





Micro-LED-based quantum random number generators

HEMING LIN,¹ HANG LU,¹ MATTHEW S. WONG,²
ABDULLAH ALMOGBEL,³  AHMED ALYAMANI,³ TIEN KHEE NG,¹ 
OSMAN BAKR,⁴ SHUJI NAKAMURA,² STEVEN P. DENBAARS,² AND
BOON S. OOI^{1,5} 

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

²Solid State Lighting & Energy Electronics Center, University of California, Santa Barbara, California 93106, USA

³King Abdulaziz City for Science and Technology (KACST), Riyadh 12354, Saudi Arabia

⁴Division of Physical Science and Engineering, King Abdullah University of Science and Technology (KAUST), Thuwal, 23955-6900, Saudi Arabia

⁵boon.ooi@kaust.edu.sa

Abstract: Quantum random number generators (QRNGs) leverage the inherent unpredictability of quantum mechanical phenomena to produce random numbers. However, the performance of many QRNGs is hindered by limitations such as low generation rates and the bulkiness of systems utilizing single-photon detectors (SPDs). In this study, we present a QRNG that addresses these challenges by using a micro-LED as an entropy source, utilizing the intensity fluctuations of spontaneous emissions. By applying post-processing techniques, our $5 \times 5 \mu\text{m}^2$ micro-LED-based system achieves a PD bandwidth-limited generation rate of 9.375 Gbit/s while successfully passing the required randomness tests outlined by the National Institute of Standards and Technology (NIST). Importantly, systematic testing across micro-LEDs of varying sizes demonstrates consistently high performance, highlighting the robustness of this approach. The compact, small footprint, scalable design, and surface emission characteristics of micro-LEDs pave the way for the development of parallel QRNG-integrated chips, which hold the potential to deliver ultra-high random number generation rates in practical, miniaturized platforms.

© 2025 Optica Publishing Group under the terms of the [Optica Open Access Publishing Agreement](#)

1. Introduction

Random numbers are fundamental to a wide range of applications that require unpredictability for various fields, including secure communications [1], cryptography protocols [2,3], Monte-Carlo simulations [4,5], optimization algorithms, and complex decision-making in artificial intelligence (AI) [6]. Two main approaches to generating random numbers are pseudo-random number generation (PRNG) and true random number generator (TRNG). PRNGs are widely used due to their easy accessibility and computational efficiency. However, they rely on deterministic algorithms, posing potential security risks in critical applications. Once initial conditions (seeds) are revealed, the random numbers can be predicted [7]. In contrast, TRNGs take advantage of measuring unpredictable classical physical processes including thermal noises of electronics [8], phase jitter of oscillators [9], and chaos [10,11] to generate random numbers. Quantum random number generators (QRNGs) can be considered a specialized subset of TRNGs, particularly those that harness the inherent unpredictability arising from the principles of quantum mechanics [12]. There are various QRNG approaches that have been proposed, such as photon arrival time measurements [13], photon arrival positions measurement [14], phase fluctuations of lasers [15],

quantum vacuum fluctuations [16], and intensity fluctuations of amplified spontaneous emissions (ASEs) [17].

The truly indeterministic randomness of QRNG makes them highly desirable for applications requiring unparallel security and randomness, particularly in the era of quantum computing threats [27]. A recent study has also demonstrated that QRNG outperforms PRNG in Monte Carlo simulation tasks [28]. The reliability of quantum key distribution (QKD) systems also depends heavily on the quality of random numbers used for cryptographic key generation [3]. As a cornerstone of secure communication, QKD leverages the principles of quantum mechanics to safeguard data transmission against eavesdropping [29]. The ultimate security assurance in QKD comes from the use of QRNGs, which produce truly unpredictable random numbers.

