. (**g**) The bandwidth test of the LNOI MZM.

cannot accurately extract the plaintext, the detected light intensity in the transmission link remains statistically proportional to the plaintext, partially exposing its information. To further obscure the plaintext and enhance security probability, two pairs of coefficients are introduced to Eqs. (1) and (2):

$$\boldsymbol{E}_P = \begin{pmatrix} k_1 \\ k_2 \end{pmatrix} = |\boldsymbol{M}_2\boldsymbol{S}\boldsymbol{M}_1|^2 \begin{pmatrix} a_1 \\ a_2 \end{pmatrix},$$

$$\begin{aligned} E_{\mathrm{D}} &= \begin{pmatrix} a_1 & a_2 \end{pmatrix} \left|\boldsymbol{M}_1^{\mathrm{T}}\boldsymbol{S}^{\mathrm{T}}\boldsymbol{M}_2^{\mathrm{T}}\right|^2 \begin{pmatrix} k_2P \\ k_1(1-P) \end{pmatrix} x \\ &= \begin{pmatrix} k_1 & k_2 \end{pmatrix} \begin{pmatrix} k_2P \\ k_1(1-P) \end{pmatrix} x \equiv k_1k_2x, \end{aligned} \tag{4}$$

where, k_1 and k_2 are private to Bob, while a_1 and a_2 are private to Alice. It is important to note that the additional coefficients can be incorporated into the transmission matrix without affecting the validity or effectiveness of Eqs. (1) and (2). The coefficients a_1 and a_2 are implemented by adding a polarization controller to one of the two polarization channels of the ASE source and can be also achieved through integrated on-chip MZIs (see Supplementary information Section 2 for the experimental setup). The coefficients k_1 and k_2 are realized using the two MZIs placed before Bob's MZI mesh. Simulations revealed that optimal encryption performance and decryption fidelity are achieved when the ratios a_1/a_2 and k_1/k_2 both lie in the ranges of [6, 10] or [1/10, 1/6] (see Supplementary information Section 3 for details). In the experiment, we selected a random large ratio for a_1/a_2 and set k_1/k_2 to 1/8. The chip-to-chip transmission was conducted over a 40 km single-mode fiber with a typical loss of 8 dB. 50% of the optical power in the transmission link was tapped out and detected as ciphertext. Figure 3(a) and 3(b) illustrate the iteration of correlation coefficient between the target ratio k_1/k_2 and the measured ratio, as well as the monitored power levels at two ports during Bob's MZI mesh training (see Methods for details). Thanks to the small number of tunable phase shifters, the training process converges after only a few dozen iterations. Assuming a refresh rate of 10 kHz for the thermal phase shifters, the time required for a single iteration is approximately 1 ms, accounting for five phase shifters with two voltage updates per phase shifter. Accordingly, the total time delay is estimated to be within 100 ms. To evaluate encryption and decryption performance, 1000 random plaintexts were tested (Fig. 3(c) and Fig. 3(e)). The decrypted data show a strong correlation with the plaintext (Fig. 3(d)), while the encrypted data are scattered in the plot (Fig. 3(f)), especially for larger plaintexts. The mean square error (MSE) was used as the metric for encryption and decryption quality:

$$MSE = \frac{1}{N}\text{sum}\left[\left(\frac{\boldsymbol{p}}{\max\left(\boldsymbol{p}\right)} - \frac{\boldsymbol{d}}{\max\left(\boldsymbol{d}\right)}\right)^2\right], \tag{5}$$

where N is the length of plaintext, $\boldsymbol{p}$ is the plaintext vector, and $\boldsymbol{d}$ is encrypted or decrypted vector. The MSE ranges from 0 to 1. A smaller MSE of the decrypted data indicates higher decryption fidelity, while a larger MSE of the encrypted data reflects stronger encryption quality. The tested MSE is 8.6×10^{-4} and 5.2×10^{-2} for the decrypted and encrypted information, respectively.

As the noise induced during encryption increases significantly with larger plaintexts, while remaining nearly constant during decryption, we normalized the image to a range of 0.5 to 1 to enhance encryption performance. Figure 4 presents image encryption results for a cat face and a dog face (adopted from Animal Faces-HQ dataset[30]). The encrypted images are virtually indistinguishable, while the main features are preserved in the decrypted images. The MSE values are 6.5×10^{-5}, 5.9×10^{-2}, 2.8×10^{-5}, and 8.2×10^{-2} for the decrypted cat, encrypted cat, decrypted dog, and encrypted dog, respectively. The results demonstrate that both encryption and decryption are achieved with high fidelity in our system.

