Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Quantum-resilient optical links using micro-LEDs generated quantum random numbers and physical unclonable functions

Tien Khee Ng
tienkhee.ng@kaust.edu.sa
King Abdullah University of Science and Technology https://orcid.org/0000-0002-1480-6975
Heming Lin
King Abdullah University of Science and Technology https://orcid.org/0009-0004-6108-6589
Wenqing Niu
King Abdullah University of Science and Technology
Tae Yong Park
King Abdullah University of Science and Technology
Hang Lu
King Abdullah University of Science and Technology
Zhican Zhou
Integrated Photonics Lab, King Abdullah University of Science and Technology (KAUST)
Yating Wan
Integrated Photonics Lab, King Abdullah University of Science and Technology (KAUST)
Boon Ooi
King Abdullah University of Science and Technology https://orcid.org/0000-0001-9606-5578

Article

Keywords: micro-LED, PUF, QRNG, OWC, PQC, IoT

Posted Date: March 4th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-8729181/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License

Additional Declarations: There is **NO** Competing Interest.

Research article

Quantum-resilient optical links using micro-LEDs generated quantum random numbers and physical unclonable functions

Heming Lin[1], Wenqing Niu[1], Taeyong Park[1, 3], Hang Lu[1], Zhican Zhou[1], Yating Wan[1], Tien Khee Ng[1, *], Boon S. Ooi[1, 2, *]

[1] *Electrical and Computer Engineering Department, Computer Electrical and Mathematical Sciences and Engineering Division*, *King Abdullah University of Science and Technology (KAUST), Thuwal 23955-6900, Saudi Arabia*

[2]*Department of Electrical, Computer, and Systems Engineering, Rensselaer Polytechnic Institute, Troy, NY, USA*

[3]*Korea Institute of Ceramic Engineering and Technology (KICET), Jinju, Republic of Korea*

[*] Corresponding Author

Email: tienkhee.ng@kaust.edu.sa, boon.ooi@kaust.edu.sa, ooib@rpi.edu

Abstract

Secure communication in Internet-of-Things (IoT) systems typically rely on separate hardware elements for key generation, device authentication, and data transmission, complicating scalable integration. Here we demonstrate that micro-LEDs can integrate all three capabilities, reducing energy and footprint overheads and avoiding exposure to additional attack surfaces. Notably, fabrication-induced structural variations can generate stable, device-unique near-field emission patterns that serve as optoelectronic physical unclonable functions (PUFs), while spontaneous-emission noise can provide a quantum-origin entropy source for quantum random number generators (QRNGs). Through min-entropy evaluation and post-processing, a single micro-LED delivers a stable QRNG throughput of 13.25 Gb/s. Using a deep-neural-network-assisted extractor, each device yields reproducible 256-bit keys, with intra- and inter-device Hamming distances separated by more than an order of magnitude. Integrated into a post-quantum cryptographic framework, the micro-LED functions as a self-contained secure transmitter, enabling authenticated and encrypted free-space optical wireless communication at 1.97 Gb/s. In principle, the security mechanisms are wavelength-independent and extendable across material platforms. Together, these results establish a quantum-resilient photonic node that consolidates transmission, identity, and randomness at the edge device level, providing a scalable hardware building block for secure, low-power connectivity in future IoT networks.

KEYWORDS: micro-LED, PUF, QRNG, OWC, PQC, IoT

Main

The rapid proliferation of interconnected devices is driving a growing demand for secure, low-power and scalable communication links, particularly at the edges of emerging Internet-of-Things (IoT) networks. Many IoT devices process sensitive data and control information while offering limited intrinsic security. Recent large-scale breaches highlight the vulnerability of these systems, with a single incident reported in 2025 compromising approximately 2.7 billion IoT records[1]. Industry analyses further report that 34% of IoT-related breaches incur losses between USD 5 million and 10 million, markedly higher than typical IT security failures[2,3]. These trends indicate the need for robust and hardware-anchored protection of data exchanged between IoT nodes. Post-quantum cryptography (PQC) offers algorithmic protection against quantum adversaries and practical compatibility with lightweight, hardware-constrained platforms. However, its practical deployment ultimately relies on hardware that can provide trustworthy entropy, device authentication, and high-speed data transmission within compact form factors[4–6]. Existing implementations often rely on separate modules for true random number generators (TRNGs), physical unclonable functions (PUFs), and wireless transceivers, increasing system complexity and exposing interfaces that can become security liabilities[7–15]. Moreover, many CMOS-based PUF–TRNG solutions rely on correlated entropy sources, such that compromising one function can significantly increase the exposure of the other, thereby limiting robustness in adversarial settings and constraining scalability for dense IoT deployments[16–18].

Micro-LEDs have recently emerged as an attractive component for optical wireless communication (OWC) and high-speed interconnection due to their high stability, energy efficiency, and amenability to array-level integration[19–22]. Beyond their role as transmitters, micro-LEDs inherently exhibit two distinct forms of physical randomness. Temporal fluctuations originating from spontaneous emission provide a high-quality entropy source for quantum random number generator (QRNG)[23]. In parallel, fabrication-induced structural variations imprint stable, device-unique near-field emission patterns, enabling micro-LEDs to function as natural PUFs. Integrating data transmission, device authentication and high-entropy key generation within micro-LEDs platform offer a compelling route to reducing trust boundaries, interface attack surfaces and system overheads; however, previous work has largely focused on micro-LEDs as transmitters, leaving the simultaneous exploitation of their quantum and structural randomness for security largely unexplored.

Here we introduce a multifunctional micro-LED platform that unifies QRNG, PUF-based identification, and quantum-resilient optical transmission. The spontaneous-emission noise supports high-throughput QRNG with a generation rate exceeding 13 Gb/s, while the near-field electroluminescence (EL) patterns serve as reliable optical fingerprints. Using a neural-network-assisted extractor, each micro-LED is mapped to a stable 256-bit identity. These physical-layer primitives are combined with lightweight PQC protocols to enable authenticated and quantum-resilient free-space communication. We demonstrate a secure OWC link delivering up to 1.97 Gb/s using a micro-LED transmitter; and propose a chip-scale architecture that co-integrates micro-LED arrays, photodetectors (PDs) and electronics to form compact, energy-efficient secure nodes for IoT meshes. This work positions micro-LEDs as a unified building block for next-generation quantum-resilient optical communication.

3-in-1 functionality system based on micro-LED

The micro-LED-based platform integrates high-speed QRNGs, AI-assisted PUFs, and direct-modulation optical links to form a compact and flexible building block for quantum-resilient IoT meshes and can be integrated into existing micro-LED-enabled devices with minimal system modification (Fig. 1a). The micro-LEDs were fabricated on m-plane GaN-on-sapphire wafers, featuring a circular geometry with a 30-μm emission aperture to eliminate the current crowding effect and a cross-shaped p-metal contact on the top surface for uniform current injection across the aperture. The QRNG extracts entropy from the fundamentally quantum-originated intensity fluctuations associated with spontaneous emission in the micro-LED, which impose irreducible temporal noise on the emitted optical intensity. In parallel, the PUF signature originates from stochastic material and structural inhomogeneities introduced during epitaxial growth and subsequent device fabrication. Under electrical injection, these microscopic variations manifest as stable yet device-specific near-field EL patterns, effectively amplifying the underlying disorder. Together, these quantum and fabrication-derived processes offer two independent and physically distinct channels for secure key generation. Coupling micro-LED entropy sources with OWC enables a physically anchored, secure optical wireless channel capable of sustaining high throughput encrypted communication.