However, QRNGs relying on photon arrival times or counting are often constrained by the limitations of single-photon detectors (SPDs) and one bit of information entropy, which tends to limit the achievable generation rates. Post-processing techniques, including random extraction algorithms, are frequently utilized to increase the output bit rates and enhance the quality and reliability of generated random bits, which has been applied to QRNG systems relying on measuring the intensity fluctuations of ASEs and spontaneous emissions (SEs) [26,30,31]. Recent research has shown LED based QRNG taking advantage of SE and absorption to realize 1 Mb/s real-time quantum random bits generation with an integrated chip [26]. SE from entropy sources offers a promising mechanism for QRNGs. The intensity fluctuations follow a Gaussian distribution as a result of randomness of SE [32]. By leveraging the cumulative distribution function (CDF) of intensity fluctuations, it can partition the output into intervals of equal probability. This method allows the efficient generation of uniformly distributed random bits, providing the potential to produce high-quality quantum random bits at high generation speed with minimal hardware complexity.

In this context, we present micro-LEDs as an attractive entropy source for QRNG. The low power consumption of micro-LEDs ensures energy-efficient operation, which is important for deploying QRNGs in resource-constrained environments or portable devices [33]. The compact size and surface-emission characteristics of micro-LEDs enable seamless chip-scale integration into 2D arrays, paving the way for QRNG systems with highly scalable, multi-parallel channels. We use atomic layer deposition (ALD) passivated micro-LEDs with different sizes as entropy sources to generate quantum bits through measuring the intensity fluctuations of micro-LEDs' spontaneous emission. The ALD passivation layer enhances the operational stability of micro-LEDs, ensuring consistent generation of quantum random bits [34]. By utilizing widely adopted post-processing algorithms including subtraction and least significant bits (LSBs) retention, high-quality random bit-streams are generated [10,35]. Micro-LEDs with a size of $5 \times 5 \mu\text{m}^2$ can reach the highest generation rate of 9.375 Gb/s at an injection current of 1 mA, and the random bits successfully pass the National Institute of Standards and Technology (NIST) tests. Other micro-LEDs with larger sizes up to $100 \times 100 \mu\text{m}^2$ can also achieve a generation rate of 9.375 Gb/s, where the speed is limited by electrical devices, such as the photodetector and the oscilloscope. Compared to other LED-related QRNG systems, our micro-LED-based QRNG achieves the highest speed, as shown in Table 1. Micro-LED opens a solution for high-density, low-cost, ultra-fast QRNG.

2. Device design and characteristics

GaN-based micro-LEDs of varying sizes are fabricated on the same wafer, with an epitaxial structure grown via atmospheric-pressure metalorganic chemical vapor deposition (MOCVD). The layer composition includes a 17 nm Mg-doped p^+ -GaN layer, a 120 nm Mg-doped p-GaN layer, and a 26 nm Mg-doped p-AlGaIn layer, followed by six periods of InGaIn/GaN multiple quantum wells (MQWs) and a 20-period InGaIn/GaN superlattice (SL) designed to enhance carrier confinement and emission efficiency. Beneath these active layers, a 4 μm Si-doped n-GaN

Table 1. Comparison between QRNGs based on the entropy source of LED^a

Year	Generation rate	Post-processing	Approaches	Integration level	Real time	Reference
2014	3 Gb/s	w/	Photon number measurements	Discrete components	No	[18]
2015	200 Mb/s	w/	Photon number measurements	Partial chip-level integration	Yes	[19]
2015	1Mb/s	w/	Photon arrival time measurements	Full chip-level integration	Yes	[20]
2017	1.68 Mb/s	w/o	Photon arrival time measurements	Discrete components	Yes	[21]
2018	0.5 Mb/s	w/o	Photon arrival time measurements	Discrete components	Yes	[22]
2021	43 Mb/s	w/	Intensity fluctuation of spontaneous emission	Partial chip-level integration	No	[23]
2021	400 Mb/s	w/	Photon arrival position distribution	Partial chip-level integration	Yes	[24]
2023	10.35 Mb/s	w/o	Projective measurements on weak coherent polarization states	Discrete components	Yes	[25]
2024	1 Mb/s	w/	Intensity fluctuation of spontaneous emission	Full chip-level integration	Yes	[26]
This report	9.375 Gb/s	w/	Intensity fluctuation of spontaneous emission	Discrete components	No	