Finally, we evaluated the high-speed performance of the proposed encryption system (Fig. 5). A bit pattern generator was used to produce a 9.95 GHz plaintext signal (OOK format), which was loaded onto the first LNOI MZM. A microwave source generating a 7.2 GHz electrical sinusoidal signal modulated the second MZM to create random light splitting. The waveform and frequency of the driving signal are carefully selected to maximize the randomness of the optical power splitting. When only the plaintext signal was applied, both the eavesdropper and Alice were able to obtain a clear eye diagram. However, due to the higher loss of the optical signal after an additional chip, the signal intensity observed by Alice was significantly lower than that of the eavesdropper, resulting in a lower extinction ratio in Alice's eye diagram after optical amplification. Replacing the grating coupler with edge coupler might lower the link loss and improve the signal quality after decryption[31]. Notably, both diagrams still represented the plaintext without encryption. Upon applying the sinusoidal splitting signal, the plaintext became encrypted. The eavesdropper could no longer retrieve a clear eye diagram, while Alice's decrypted signal remained nearly unaffected. This

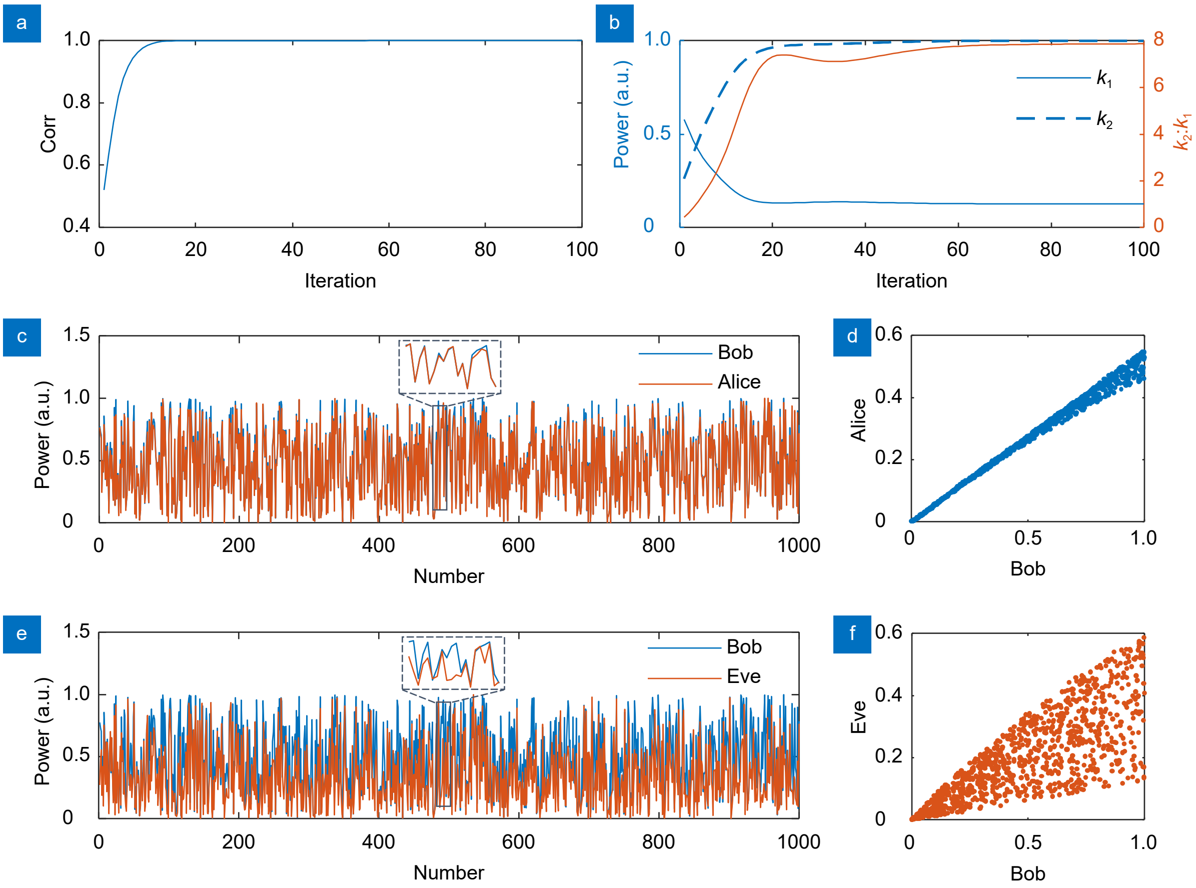

Fig. 3 | (**a**) The iteration curve of the correlation during the training of Bob's MZI mesh. (**b**) The evolution of the power of the two monitor ports. (**c**) The decrypted plaintext by Alice with 1000 random plaintexts between 0 and 1. (**d**) The scattering plot of the data in (c). (**e**) The derived information by eavesdropper with direction detection. (**f**) The scattering plot of the data in (e).