Figure 1b illustrates both the inter-device variability and the intra-device stability across different injection currents

and environmental temperatures, whereas Supplementary Fig. 3e further characterizes the thermal robustness from 20 to 80°C, confirming the reproducibility of the PUF responses under practical operating conditions. The zero-mean normalized cross-correlation (ZNCC) analysis quantitatively evaluates the similarity of images obtained from the same micro-LED and discriminates them from those originating from different devices. AI-assisted feature extraction further stabilizes the PUF output, ensuring reliable device fingerprints. The power spectral density (PSD) of the whole measurement system when a micro-LED is illuminated under 10 mA injection current or off is illustrated in Fig. 1c. LED noises from micro-LED EL emission dominates aggregate noises. The roll-off of both aggregate noises and background noises observed at 1000 MHz is attributed to the limited bandwidth of the PD. Below this cutoff, the normalized RF spectrum remains flat, demonstrating that the detected aggregate noise closely approximates white noise, which ensures uniform entropy distribution across the bandwidth and facilitates efficient quantum random number extraction. When combined with post-quantum cryptographic (PQC) algorithm, the PUF- and QRNG-derived entropy enables the micro-LED to operate as a secure optical node within distributed IoT meshes. Rather than replacing higher-layer cryptography, these physical-layer functions supply device-specific authentication and fresh key material, strengthening end-to-end trust without compromising the compactness or energy efficiency required for portable IoT hardware. This integration highlights a practical route for embedding robust entropy sources directly into optoelectronic transmitters, supporting secure device pairing, autonomous node onboarding, and rapid session-key refresh in large-scale IoT deployments.

High throughput quantum random number generation

To extract quantum random numbers from the micro-LED, a high-speed PD and a real-time oscilloscope were employed to capture and digitize the intrinsic intensity fluctuations, as illustrated in Fig. 2a. Under constant DC injection, the optical output is characterized by a stable mean power accompanied by intrinsic intensity fluctuations. These fluctuations arise from the discreteness of spontaneous emission: photon-generation events occur stochastically with quantum-mechanical transition probabilities between electronic states, reflecting the inherent quantum uncertainty of photon emission. The resulting photon-flux variations are transduced by the photodetector into voltage noise. A detailed derivation linking spontaneous emission statistics to the measured voltage noise is provided in Supplementary Section 2.

Based on the measured PSD, the spectral noise of the LED source remains above the background noise level up to approximately 1.5 GHz (the APD has a −3 dB bandwidth of 1 GHz with a usable frequency response up to 1.6 GHz). To guarantee complete retrieval of the quantum noise contribution while reducing quantization errors, the sampling rate was chosen to slightly exceed the Nyquist criterion ($f_s > 2B$) for a 1.5 GHz quantum-noise bandwidth to avoid aliasing, resulting in a digitization rate of 3.125 Gsa·s^{-1}. Following data acquisition, a band-pass filter (BPF) with frequency range from 100 MHz to 1.5 GHz was employed to suppress low-frequency noise (e.g., 1/f noise, power-supply ripple, and thermal or mechanical drifts) and maintain the spectral purity of the quantum noise[24,25]. To mitigate temporal correlation arising from finite detection bandwidth and sampling, post-processing algorithms including

Toeplitz Hash function and multi-delay XOR-based whitening are applied to further extract randomness as illustrated in Fig. 2b[26]. The min-entropy of the raw bits is evaluated to guide a 256-bit Toeplitz hash, which extracts nearly uniform random sequences from the intrinsic entropy and ensures stable output. Figure 2c summarizes the NIST SP 800-22 randomness tests on the 1800 × 1 million random bits extracted from 9 micro-LEDs with injection currents from 10 to 30 mA and operation temperatures from 20 to 80 °C[27]. The NIST test and Dieharder test (Supplementary Section 4) results demonstrate that the QRNG output has excellent statical randomness[28].

Figures 2d and 2g compare the estimated 8-bit min-entropy of the raw bitstream with that of the post-processed output by the formula $H_{min}(X) = -\log_2\left(\max_{x\in[0,255]} \hat{P}(X=x)\right)$, where X denotes the 8-bit digitized sample and $\hat{P}(X=x)$ is the empirically estimated probability of observing symbol x. This definition quantifies the predictability of the digitized output by considering the most probable symbol. Owing to the Gaussian-like distribution of the sampled noise, the raw bits exhibit a normalized min-entropy ranging from 0.72 to 0.75 per bit, corresponding to 5.76 to 6 bits of entropy for each 8-bit sample. After applying the Toeplitz hash function, the min-entropy of the processed bits increases to values exceeding 0.997 per bit, indicating a near-ideal entropy level of the extracted random numbers across different injection currents and operating temperatures. The autocorrelation results are summarized in Fig. 2e and 2h. Owing to the different sample lengths used for the raw and processed bitstreams, the corresponding 95% confidence intervals (CI) are ±0.00054 and ±0.000197, respectively. For the raw bits, 13.9% of the autocorrelation values exceed the confidence bounds, indicating residual temporal correlations arising from practical sampling and electronic effects. After post-processing, only 4.95% of the autocorrelation values fall outside the CI, confirming the effective decorrelation in the extracted random bits. Figures 2f and 2i quantify the similarity of the extracted bitstreams using the Hamming distance. Figure 2f compares output generated by different micro-LEDs operated across a range of driving conditions, revealing consistently low similarity between devices. Figure 2i evaluates repeated bitstreams produced by the same device under identical operating conditions over time, and likewise shows low similarity between successive outputs. Together, these results indicate that the processed QRNG sequences exhibit minimal inter-device overlaps and negligible temporal repeatability, consistent with an intrinsically unpredictable and unbiased entropy source.

At a sampling rate of 3.125 Gsa·s^{-1} and a per-bit min-entropy exceeding 0.72 for the raw bitstream, the micro-LED-based QRNG achieves a physical entropy throughput exceeding 18 Gb·s^{-1} over a wide operating window, with temperatures ranging from 20 to 80 °C and injection currents between 10 and 30 mA. While classical noise contributions are susceptible to external manipulation or information leakage, we further assess the entropy of the raw bitstream using the NIST SP 800-90B framework to obtain a conservative lower bound. This evaluation yields a worst-case min-entropy $H_{min}^{90B} = 0.53$ per bit, corresponding to a guaranteed quantum random-bit generation rate of 13.25 Gb·s^{-1}. When operated at an injection current of 10 mA, the corresponding energy consumption at the micro-LED side is calculated to be 3.7 pJ·bit^{-1}.

A physics-based noise decomposition (Supplementary section 2 and Supplementary Fig. 2c) reveals that the quantum noise contribution reaches up to 52% of the total detected fluctuations when operating at 57 mA injection current (63% after background subtraction). Supplementary Figure. 2b shows that the measured noise exhibits no discernible quadratic dependence on optical power, indicating that the fluctuations are not dominated by relative intensity noise (RIN). Instead, the noise scales linearly with optical power, consistent with shot-noise-limited detection. Within the derived model, increasing the optical power incident onto the PD enhances the fractional contribution of quantum noise when detector saturation and non-linearities are avoided.

AI-enhanced near-field emission-based PUF

Figure 4a schematically depicts the AI-enhanced, image-based PUF architecture for secure device identification. An array of micro-LEDs is fabricated, and their near-field emission patterns are recorded at manufacture. These images are augmented and used to train a ResNet34-based deep learning model to capture the intrinsic device-specific features encoded within the PUF[29]. The trained model is subsequently embedded within isolated computing hardware to enable secure authentication. During verification, selected micro-LEDs are illuminated according to a challenge, and the resulting near-field emission patterns are captured and processed to retrieve the corresponding cryptographic key from the isolated hardware. This approach yields a PUF with high inter-device uniqueness and strong temporal and environmental stability, providing robust resistance against cloning and unauthorized access.

To support reliable key extraction under practical imaging conditions, we developed a deep-learning architecture tailored to the spatial characteristics of micro-LED EL patterns (Fig. 3b). Wide-field images are localized using a computer vision model YOLOv8 and cropped into device-specific regions, followed by geometric normalization performed through a Spatial Transformer Network (STN), which mitigates tilt, displacement and optical distortions[30,31]. The stabilized patches are processed by a ResNet34 backbone augmented with Convolutional Block Attention Modules (CBAMs), enabling the model to emphasize subtle, device-unique spatial features while suppressing illumination-dependent variations[32].