^aw/: with; w/o: without.

layer and a 1.4 μm unintentionally doped (UID) GaN layer are deposited on a patterned sapphire substrate (PSS), which facilitates improved light extraction and high-intensity spontaneous emission. This optimized epitaxial design ensures uniform device performance across the wafer, a crucial factor for employing micro-LEDs as compact entropy sources in QRNGs.

Figure 1. (a) indicates the pictures for different sizes of micro-LEDs under different injection currents. The EL intensity measurement of micro-LEDs under different injection currents is shown in Fig. 1. (b). The spectral blue shift as the decreasing sizes of micro-LEDs is primarily attributed to enhanced quantum confinement, which increases the bandgap energy by confining carriers to smaller spatial dimensions. Additionally, effective strain relaxation in smaller LEDs reduces the lattice mismatch-induced stress, further modifying the band structure and contributing to the blue shift. The blue shift observed with increasing injection current arises from two primary mechanisms: the screening of the quantum-confined stark effect (QCSE), which mitigates the internal electric field in quantum wells, and the enhanced carrier band-filling effect [36,37]. As injection current density increases, the higher density of carriers populates higher energy states within the conduction and valence bands, leading to an overall shift toward shorter wavelengths in the emitted spectrum. The inset in Fig. 1. (b) indicates the output power of micro-LEDs with the changing of injection current density. Smaller sizes of micro-LEDs can sustain high current density while maintaining lower power compared to larger sizes of micro-LEDs at the same injection current density. The $5 \times 5 \mu\text{m}^2$ micro-LED can sustain an extremely high current density of 40 kA/cm^2 , presenting the stability of ALD passivated micro-LEDs. The $100 \times 100 \mu\text{m}^2$ micro-LED can reach the highest output power of 107 mW.