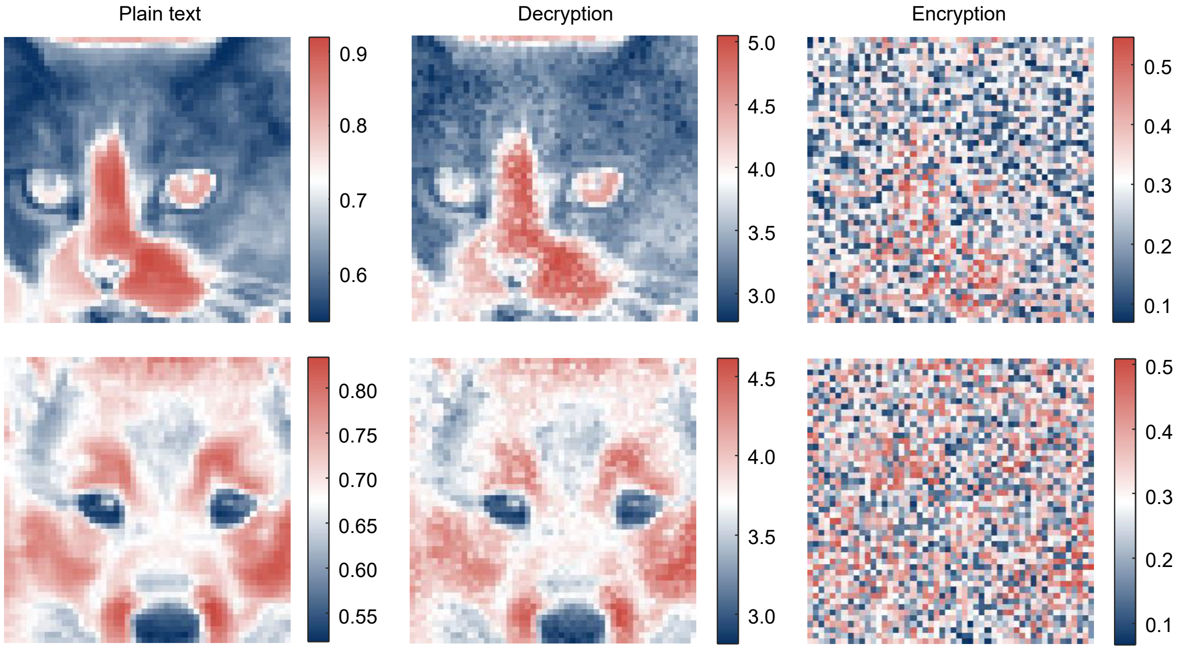

Fig. 4 | The image encryption results of our experiment system.

demonstrates successful encryption and decryption under high-speed transmission conditions. Results for 1.24 Gbit/s and 4.98 Gbit/s transmission are provided in Supplementary information Section 4.

Discussion

The proposed optical encryption scheme demonstrates significant advantages over other physical-layer encryption methods in terms of security, cost, energy efficiency, and speed. Unlike schemes that require pre-shared information, such as the synchronization of chaos sources in chaos-based encryption[5], our scheme is fully private to users, relying solely on knowledge of the basic protocol. Security is guaranteed by the reciprocity of the optical matrix and the intrinsic characteristics of the partially coherent optical source, providing a robust advantage in safeguarding communications. Additionally, the use of a partially coherent optical source simplifies system design and operation compared to the narrow-linewidth lasers or quantum sources required by other schemes. This simplification significantly reduces the cost associated with source generation and detection[18]. Furthermore, encryption and decryption are performed entirely in the optical domain, ensuring full compatibility with commercial optical fiber communication systems. This compatibility minimizes electrical energy consumption and latency while enabling ultrafast encryption speeds, positioning the system as a highly efficient and practical solution for secure communication[32].