To evaluate the suitability of micro-LEDs as physical unclonable functions (PUFs), we investigated an array of nine individual devices. For each micro-LED, near-field EL images were acquired under injection currents ranging from 10 to 30 mA and operating temperatures between 20 and 50 °C, yielding a total of 1,800 images per device. The dataset was augmented to improve robustness against variations in imaging conditions. For each device class, 1,440 images were used for training, and the remaining 360 images were reserved for testing, enabling a systematic assessment of intra-device stability and inter-device distinguishability under realistic operating conditions. The network converges reliably and achieves near-perfect identification accuracy on test sets (Fig. 3c, d), confirming that the micro-LED near-field emission images provide strongly device-specific optical signatures. The learned feature space forms clearly separated device clusters (Fig. 3e), reflecting tight intra-device consistency and large inter-device variability. A quantitative analysis of the 256-bit embeddings shows that the mean intra-class Hamming distance remains low

(0.053), whereas the inter-class distance exceeds 0.53 (Fig. 3f), differing by more than an order of magnitude. This substantial statistical margin demonstrates that the physical disorder encoded in the EL patterns yields highly discriminative binary fingerprints. To ensure reproducibility across repeated measurements, a fuzzy extractor is applied, enabling deterministic reconstruction of the 256-bit keys with input error rates up to 17% while preserving class distinctiveness (Fig. 3g)[33]. Additional details of the fuzzy extractor implementation are provided in Supplementary Fig. 5.

To further assess the stability of the micro-LED near-field EL-based PUF, the devices were transferred to an independent thermoelectric controller and operated at temperatures up to 80 °C. When evaluated on these previously unseen images, the trained model maintained a classification accuracy of 100%, confirming the robustness of the extracted PUF signatures under extended thermal variation (Supplementary section 8).

In a practical implementation, the trained PUF extractor can be embedded directly on-chip and integrated with chip-scale micro-LEDs, enabling each node to derive its device identity optically and on demand. Addressing individual emitters within a micro-LED array offers a naturally large challenge space, while the cryptographic response is obtained by processing the captured near-field emission pattern to reconstruct the 256-bit key.

Quantum-resilient optical links

Building on quantum-derived randomness and physically anchored device identity established in the preceding section, micro-LED can simultaneously operate as a secure optical transmitter through direct modulation (Fig. 4a). This enables a unified communication scheme in which PUF-based authentication, QRNG-generated one-time keys and high-speed optical transmission can be implemented within a single platform.

In the scheme, each node locally regenerates a PUF-derived secret, provides a fresh QRNG nonce for the session, and signs a compact authentication token that cryptographically binds its device identity to this nonce. The peer verifies the token using the corresponding registered public key, and the procedure is performed symmetrically in both directions to complete mutual authentication. All PUF feature extraction and key binding are executed on-device, while only signed, nonce-dependent cryptographic proofs are exchanged, ensuring that neither raw PUF information nor intermediate features are ever exposed on the optical link and that replayed attacks are inherently rejected.

Once mutual authentication is established, the nodes upgrade the optical link to quantum-resilient security by running a post-quantum authenticated key-establishment protocol based on the NIST-recommended CRYSTALS-Kyber scheme, whose security relies on the hardness of structured lattice problems that withstand all known classical and quantum attacks[34,35]. The Kyber public keys are bound to the PUF-derived identities established in the previous step, so that any key encapsulation and decapsulation operations are cryptographically linked to a verified device. Using QRNG-generated seeds, the initiating node encapsulates a random message under the peer's Kyber public key, and both sides derive a shared symmetric session key from this message that never appears in clear on the channel. This session key is subsequently applied to secure authenticated and encrypted data transmission over the optical link using

Advanced Encryption Standard in Galois/Counter Mode (AES-GCM)[36,37]. The details of QRNG- and PUF- enabled PQC framework is provided in Supplementary Section 9.

In this way, PUF-based authentication ensures that only genuine devices can participate in the protocol, QRNG-based randomness guarantees high-entropy and unpredictable session keys, and PQC-based key establishment maintains security even against adversaries equipped with quantum computers. The combination of these layers prevents man-in-the-middle and passive eavesdropping attacks on the optical channel without relying on external key servers, allowing micro-LED-based nodes to operate as a self-contained secure optical transmitter within a quantum-resilient communication framework.

We implemented a free-space optical link with the proposed quantum-resilient protocol using micro-LEDs (see experimental details in Supplementary Section 10). The −3 dB modulation bandwidths of nine devices were characterized at 20 mA injection current and 20 °C working temperature, yielding a representative value of 64.5 MHz (Fig. 4b). To evaluate secure data transmission, Orthogonal Frequency-Division Multiplexing (OFDM) with Quadrature Amplitude Modulation (QAM) was used to modulate the micro-LED, and a test image was encrypted blockwise using the post-quantum scheme described above[38]. Figures 4c and 4d show the subcarrier SNR distribution and corresponding QAM constellations, both before and after applying a lightweight Multilayer Perception (MLP)-based equalizer.

With the equalizer, the achievable data rate increased from 1.25 to 1.97 Gb/s, and the post forward-error-corrected (FEC) bit-error rates (BER) was 0, enabling faithful recovery of the transmitted image (Fig. 4e). In contrast, without equalization, residual errors produce visible artifacts in the decrypted output.

Beyond cryptographic protection, the OFDM waveform itself introduces an additional layer of physical security due to its frequency-domain dispersion, subcarrier orthogonality and channel-dependent time-frequency structure, which together hinder unauthorized demodulation. These physical properties complement the PUF-anchored authentication and PQC-based key establishment, resulting in a high-speed micro-LED-based optical link that provides both high fidelity and quantum-resilient security.

Towards hierarchical security architectures and co-packaged hardware for quantum-resilient IoT

Figure 5a illustrates representative deployment environments in which micro-LED secure nodes can operate, including smart manufacturing, drone-based networking, vehicle-to-everything (V2X) links, privacy-preserving healthcare and smart-city infrastructure. These scenarios are characterized by dense distributions of edge devices communicating over short-range optical wireless links, often without fixed trusted gateways. The resulting exposure to untrusted or potentially compromised nodes necessitates a security architecture that remains robust even when individual endpoints

cannot be fully trusted.

To meet these requirements, we have structured the system into three functional layers (Fig. 5b). At the device layer, each IoT node incorporates a micro-LED array that provides three core functionalities demonstrated earlier, including QRNG, PUF, and secure optical transmission, establishing a hardware-rooted trust anchor independent of the firmware or software running on the host controller. Building on this foundation, quantum-resilient link layer establishes encrypted optical channels between neighboring nodes. All cryptographic and signal-processing tasks are offloaded to dedicated hardware so that the resource-constrained IoT micro-controller unit (MCU) only issues lightweight control commands and consumes session keys or ciphertext. At the network level, a decentralized trust layer can register PUF-derived public keys, manage revocation and propagate trust across the mesh by means of a distributed ledger, enabling secure onboarding and long-term integrity of large device populations.

We further propose a co-packaged platform (Fig. 5c) that integrates QRNG, PUF, and quantum-resilient optical communication, thereby reducing system complexity, minimizing operational latency, and improving energy efficiency[39]. In this architecture, application-specific integrated circuits (ASICs) provide control, configuration and secure enclaves for QRNG post-processing and PUF response generation, ensuring that raw entropy sources including near-field PUF images and QRNG bitstreams never leave the protected boundary. A secure interface allows encrypted readout without revealing underlying device secrets.

A 3D co-packaged optical front end offloads time-critical signal processing and modulation control, while micro-LED arrays on the chiplet serve as optical transmitters, PUF entropy sources and quantum-noise emitters for QRNG. Devices intended for QRNG and PUF functions may employ larger emission apertures to facilitate near-field imaging and to provide sufficient photon flux for extracting spontaneous-emission fluctuations. The PUF and QRNG rely on different physical mechanisms, which provides an additional layer of security and prevents the simultaneous compromise of both entropy sources.

Near-field patterns and QRNG signals can be routed to on-chip detectors using compact imaging optics or photonic interconnects, while micro-LED/PD pairs equipped with microlenses enable short-range free-space communication suitable for distributed IoT nodes. The detected signals are conditioned and digitized on the chip before being forwarded to the logic layer for authentication or key generation.

By consolidating transmission, identity and randomness into the same device, this architecture provides a practical route toward secure optical communication between IoT nodes. As each micro-LED contributes an independent optical channel, the achievable data rate, random-number throughput and PUF challenge space can be increased simply by scaling the array size. This integrated approach enables dense, low-power and cryptographically resilient wireless links for future interconnected devices.