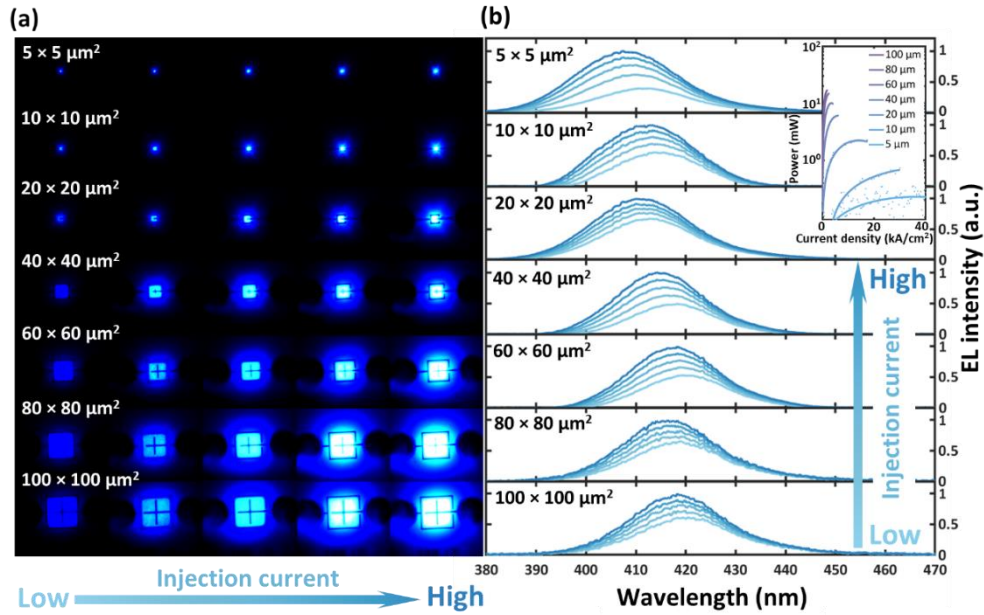


Fig. 1. (a) Photos of different sizes of micro-LEDs under different injection currents. Each row has 5 pictures of a single-size micro-LED taken at the same exposure time. (b) Electroluminescence (EL) characteristics of different sizes of micro-LEDs ranging from $5 \times 5 \mu\text{m}^2$ to $100 \times 100 \mu\text{m}^2$ from low (light blue) to high (dark blue) injection current. The inset plot shows the output power of different sizes of micro-LEDs under different current densities.

3. Micro-LED-based quantum random number generation

The quantum randomness in micro-LED intensity fluctuations originates from spontaneous emission. In quantum electrodynamics, spontaneous emission occurs when an electron in an excited state randomly decays to a lower energy state, emitting a photon in the process. The emission power of micro-LED is related to the quantum uncertainty of photon transition probability.

To extract quantum random bits, the micro-LED is mounted on a thermoelectric cooler (TEC) set to 17°C . The emitted light is collimated using a Nikon 20 \times objective lens and focused onto a silicon avalanche photodetector (APD) via a dichroic beamsplitter and a bi-convex lens. The optical intensity is detected by the APD, which has a limited bandwidth of 400 MHz. An amplifier amplifies the alternating current (AC) component of the detected signal while suppressing the direct current (DC) component. The amplified signal is then digitized by an oscilloscope with a sampling rate of 1.5625 GS/s. To maximize the extracted bits, the AC signal is adjusted to fully utilize the oscilloscope's dynamic range without clipping. The APD amplification and oscilloscope voltage range are finely tuned based on the size and operating current of each micro-LED. Power to the micro-LEDs is supplied by a source meter (Keithley 2420) using ground signal (GS) probes. The experimental setup is illustrated in Fig. 2(a).

The data collected is then sent to the computer for proceedings. As illustrated in Fig. 2. (b), there are two post-processing steps applied. First, the whole signal will go through self-subtraction. The original signal $S(t)$ is divided into two equal-length, non-overlapping segments $S_1(t_1)$ and $S_2(t_2)$, corresponding to distinct temporal intervals, where $t = t_1 + t_2$. Then, the subtracted signal is represented as $S_f = S_1(t_1) - S_2(t_2)$. By adopting self-extraction, the unwanted bias can be removed [11]. Moreover, since the subtraction can produce values that exceed the

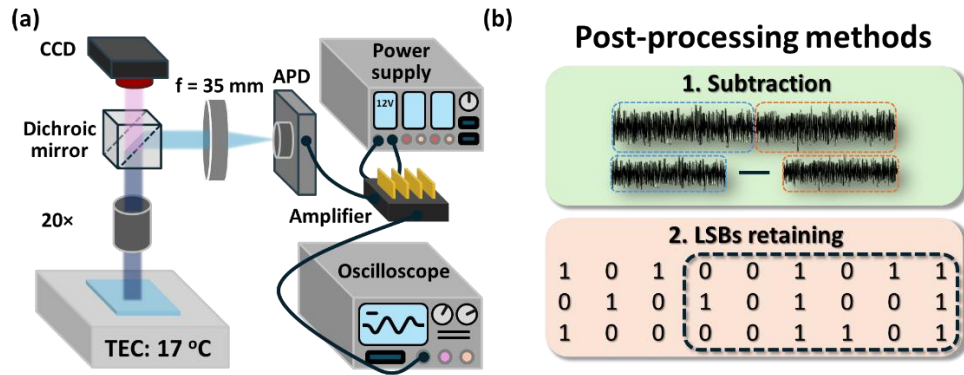


Fig. 2. (a) Experimental setup of QRNG, which consists of a thermoelectric cooler (TEC, LDC-3900) set at 17°C, a 20× objective lens, a dichroic beamsplitter (DMLP490), a charge-coupled device (CCD) camera, a bi-convex lens with focus length of 35 mm (LB1811, $f = 35$ mm), a silicon avalanche photodetector (APD430A2/M), an amplifier (ZVA-183WA-S+), a power supply (E36312ADC), an oscilloscope (DPO 72004C). (b) Post-processing methods to extract quantum random bits after extracting signals from the oscilloscope.