Optical transmission networks further enhance the proposed scheme by offering advanced multiplexing capabilities. The wavelength multiplexing capability, in particular, has the potential to enable parallel encryption in our proposed scheme, as shown in Fig. 6. Specifically, Alice can utilize an ultra-broadband ASE source to distribute multiple public keys simultaneously across different wavelength bands. Each user would encrypt their plaintext using a designated wavelength band, while Alice could recover the decrypted information using a demultiplexer. For instance, by leveraging the C+L band (1530–1625 nm) and allocating a 10 nm bandwidth per user, the system could support up to 10 parallel channels for public key encryption. Given that the encryption speed is 10 Gbit/s per channel, the system can achieve an equivalent encryption rate of up to 100 Gbit/s, demonstrating significant potential for large-capacity encryption.

System stability is another critical consideration. Environmental fluctuations—such as temperature drift, mechanical vibration, and component aging—can perturb the transmission matrix, impacting the encryption key. A key strength of our approach lies in its ability to perform real-time key calibration, independent of the data channel (as illustrated in Fig. 1(b)). This enables continuous public key updates without interrupting encrypted communication, ensuring operational robustness under dynamic conditions.

The difficulty for an adversary to infer the private key

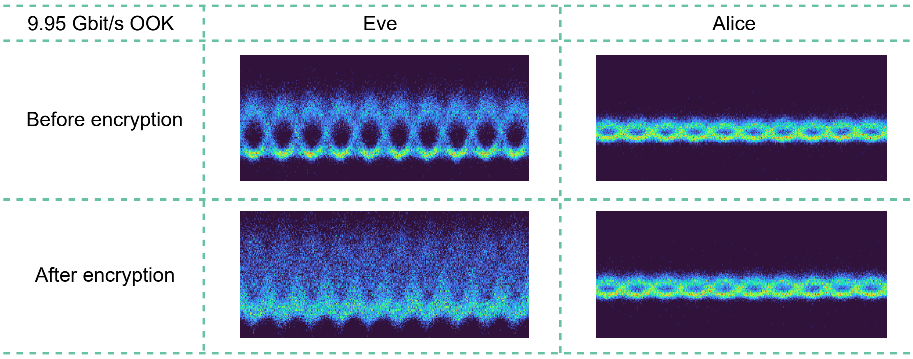

Fig. 5 | Eye diagrams of 9.95 Gbit/s OOK signal before and after encryption.

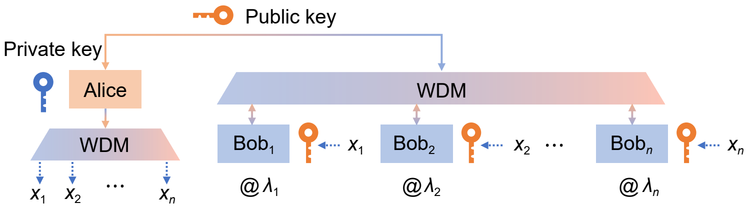

Fig. 6 | The parallel optical encryption enabled by wavelength multiplexing technology. WDM, wavelength division multiplexer.

is determined by the system's key space. We estimate the key space based on the degrees of freedom in Alice's 2×2 complex valued optical matrix, excluding global phase and amplitude, yielding six independent parameters. Assuming 8 quantized levels per parameter, the key space is 8^6=262144. Although this is a conservative estimate for a proof-of-concept demonstration, significantly larger key spaces can be achieved by adopting higher-dimensional matrices —e.g., using spatial dimensions in multi-core fibers as optical information carriers.

The energy consumption of the proposed scheme primarily originates from the ASE source, optical modulator, and thermal phase shifters. Assuming an electrical root-mean-square voltage of V_{rms}=1 V for the modulator, its power consumption is estimated as V_{rms}^2/50 Ω=20 mW. The total power consumption can be calculated as: P=P_{S} (ASE source)+P_{MOD} (modulator)+P_{PS} (phase shifter)=200 mW+2×20 mW+12×22.4 mW=508.8 mW. Given an encryption rate of 10 Gbit/s, the corresponding energy efficiency is: P/10 Gbit/s=50.88 pJ/bit. This energy efficiency can be further improved by reducing transmission losses and increasing the tuning efficiency of the phase shifters.