Conclusions

We have proposed and experimentally demonstrated a micro-LED-based quantum-resilient architecture that unifies QRNG, PUF, and OWC for decentralized IoT networks. A micro-LED enables 13.25 Gb/s quantum random number generation and optical wireless transmission at 1.97 Gb/s, while a nine-element micro-LED array provides PUF functionality with reproducible 256-bit responses per element. The QRNG and PUF outputs are incorporated into a PQC framework to support decentralized device authentication and encrypted communication. By integrating identity, randomness, and data transmission within a single epitaxial platform and fabrication process, this approach substantially reduces system complexity and removes the need for discrete security modules. Owing to the vertically emitting geometry of micro-LEDs, QRNG throughput, communication bandwidth, and PUF challenge space can be naturally scaled through array expansion. To support system-level integration with low latency and energy overhead, we designed a CPO architecture that interfaces directly with existing IoT hardware. Together, this work extends the role of micro-LEDs beyond conventional display and communication functions, establishing them as a unified, hardware-rooted platform for quantum-resilient security that enables lightweight and scalable post-quantum resilient communication across decentralized IoT systems and other security-critical infrastructures.

Materials and methods

Device design and fabrication

A schematic of the detailed device fabrication process is provided in Supplementary Fig. 1. The micro-LEDs and micro-LED arrays are fabricated using a 405 nm micro-LED wafer with standard process steps. The wafer is grown on PSS using metal-organic chemical vapor deposition (MOCVD). The fabrication process starts with mesa definition by a two-step inductively coupled plasma reactive ion etching (ICP-RIE) using 300 nm plasma-enhanced chemical vapor deposition (PECVD) SiO_2 as hard mask. The hard mask is removed by immersing the chip inside buffered oxide etch (BOE) solution, which also helps to repair the sidewall damage caused by ICP-RIE. E-beam evaporation of a 5-nm Ni layer and RF magnetron sputter of a 120-nm indium-tin-oxide (ITO) are deposited for p-contact. After 250 °C annealing in an O_2 atmosphere for 10 min, the n-metal contact of Ti/Au is deposited using RF magnetron sputtering.

Characterization setup for the micro-LED based QRNG, PUF, and secure communication

The experimental setup for QRNG and PUF is shown on Fig. 2a. The constant current source is provided by a source meter (Keithley 2420). The temperature control is conducted by a TEC (ILX Lightwave LDC-3900) for primary data collection (20℃ to 50℃). For higher temperature (50℃ to 80℃) characterization, another TEC (Apico Pro TEC controller) is used to stabilize the temperature. The emitted light passes through a 50× objective lens (Nikon CFP-LAN-50X), a positive lens (Thorlabs LB1901-A, BI-CONVEX, f = 75.0 mm), and a dichroic mirror (Thorlabs DMLP490-Ø1), getting into an APD (Menlo Systems APD 210) and a camera, separately. The detected electrical signal is then amplified by an amplifier (Mini-Circuits ZVA-183WA-S+) and digitized by an 8-bit oscilloscope (DPO 72004C Digital Phosphor Oscilloscope) for noise data collection.

A schematical of the experimental setup for secure OWC is shown on Supplementary Fig. 7c. Optical signal transmission in free space is the same as the experimental setup for QRNG. The encrypted data is loaded to an arbitrary waveform generator (Tektronix AWG70002A), converted into analog signal, amplified by an amplifier (Mini-Circuits ZVA-183WA-S+), and applied to a micro-LED at a sampling rate of 1.6 GSa/s with a driving DC through a bias-tee. The micro-LED is then working as a transmitter to emit modulated light. The emitted light passes through a 50× objective lens (Nikon CFP-LAN-50X), a positive lens (Thorlabs LB1901-A, BI-CONVEX, f = 75.0 mm), and a dichroic mirror (Thorlabs DMLP490-Ø1), focused on an APD (Thorlabs APD430A2/M) as a receiver. The collected signal from APD is then digitized by an oscilloscope (DPO 72004C Digital Phosphor Oscilloscope). The communication channel was first characterized to determine its frequency response and noise properties. This measurement provided the basis for selecting appropriate OFDM parameters, such as subcarrier spacing and equalization strategy, ensuring that subsequent transmission experiments accurately reflected the channel behavior.

ZNCC calculation

To quantify the similarity between two images, ZNCC is computed. For each image $A = \{A_i\}_{i=1}^{N}$ and $B = \{B_i\}_{i=1}^{N}$,

the mean intensity (μ_A, μ_B) are calculated and normalized by the corresponding standard deviation (σ_A, σ_B). The similarity score is then evaluated as

$$ZNCC(A,B) = \frac{\sum_{i=1}^{N}(A_i - \mu_A)(B_i - \mu_B)}{\sqrt{\sum_{i=1}^{N}(A_i - \mu_A)^2}\sqrt{\sum_{i=1}^{N}(B_i - \mu_B)^2}}\ . \quad (1)$$

QRNG generation rate calculation

The QRNG generation rate is calculated at the transceiver (TRx) side from the digitized detector waveform. The oscilloscope samples the analogue signal at K GSa·s^{-1} using an 8-bit ADC, producing a discrete symbol sequence $X_n \in \{0, \ldots, 255\}$. The amount of trusted randomness per bit is quantified by the min-entropy estimated following NIST SP 800-90B H_{min}^{90B}. The extractable random-bit generation rate is then

$$R = 8 \times K \times H_{min}^{90B}, \quad (2)$$

$$R = 8 \times 3.125 \times 0.53 = 13.25\ Gbit \cdot s^{-1}. \quad (3)$$

QRNG energy consumption at micro-LED side

At injection current of $I = 10$ mA, the micro-LEDs have an average voltage of $V = 4.9$ V, so the power consumption is $P = I \times V = 48$ mW. With a generation rate of $R = 13.25$ Gbit·s^{-1}, the energy consumption per bit can be denoted as

$$E = \frac{P}{R} = \frac{I \times V}{R}, \quad (4)$$

$$E = \frac{49 \times 10^{-3}\ J \cdot s^{-1}}{13.25 \times 10^{9}\ bit \cdot s^{-1}} = 3.70\ pJ \cdot bit^{-1}. \quad (5)$$

Deep-learning-assisted PUF extraction

All deep-learning experiments were conducted on a laptop equipped with an NVIDIA GeForce RTX 3060 GPU, using Python 3.9 and PyTorch 2.9.0 with CUDA 12.9. The dataset consists of near-field electroluminescence images of micro-LED devices, with 1,800 images per device label, of which 1,440 images were used for training and 360 images for testing. Micro-LED emission regions were detected using a pretrained YOLOv8n object detection model trained on 75 manually annotated images and validated on 46 images, with a single target class. Training was performed with an input resolution of 640 × 640 pixels, batch size 16, and 50 epochs. During inference, detections with confidence above 0.25 were cropped into square regions centered on the bounding boxes and resized to 256 × 256 pixels.

Cropped images were converted to 80 × 80 grayscale inputs and normalized to zero mean and unit variance. Binary PUF embeddings were extracted using a customized convolutional neural network incorporating a spatial transformer for geometric alignment, a ResNet-34 backbone pretrained on ImageNet with attention augmentation, and an

embedding head producing 256-bit binary outputs via a straight-through estimator. The network was trained using a composite loss combining cross-entropy classification, batch-hard triplet loss (margin = 1.0), quantization regularization, and bit-distribution constraints. Optimization employed the Adam optimizer with a learning rate of 1×10^{-4}, weight decay of 1×10^{-5}, batch size 64, and up to 50 epochs with early stopping. Data augmentation, including random rotations, affine transformations, scaling, and brightness and contrast jittering, was applied during training. Model performance was evaluated using classification accuracy, normalized Hamming-distance analysis of binary embeddings, and t-SNE visualization to assess inter-device separability. The neural network architecture and layer configuration are provided in Supplementary Section 6.

Fuzzy extraction and key reconstruction

A software-based fuzzy-extraction pipeline was implemented in Python to stabilize and reproduce cryptographic keys from noisy physical unclonable function (PUF) responses as illustrated in Supplementary Fig. 5. Each measured binary PUF response consisted of 256 bits and was divided into four 64-bit segments. To mitigate spatially correlated errors, each segment was interleaved at the bit level prior to error correction.