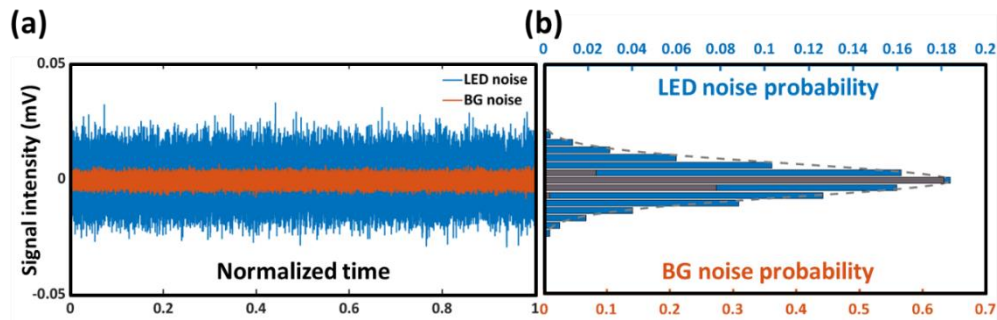


Fig. 3. (a) Signal intensity of LED noise at an injection current of 1 mA and background (BG) noise with normalized time. (b) Probability distribution of LED noise and BG noise.

range of original signals, requiring an additional bit to represent the result accurately, the 8-bit signal S_1 becomes 9-bit signal S_2 due to the increase in the dynamic range of the result. After subtraction, LSBs retention is performed to remove the correlation of the bits. The LSB refers to the rightmost bit in a binary number representation. It preserves inherent unpredictability without affecting the overall signal's main characteristics. After subtraction, LSBs retention ensures the preservation of critical fine-grained variations in the signal, capturing noise and subtle fluctuations that contribute to randomness. This process is essential for applications such as quantum random number generation, where the unpredictability of these small-scale features underpins the statistical quality and security of the generated numbers. In our case, since we let the optical noise occupy the whole screen of the oscilloscope, the noise can offer a total range of 8 bits and 9 bits after subtracting. Figure 3. (a) shows the signal intensity comparison between $5 \times 5 \mu\text{m}^2$ micro-LED noise under an injection current of 1 mA and BG noise. BG noise is the signal measured when the micro-LED is off, mainly contains classical noises from the electrical part, including APD, amplifier, and other electronic devices. It's obvious that LED noise dominates the overall signal. It can be found from Fig. 3. (b) that LED noise has an approximate intensity probability of Gaussian distribution. The dashed line shows the Gaussian