Several factors currently limit encryption speed and transmission distance. Chromatic dispersion, for instance, introduces a trade-off between rate and range. Our 10 Gbit/s experiment was conducted over a 1 m fiber to exhibit the core encryption functionality. For long-haul applications, dispersion can be mitigated using conventional solutions such as dispersion-compensating fibers or operating at the O-band zero-dispersion point. Data rate is also constrained by the modulation and detection bandwidths, but with modern devices exceeding 100 GHz[33,34], there is significant potential for higher rates. Link loss is another limiting factor, as it degrades the signal-to-noise ratio and thus increases the decryption mean square error. A clear roadmap exists for future improvements. At the component level, replacing high-loss polarization-splitting grating couplers with edge couplers and integrated polarization splitter and rotator will reduce insertion losses and enhance overall efficiency[31,35]. At the system level, the future heterogeneous integration of the LNOI modulation and silicon encryption stages onto a single chip will eliminate chip-to-chip coupling losses and significantly improve the overall power budget[36].

Conclusion

In conclusion, we introduced a groundbreaking public-key encryption scheme leveraging the physical properties of partially coherent light sources. Unlike conventional cryptographic approaches that rely on computational complexity, our method exploits the reciprocal and incoherent characteristics of optical systems to achieve secure encryption at the physical layer. This approach inherently addresses vulnerabilities associated with traditional encryption schemes, such as susceptibility to quantum computing attacks, by shifting the foundation of security to the optical domain. Compared to existing physical-layer cryptographic methods, our scheme offers a distinct advantage by utilizing the unique capabilities of photonic systems, such as compatibility with high-bandwidth optical communication networks and the intrinsic randomness of light's coherence properties. We demonstrated high encryption security and a transmission rate of 10 Gbit/s using a highly integrated photonic chip. By bridging the gap between optics and cryptography, this work paves the way for innovative solutions to the pressing challenges of secure communication in the digital era.

Methods

Optical matrix training algorithm

We use the gradient descent algorithm to train the Bob's MZI mesh, aiming to maximize the correlation between the target ratio of k_1/k_2 and the measured ratio by optimizing the voltages applied to the thermal phase shifters. The correlation is defined as the cosine of the angle between the target vector $[k_1\ k_2]$ and measured power vector. The detailed training process is as follows:

1) Initialization: randomly initialize the voltages applied to the thermal phase shifters.

2) Gradient approximation:

- Increment the voltage by 0.05 V for each thermal phase shifter and calculate the corresponding correlation Corr(U+0.05).
- Decrement the voltage by 0.05 V for each thermal phase shifter and calculate the correlation Corr(U–0.05).
- Estimate the approximate gradient of the correlation using the formula:

$$G=\frac{\mathrm{Corr}(U+0.05)-\mathrm{Corr}(U-0.05)}{0.1}. \tag{6}$$

3) Voltage update: update the voltages using the Adam algorithm, a fast-converging gradient descent method, as described by the formula[37]:

$$\begin{aligned} U(\text{iter}+1) =& U(\text{iter}) + \alpha\left(v_{\text{iter}}/(1-\beta_1{}^{\text{iter}})\right) \\ & /\sqrt{s_{\text{iter}}/(1-\beta_2{}^{\text{iter}})} + \varepsilon, \\ v_{\text{iter}} =& \beta_1 v_{\text{iter}-1} + (1-\beta_1)G, \\ s_{\text{iter}} =& \beta_2 s_{\text{iter}-1} + (1-\beta_2)G^2, \end{aligned} \tag{7}$$

where iter is the current iteration number, α is the learning rate which is set to 0.05 during training, β_1, β_2, and ε are hyperparameters set to 0.9, 0.999, and 10^{-8}, respectively. The initial values of v_{iter} and s_{iter} are zero.

4) Iteration: repeat steps 2) and 3) until the correlation converges.

5) Save optimized parameters: once the training is complete, save the optimized voltages for deployment.