Each segment was encoded using a systematic Reed-Solomon (RS) code with 16 parity bytes (RS (24,8)), where the original 8-byte message was preserved and appended with redundancy. During enrollment, the RS parity bytes were stored as public helper data, while the enrolled 256-bit response served as the reference PUF response.

During reconstruction, noisy PUF responses were processed using the same interleaving scheme and combined with the stored parity bytes to form complete RS codewords. RS decoding was applied independently to each segment to recover the enrolled bits. Reconstruction performance was evaluated by comparing the recovered responses with the enrolled references in terms of bit error rate and decoding success probability.

Following successful reconstruction, a cryptographic key was derived from the stabilized 256-bit response using the SHA-256 hash function, providing privacy amplification and generating a fixed-length key suitable for subsequent cryptographic operations.

Data availability

All other data used in this study is available from the corresponding authors upon reasonable request.

Code availability

Source codes in this study are available online: https://github.com/Mortefontaine/Micro-LED-based-PUF-release

References

1. 2.7 billion records exposed in IoT devices data breach. *vpnMentor* https://www.vpnmentor.com/news/report-marshydro-breach/.

2. IoT security archives. *Forrester* https://www.forrester.com/blogs/category/iot-security/.

3. IoT hacking statistics 2025: Threats, risks & regulations. *DeepStrike* https://deepstrike.io/blog/iot-hacking-statistics (2025).

4. Dam, D.-T., Tran, T.-H., Hoang, V.-P., Pham, C.-K. & Hoang, T.-T. A survey of post-quantum cryptography: Start of a new race. *Cryptography* **7**, 40 (2023).

5. Joseph, D. *et al.* Transitioning organizations to post-quantum cryptography. *Nature* **605**, 237–243 (2022).

6. Mojtaba Bisheh-Niasar, Reza Azarderakhsh, & Mehran Mozaffari-Kermani. High-speed NTT-based polynomial multiplication accelerator for post-quantum cryptography. in *2021 IEEE 28th Symposium on Computer Arithmetic (ARITH)* (IEEE, Lyngby, Denmark, 2021). doi:10.1109/ARITH51176.2021.00028.

7. Chaos-based scalable optoelectronic physical unclonable functions with AI-driven dynamic authentication. https://www.researchsquare.com (2025) doi:10.21203/rs.3.rs-6484421/v1.

8. Physical unclonable function: architectures, applications and challenges for dependable security. https://doi.org/10.1049/iet-cds.2019.0175 doi:10.1049/iet-cds.2019.0175.

9. Unclonable fluorescence behaviors of perovskite quantum dots/chaotic metasurfaces hybrid nanostructures for versatile security primitive. *Chemical Engineering Journal* **411**, 128350 (2021).

10. Al-MeerAbdulaziz & Al-KuwariSaif. Physical unclonable functions (PUF) for IoT devices. *ACM Computing Surveys* https://doi.org/10.1145/3591464 (2023) doi:10.1145/3591464.

11. Sandeep S. Kumar, Jorge Guajardo, Roel Maes, Geert-Jan Schrijen, & Pim Tuyls. Extended abstract: The butterfly PUF protecting IP on every FPGA. in *2008 IEEE International Workshop on Hardware-Oriented Security and Trust* (IEEE, Anaheim, CA, USA, 2008).

12. Stipčević, M. & Koç, Ç. K. True random number generators. in *Open Problems in Mathematics and Computational Science* 275–315 (Springer, Cham, 2014). doi:10.1007/978-3-319-10683-0_12.

13. Berk Sunar, William J. Martin, & Douglas R. Stinson. A provably secure true random number generator with built-in tolerance to active attacks. *IEEE Transactions on Computers* **56**, 109–119 (2007).

14. Lu, H. *et al.* Low-coherence semiconductor light sources: Devices and applications. *npj Nanophoton.* **1**, 9 (2024).

15. Alkhazragi, O. *et al.* Semiconductor emitters in entropy sources for quantum random number generation. *Annalen der Physik* **535**, 2300289 (2023).

16. Li, X. *et al.* A memristor-based unified PUF and TRNG chip with a concealable ability for advanced edge security. *Science Advances* https://doi.org/10.1126/sciadv.adr0112 (2025) doi:10.1126/sciadv.adr0112.

17. Iluminada Baturone, Roberto Román, & Ángel Corbacho. A unified multibit PUF and TRNG based on ring oscillators for secure IoT devices. *IEEE Internet of Things Journal* **10**, 6182–6192 (2023).

18. S. Larimian, M. R. Mahmoodi, & D. B. Strukov. Lightweight integrated design of PUF and TRNG security primitives based on eFlash memory in 55-nm CMOS. *IEEE Transactions on Electron Devices* **67**, 1586–1592 (2020).

19. Park, T.-Y. *et al.* 2-gb/s ultraviolet-light optical wireless communication by InGaN/GaN multi-quantum well dual-function micro-photodetector. *Appl. Phys. Lett.* **124**, (2024).

20. P. Tian *et al.* Micro-LED based optical wireless communications systems. in *Semiconductors and Semimetals* vol. 106 281–321 (Elsevier, 2021).

21. Xinyi Shan *et al.* Multifunctional ultraviolet-C micro-LED with monolithically integrated photodetector for optical wireless communication. *Journal of Lightwave Technology* **40**, 490–498 (2022).

22. Pezeshki, B. *et al.* 10-gb/s NRZ per lane data links with transferred micro-LEDs with record BER and energy efficiency. *IEEE Photonics Technology Letters* **37**, 453–456 (2025).

23. Lin, H. *et al.* Micro-LED-based quantum random number generators. *Opt. Express, OE* **33**, 22154–22164 (2025).

24. Bychikhin, S., Pogany, D., Vandamme, L. K. J., Meneghesso, G. & Zanoni, E. Low-frequency noise sources in as-prepared and aged GaN-based light-emitting diodes. *J. Appl. Phys.* **97**, (2005).

25. Sawyer, S. *et al.* Current and optical noise of GaN⁄AlGaN light emitting diodes. *J. Appl. Phys.* **100**, (2006).

26. Ma, X. *et al.* Postprocessing for quantum random number generators: Entropy evaluation and randomness extraction. Preprint at https://doi.org/10.1103/PhysRevA.87.062327 (2012).

27. Rukhin, A. *et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. https://csrc.nist.gov/pubs/sp/800/22/r1/upd1/final (2010) doi:10.6028/NIST.SP.800-22r1a.

28. Brown, R. G., Dirk, E. & David, B. Dieharder. *Duke University Physics Department Durham* **NC**, 27708 (2018).

29. He, K., Zhang, X., Ren, S. & Sun, J. Deep residual learning for image recognition. in *2016 IEEE Conference*

on Computer Vision and Pattern Recognition (CVPR) 770–778 (IEEE, Las Vegas, NV, USA, 2016). doi:10.1109/CVPR.2016.90.

30. Reis, D., Kupec, J., Hong, J. & Daoudi, A. Real-Time Flying Object Detection with YOLOv8. Preprint at https://arxiv.org/abs/2305.09972v2 (2023).

31. Jaderberg, M., Simonyan, K., Zisserman, A. & Kavukcuoglu, K. Spatial transformer networks. *Advances in Neural Information Processing Systems* **28**, (2015).

32. Woo, S., Park, J., Lee, J.-Y. & Kweon, I. S. CBAM: Convolutional block attention module. in 3–19 (2018).

33. Dodis, Y., Reyzin, L. & Smith, A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. in *Advances in Cryptology - EUROCRYPT 2004* 523–540 (Springer, Berlin, Heidelberg, 2004). doi:10.1007/978-3-540-24676-3_31.

34. Avanzi, R. *et al.* CRYSTALS-Kyber algorithm specifications and supporting documentation. (2019).

35. Bos, J. *et al.* CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM. in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)* 353–367 (2018). doi:10.1109/EuroSP.2018.00032.

36. Marie A Wright. The advanced encryption standard. *Network Security* **2001**, 11–13 (2001).

37. McGrew, D. A. & Viega, J. The security and performance of the galois/counter mode (GCM) of operation. in *Progress in Cryptology - INDOCRYPT 2004* 343–355 (Springer, Berlin, Heidelberg, 2004). doi:10.1007/978-3-540-30556-9_27.