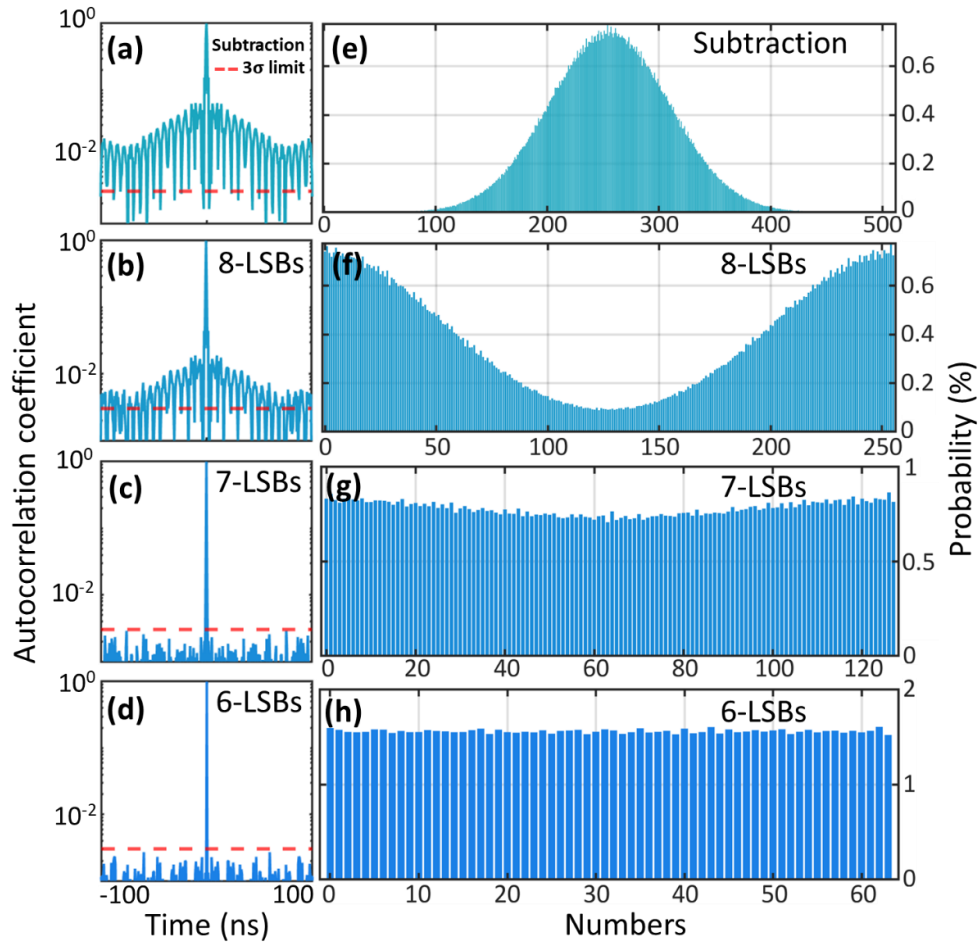


Fig. 4. (a) Autocorrelation coefficient of signal extracted from $5 \times 5 \mu\text{m}^2$ micro-LED under an injection current of 1 mA after subtraction and m-LSBs ($m = 8, 7, 6$) retention. The red dash exhibits 3σ limits of the random bits. (b) Histogram of random bits extracted from $5 \times 5 \mu\text{m}^2$ micro-LED under an injection current of 1 mA after subtraction and m-LSBs ($m = 8, 7, 6$) retention.

fitting results for LED noise probability. The BG noise probability, represented by the orange bar, exhibits a bias that can be reduced through subtraction.

To expose time correlation and periodicity, autocorrelation coefficient of signal extracted from $5 \times 5 \mu\text{m}^2$ micro-LED are calculated after different post-processing schemes and the results as a function of delay are shown in Fig. 4. (a-d). The red dashed lines represent the 3σ limits of the autocorrelation for truly random bits, which is calculated as $3\sigma = \frac{3}{\sqrt{N}}$ (N is the length of the data) [38]. If the coefficients lie within these limits, the extracted bits are considered uncorrelated and independent. With subtraction and 8-LSBs retention, some peaks surpass the 3σ limit, indicating potential correlations. Retaining fewer LSBs helps to reduce correlation, with 6-LSBs retention achieving a high performance. The histograms of bits extracted after different post-processing methods are indicated in Fig. 4. (e-h) to show the probability of each bit streams. After subtraction, the histogram stays a Gaussian distribution. When introducing 6-LSBs retention, the probability of different bits is almost the same, indicating difficulty in

predicting the signal. Then, the NIST test suite results of quantum random bits from $5 \times 5 \mu\text{m}^2$ micro-LED after post-processing methods including subtraction and 6-LSBs retention are presented in Table 2 [39]. The tested data contains a series of $350 \times 1 \text{ M}$ random bits with a significance level $\alpha=0.01$, which satisfies the successful conditions that the p-values are larger than 0.0001, and the proportions are above the critical value 340/350. The post-processed signal successfully passes all NIST tests, ensuring the randomness of the signal. With a sampling rate of 1.5625 GS/s and 6-LSBs retention, a 9.375 Gb/s data rate is achieved for the $5 \times 5 \mu\text{m}^2$ micro-LED.