Experiment methods

The silicon photonic chip was fabricated using a 200 mm CMOS process line, with a silicon thickness of 220 nm. The plaintext encoding chip was developed on a 4-inch silicon-based thin-film lithium niobate wafer, featuring a lithium niobate thickness of 600 nm and a rib waveguide etching depth of 300 nm. The modulator incorporates a traveling-wave gold electrode, and the electrical signal is applied to the Mach-Zehnder Modulator (MZM) using a 40 GHz RF probe. A triangular-wave signal, generated by an arbitrary waveform generator (GIGOL DG4202), was employed to evaluate the modulation efficiency of the MZM. The bias point was set at the center of the linear region, with the frequency fixed at 50 kHz. The output optical signal was detected using a 200 MHz photodetector and compared with the driving signal by oscilloscope (GIGOL DS4022). The modulator's bandwidth was characterized using a 67 GHz vector network analyzer. Eye diagrams of the plaintext, encrypted, and decrypted signals were recorded using a bit pattern generator (SHF BPG 44 E), a microwave generator (Sinolink SLFS24C), an 18 GHz bandwidth photodetector, and an oscilloscope (Tektronix DSA72004B). Thermal phase shifters and the MZM bias voltage were driven by a digital-to-analog converter (LTC2688) controlled via a field-programmable gate array (FPGA) chip (7K325T). The experimental setup was managed through a personal computer via serial ports, while the chip was thermally stabilized using a thermoelectric cooler (TEC).

References

1. Diffie W, Hellman M. New directions in cryptography. *IEEE Trans Inf Theory* **22**, 644–654 (1976).
2. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Commun ACM* **21**, 120–126 (1978).
3. Ahlswede R. Elliptic curve cryptosystems. In Ahlswede R. *Hiding Data - Selected Topics: Rudolf Ahlswede's Lectures on Information Theory 3* 225–336 (Springer, Cham, 2016).
4. Scarani V, Bechmann-Pasquinucci H, Cerf NJ et al. The security of practical quantum key distribution. *Rev Mod Phys* **81**, 1301–1350 (2009).
5. Gao H, Wang AB, Wang LS et al. 0.75 Gbit/s high-speed classical key distribution with mode-shift keying chaos synchronization of Fabry-Perot lasers. *Light Sci Appl* **10**, 172 (2021).
6. Qu GY, Yang WH, Song QH et al. Reprogrammable meta-hologram for optical encryption. *Nat Commun* **11**, 5484 (2020).
7. Bian LH, Chang XY, Jiang SW et al. Large-scale scattering-augmented optical encryption. *Nat Commun* **15**, 9807 (2024).
8. Guo XY, Li P, Zhong JZ et al. Stokes meta-hologram toward optical cryptography. *Nat Commun* **13**, 6687 (2022).
9. Zhang F, Guo YH, Pu MB et al. Meta-optics empowered vector visual cryptography for high security and rapid decryption. *Nat Commun* **14**, 1946 (2023).
10. Ji JT, Chen C, Sun JC et al. High-dimensional Poincaré beams generated through cascaded metasurfaces for high-security optical encryption. *PhotoniX* **5**, 13 (2024).
11. Liu YL, Dong Z, Zhu YM et al. Three-channel robust optical encryption via engineering coherence Stokes vector of partially coherent light. *PhotoniX* **5**, 8 (2024).
12. Sun S, Gou Y, Cui TJ et al. High-security nondeterministic encryption communication based on spin-space-frequency multiplexing metasurface. *PhotoniX* **5**, 38 (2024).
13. Yu ZP, Li HH, Zhao WN et al. High-security learning-based optical encryption assisted by disordered metasurface. *Nat Commun* **15**, 2607 (2024).
14. Wang AB, Wang JL, Jiang L et al. Experimental demonstration of 8190-km long-haul semiconductor-laser chaos synchronization induced by digital optical communication signal. *Light Sci Appl* **14**, 40 (2025).
15. Li W, Zhang LK, Tan H et al. High-rate quantum key distribution exceeding 110 Mb·s^{-1}. *Nat Photonics* **17**, 416–421 (2023).
16. Zheng XD, Zhang PY, Ge RY et al. Heterogeneously integrated, superconducting silicon-photonic platform for measurement-device-independent quantum key distribution. *Adv Photonics* **3**, 055002 (2021).
17. Yu JY, Zhu XL, Wang F et al. Research progress on manipulating spatial coherence structure of light beam and its applications. *Prog Quantum Electron* **91–92**, 100486 (2023).
18. Dong BW, Brückerhoff-Plückelmann F, Meyer L et al. Partial coherence enhances parallelized photonic computing. *Nature* **632**, 55–62 (2024).
19. Brückerhoff-Plückelmann F, Borras H, Klein B et al. Probabilistic photonic computing with chaotic light. *Nat Commun* **15**, 10445 (2024).
20. Brückerhoff-Plückelmann F, Ovvyan AP, Varri A et al. Probabilistic photonic computing for AI. *Nat Comput Sci* **5**, 377–387 (2025).
21. Wang YK, Gu KX, Dong Z et al. Generation of partially coherent full Poincaré beam arrays and their Stokes scintillations in turbulent media. *Appl Phys Lett* **125**, 171102 (2024).
22. Peng YF, Choi S, Kim J et al. Speckle-free holography with partially coherent light sources and camera-in-the-loop calibration. *Sci Adv* **7**, eabg5040 (2021).