38. Jean Armstrong. OFDM for optical communications. *Journal of Lightwave Technology* **27**, 189–204 (2009).

39. Papatryfonos, K. *et al.* Co-Package Technology Platform for Low-Power and Low-Cost Data Centers. *Applied Sciences* **11**, (2021).

Acknowledgments

This publication is based upon work supported by King Abdullah University of Science and Technology under the Grant of Transition Award in Semiconductors: FCC/1/5939; KAUST Center of Excellence for Renewable Energy and Storage Technologies (CREST) FCC/1/5937; King Abdullah University of Science and Technology (BAS/1/1614-01-01, ORA-2022-5313, ORFS-2022-CRG11-5079, KCR/1/4055-01-01). The authors further acknowledge the use of the KAUST Nanofabrication Core Lab and the KAUST Imaging and Characterization Core Lab facilities.

Author contributions

H. Lin and B. O. conceived the research concept and experimental methodology. T. Y. P. designed and fabricated the devices in discussion with T. K. N. H. Lin performed the QRNG and PUF experimental characterization, developed the PUF algorithm with support from H. Lu, Z. Z. and Y. W. W. N. developed the MLP equalizer and, together with H. Lin, carried out the optical wireless communication experiments. H. Lin designed the quantum-resilient communication architecture together with W. N. H. Lin designed the 3D packaging concept. H. Lin wrote the manuscript with input from others. B. O. (principal investigator) and T. K. N. (co-principal investigator) led the quantum technology thrust; initiated, supervised and administered the project, and secured related funding for the semiconductor photonics and device group. All authors discussed the results and contributed to the final manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/XXX.XXXX/XXXXX-XXX-XXXXX-X.

Correspondence and requests for materials should be addressed to Boon Ooi

© The Author(s) 2025

Figures and captions

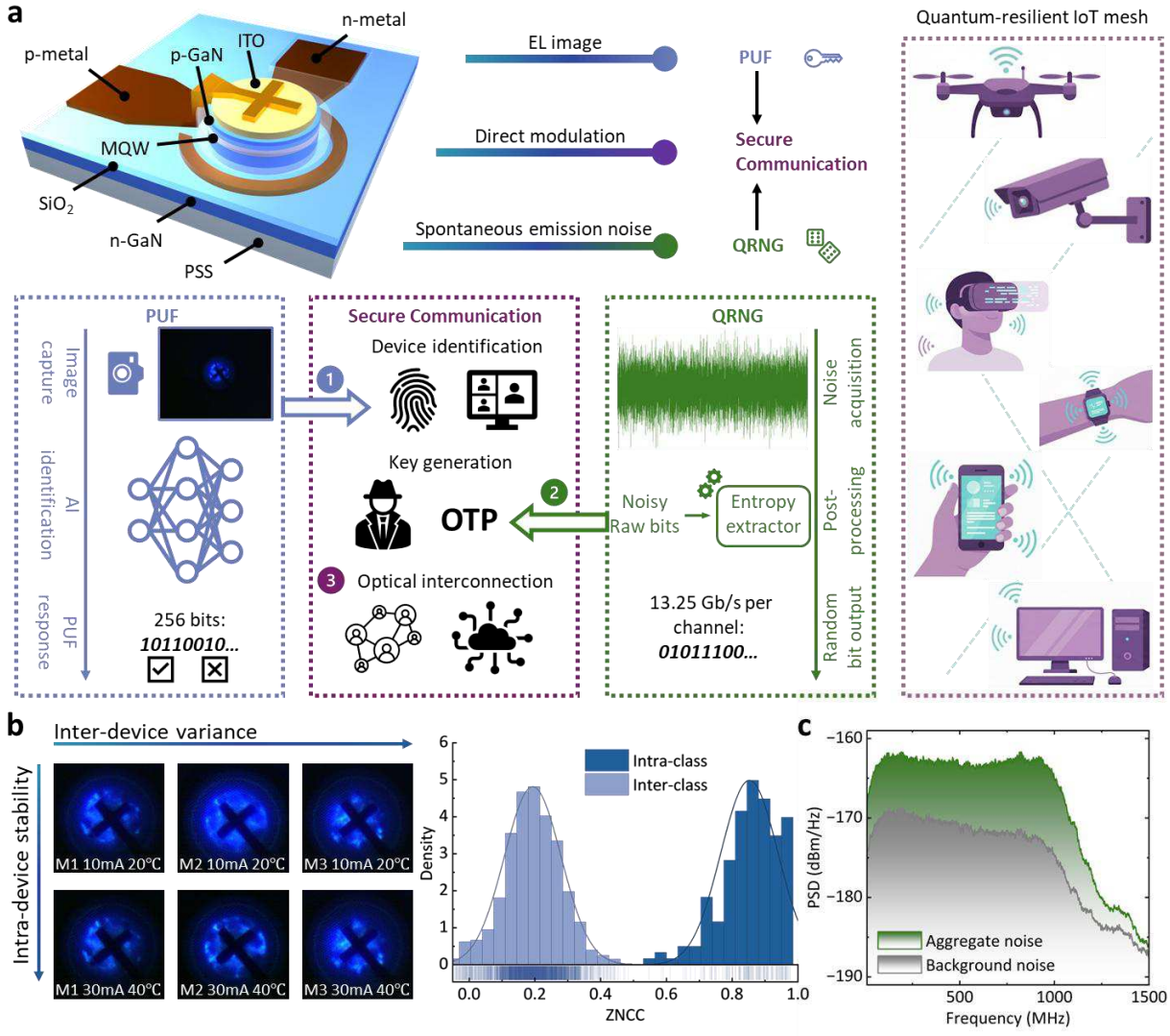


Figure 1. Micro-LED-enabled quantum-resilient optical interconnects incorporating physical unclonable functions and quantum random number generation. a, Overview of the security architecture and the quantum-resilient IoT mesh network. b, Inter-device variance and intra-device stability of the near-field emission, with zero-mean normalized cross-correlation (ZNCC) distributions for inter- and intra-class comparisons. c, Power spectra density of the system when the micro-LED is driven at 10 mA injection current (aggregate noise) and when it is off (background noise).

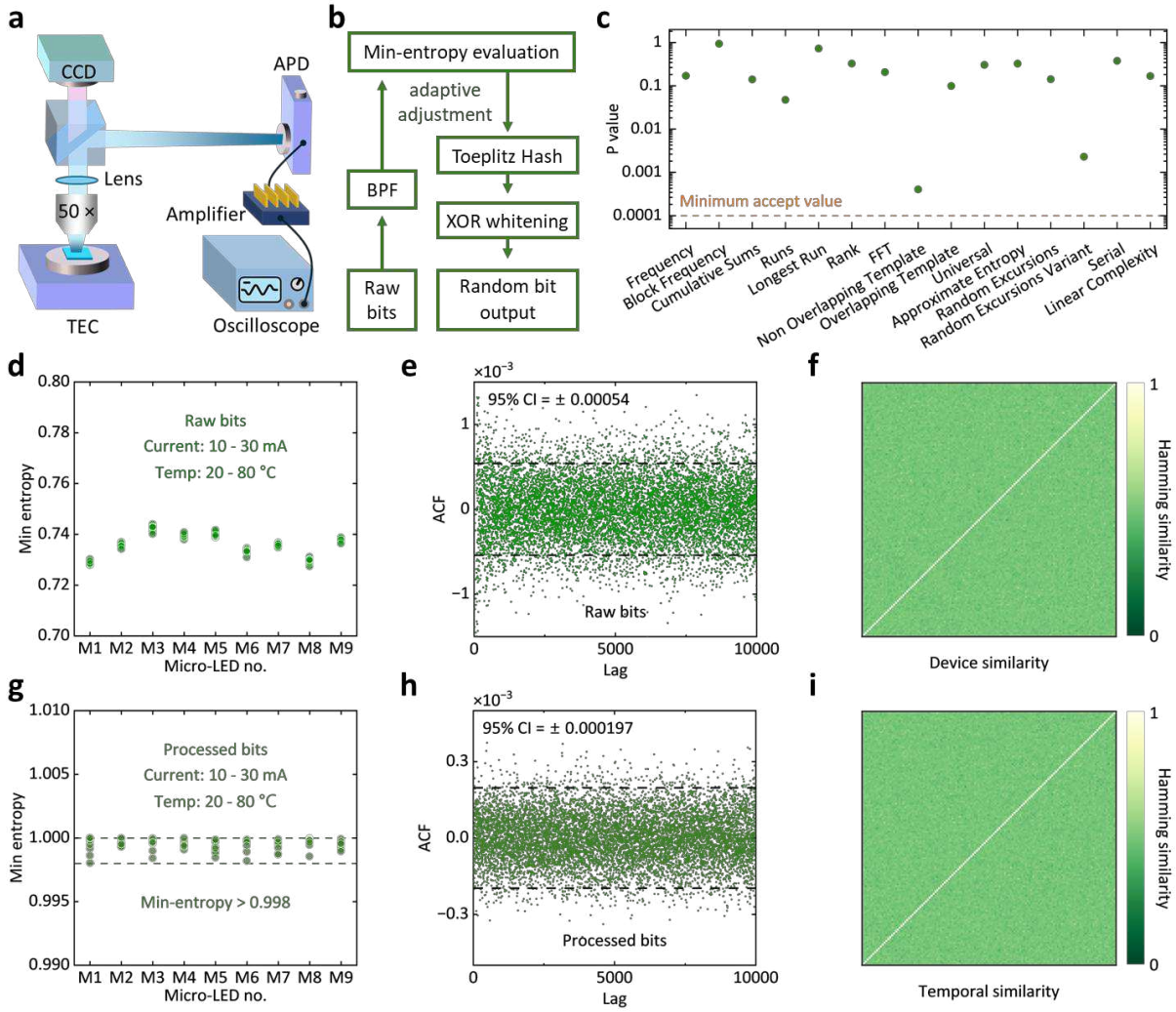


Figure 2. Micro-LED-based quantum random number generation. a, Proof-of-concept experimental setup for acquiring intensity-fluctuation signals from micro-LEDs using a high-speed photodetector and a real-time oscilloscope. b, Post-processing pipeline for random-bit extraction from oscilloscope-recorded noise traces, including band-pass filtering and subsequent randomness extraction/whitening. c, NIST SP 800-22 randomness test results for 1,800 × 1-million random bits generated from nine micro-LED devices operated with injection currents from 10 to 30 mA and temperatures from 20 to 80 °C. d–i, Statistical characterization of the raw and post-processed bitstreams. d and g, Estimated min-entropy of raw bits (d) and processed bits (g). e and h, Autocorrelation function (ACF) of raw bitstream (e) and the processed bitstream (h). f, Inter-device similarity matrix of the post-processed bitstreams across the nine devices measured over 135 operating conditions (all combinations within 10–30 mA and 20–80 °C). i, Temporal similarity matrix of post-processed bitstreams acquired from the same device under an identical operating condition at different times. Similarity is quantified using the Hamming distance, computed on bit segments of 1,000 bits and 135 segments.

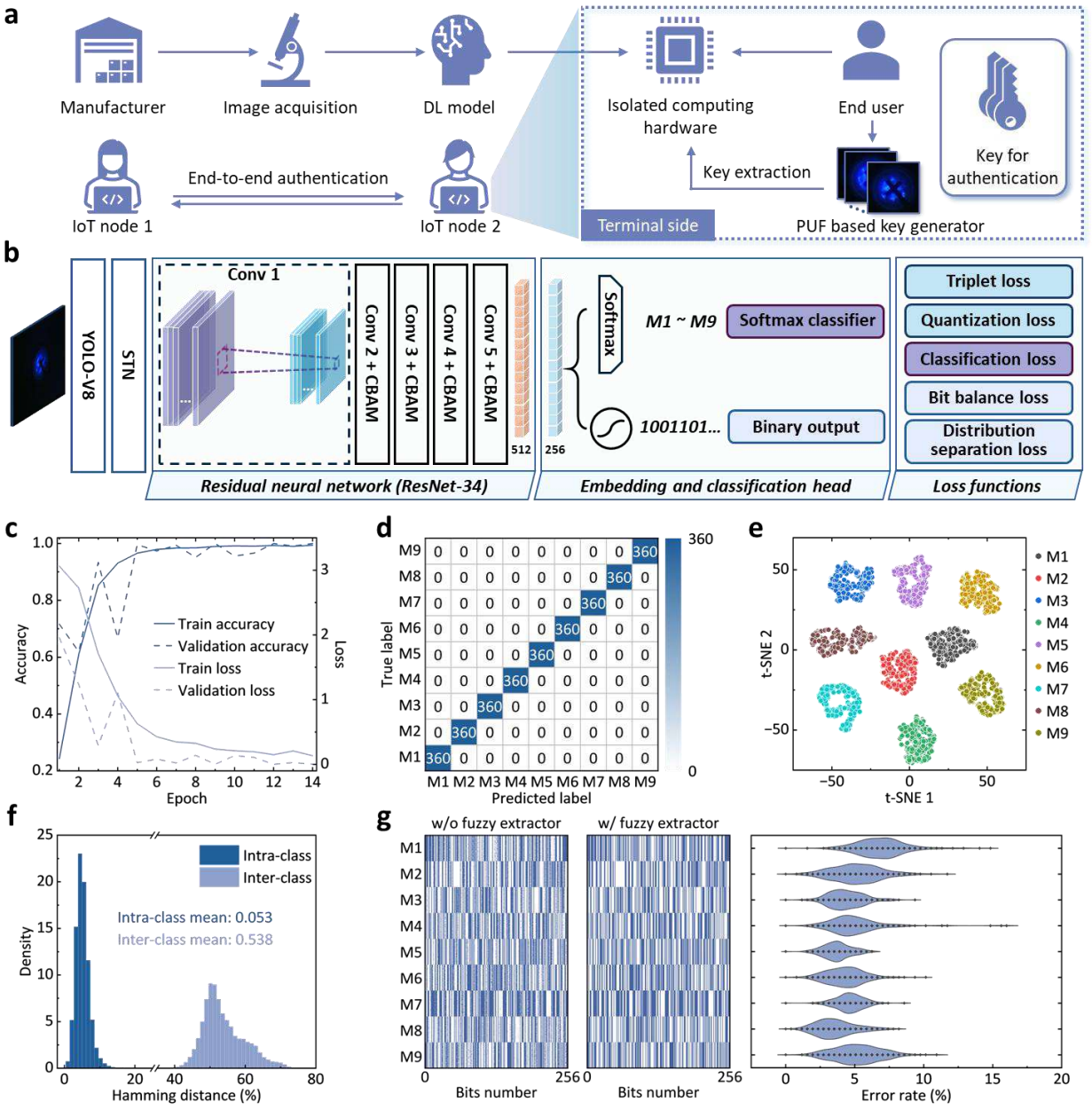


Figure 3. Micro-LED-based PUF. a, Application workflow of the micro-LED PUF used as an authentication key source in secure communication. b, ResNet-34-based deep neural network (DNN) architecture for PUF key extraction. c, Training histogram. d, Confusion matrix of the test set, with each label containing 360 samples. e, t-SNE evaluation for nine different micro-LED devices. f, Inter-device separability quantified by the Hamming distance between the derived 256-bit binary outputs (intra-device versus inter-device distributions). g, Binary outputs for different labels before and after fuzzy extraction (binary values are encoded as dark (1) and light (0) pixels), along with the bit-error rates of extracted bits from different images without fuzzy extraction.