23. Liu YL, Dai ST, Zhu YM et al. Full-dimensional complex coherence properties tomography for multi-cipher information security. *Opto-Electron Adv* **8**, 240278 (2025).
24. Peng DM, Huang ZF, Liu YL et al. Optical coherence encryption with structured random light. *PhotoniX* **2**, 6 (2021).
25. Wu B, Zhou HL, Dong JJ et al. Chip-encoded high-security classical optical key distribution. *Nanophotonics* **13**, 3717–3725 (2024).
26. Potton RJ. Reciprocity in optics. *Rep Prog Phys* **67**, 717–754 (2004).
27. Feng HK, Ge T, Guo XQ et al. Integrated lithium niobate microwave photonic processing engine. *Nature* **627**, 80–87 (2024).
28. Wang C, Zhang M, Chen X et al. Integrated lithium niobate electro-optic modulators operating at CMOS-compatible voltages. *Nature* **562**, 101–104 (2018).
29. Wu B, Zhou HL, Dong JJ et al. Programmable integrated photonic coherent matrix: principle, configuring, and applications. *Appl Phys Rev* **11**, 011309 (2024).
30. Choi Y, Uh Y, Yoo J et al. StarGAN v2: diverse image synthesis for multiple domains. In *Proceedings of 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition* 8185–8194 (IEEE, 2020). http://doi.org/10.1109/CVPR42600.2020.00821.
31. Marchetti R, Lacava C, Carroll L et al. Coupling strategies for silicon photonics integrated chips [Invited]. *Photonics Res* **7**, 201–239 (2019).
32. Wu B, Zhang WK, Zhou HL et al. Chip-to-chip optical multimode communication with universal mode processors. *PhotoniX* **4**, 37 (2023).
33. Hu YW, Zhu D, Lu SY et al. Integrated electro-optics on thin-film lithium niobate. *Nat Rev Phys* **7**, 237–254 (2025).
34. Lischke S, Peczek A, Morgan JS et al. Ultra-fast germanium photodiode with 3-dB bandwidth of 265 GHz. *Nat Photonics* **15**, 925–931 (2021).
35. Sacher WD, Barwicz T, Taylor BJF et al. Polarization rotator-splitters in standard active silicon photonics platforms. *Opt Express* **22**, 3777–3786 (2014).
36. He MB, Xu MY, Ren YX et al. High-performance hybrid silicon and lithium niobate Mach-Zehnder modulators for 100 Gbit·s^{-1} and beyond. *Nat Photonics* **13**, 359–364 (2019).
37. Kingma DP, Ba J. Adam: a method for stochastic optimization. In *Proceedings of the 3rd International Conference on Learning Representations* (2015).

Acknowledgements

The work was supported by the Fundamental Research Funds for the Central Universities. National Natural Science Foundation of China (62425504, U21A20511, 62275088).

Author contributions

B. W., H. L. Z., and J. J. D. conceived the idea. B. W. and W. K. Z. designed and fabricated the chip. B. W. carried out theoretical analysis and simulation. B. W. and W. K. Z. designed and performed the experiments. H. L. Z., J. J. D., and B. W. discussed and analyzed data. B. W. prepared the manuscript. H. L. Z. and J. J. D. revised the paper and X. L. Z. supervised the project. All authors contributed to the writing of the manuscript.

Competing interests

The authors declare no competing financial interests.

Supplementary information

Supplementary information for this paper is available at https://doi.org/10.29026/oea.2025.250098