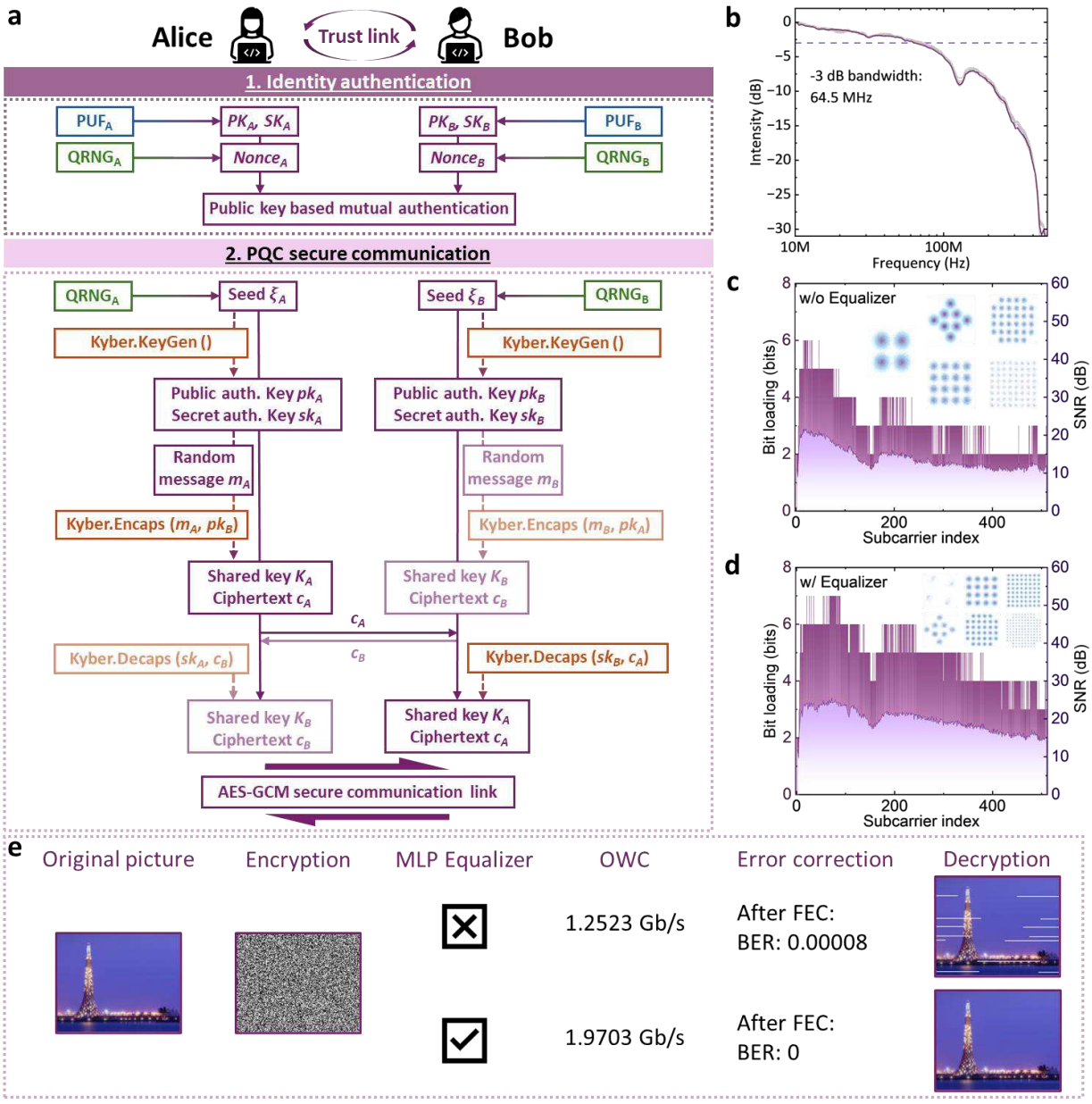


Figure 4. Micro-LED-based quantum-resilient communication. a, Architecture of the micro-LED–enabled quantum-resilient communication system with in-situ PUF and QRNG. b, −3 dB bandwidth of nine micro-LED devices under 20 mA injection current and 20 °C working temperature. c-d, Bit loading, and SNR of the transmitted signal without (c) and with (d) the MLP equalizer; the inset shows constellation diagrams of QAM signals. d, Experimental demonstration and performance comparison of micro-LED-based quantum-resilient optical wireless communication with and without the MLP equalizer.

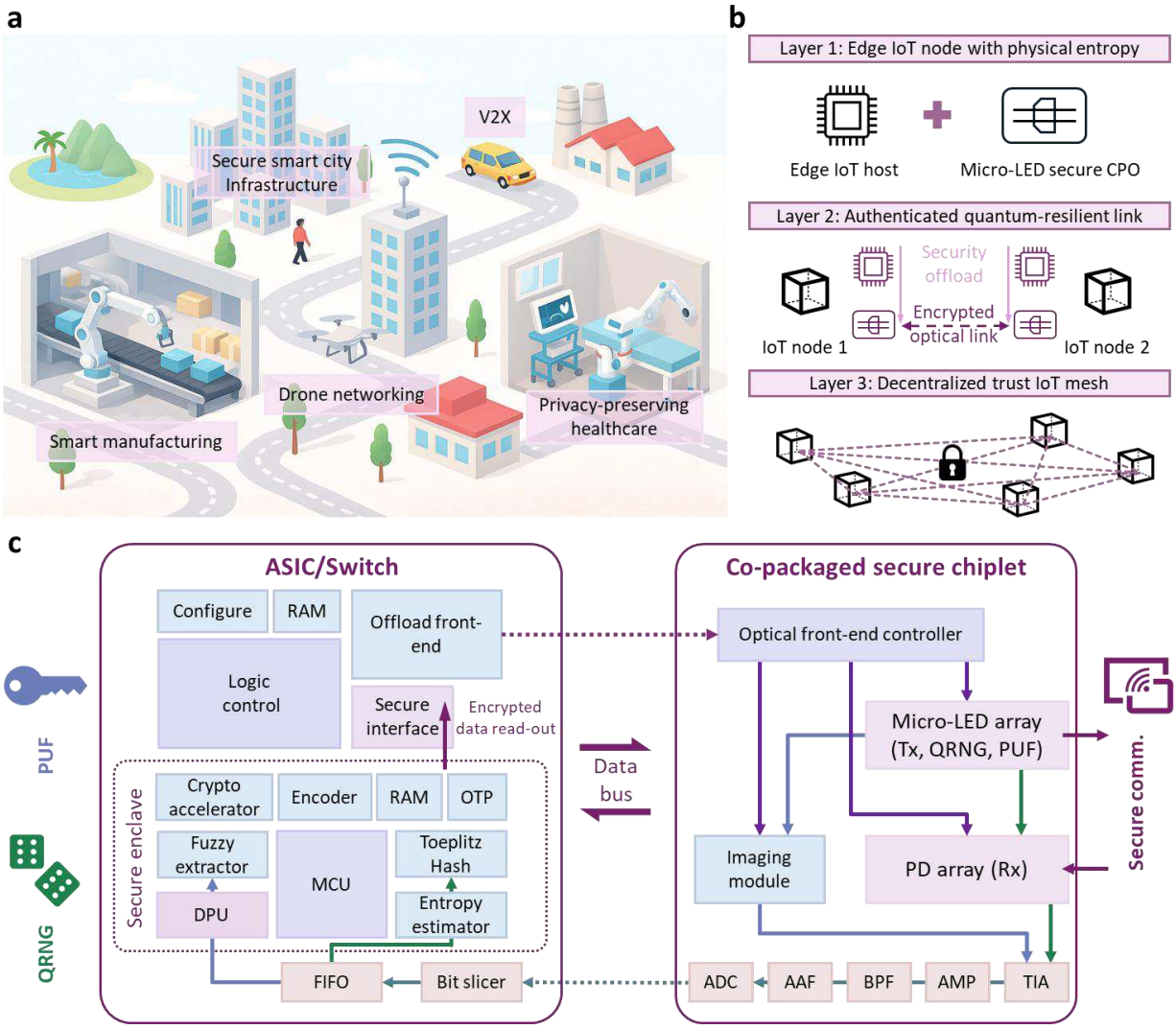


Figure 5. End-to-end architecture and deployment of the quantum-resilient optical IoT platform. (a) Real-world deployment scenarios where the proposed platform enables secure optical connectivity across smart manufacturing, smart city infrastructure, drone networking, Vehicle-to-Everything (V2X) communication, and privacy-preserving healthcare. (b) Layered system stack consisting of 3 layers. Layer 1: edge IoT node with physical entropy (PUF and QRNG); Layer 2: authenticated, post-quantum-resilient optical link with hardware security offload; and Layer 3: a decentralized, blockchain-anchored IoT trust mesh. (c) Hardware architecture of the secure optical node, integrating a cryptographic secure enclave, PUF/QRNG primitives, encoder/DPU pipeline, entropy estimator, and a co-packaged micro-LED/photodiode chiplet for optical transmission, reception, and security offload.

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- SupplementaryInformation.docx