Table 2. NIST test suite results of $5 \times 5 \mu\text{m}^2$ micro-LED under an injection current of 1 mA after post-processing

Statistical Test	P-value	Proportion
Frequency	0.000401	0.971429
Block Frequency	0.269879	0.991429
Cumulative Sums	0.002043	0.974286
Runs	0.728428	0.980000
Longest Run	0.445224	0.991429
Rank	0.711017	0.994286
FFT	0.586684	0.991429
Non-Overlapping Template	0.628196	0.988571
Overlapping Template	0.967596	0.982857
Universal	0.657933	0.997143
Approximate Entropy	0.413884	0.997143
Random Excursions	0.559523	0.985075
Random Excursions Variant	0.652733	0.990050
Serial	0.393698	0.994286
Linear Complexity	0.831811	0.997143

Additionally, Shannon entropy and min-entropy are calculated for the original signal and post-processed signal, which are fundamental concepts in information theory that quantify the uncertainty or randomness of dataset [1]. The Shannon entropy can be described as

$$H(x) = - \sum_{i=1}^n P(x_i) \log_2 P(x_i) \quad (1)$$

where P_x is probability of x_i . The Shannon entropy can give an upper bound of the randomness, which is an inadequate measure when it comes to quantifying randomness, especially when there are extraordinary values. Therefore, min-entropy is also calculated as

$$H_{min}(x) = -\log_2 \left[\max_{x_i \in x} P_x(x_i) \right] \quad (2)$$

Min-entropy is the logarithm of the bin with the highest probability, which is more robust regardless of the distribution of signals when measuring randomness. It quantifies the maximum amount of (almost) uniform randomness that can be extracted out of a distribution. Min-entropy is generally smaller than Shannon entropy, except in the case of a uniform distribution, where the two are equal. For original signal with quasi-Gaussian distribution, $H(x) = 6.7780$, $H_{min} = 5.6222$ because of the bias and some extraordinary values in the original data. After subtraction and 6-LSBs retention, $H(x) = 5.9999$, $H_{min}(x) = 5.9714$, which indicates the elimination of outliers and uniformity of the signal as well as the maximum extracted bits of 6. The reduction in

Shannon entropy arises from the decrease in the number of retained data bits, from 8 bits in the raw data to 6 bits after post-processing. After post-processing, the Shannon entropy is very close to the ideal value of 6, indicating a highly uniform distribution of random bits, which ensures the unpredictability of the output.

The randomness of other sizes micro-LED is also assessed. All of them can pass NIST randomness test suits under a sampling rate of 1.5625 GS/s by implementing post-processing methods including subtraction and 6-LSBs retention. The tested micro-LEDs that successfully passed NIST test suits with different injection current are listed below:

- a) $5 \times 5 \mu\text{m}^2$: Driven by 0.5, 1.0, 1.5 mA DC
- b) $10 \times 10 \mu\text{m}^2$: Driven by 1.0, 1.5, 2.0 mA DC
- c) $20 \times 20 \mu\text{m}^2$: Driven by 1.0, 2.0, 3.0, 4.0 mA DC
- d) $40 \times 40 \mu\text{m}^2$: Driven by 1.0, 2.0, 3.0, 4.0, 16 mA DC
- e) $60 \times 60 \mu\text{m}^2$: Driven by 10, 20, 30, 36, 40 mA DC
- f) $80 \times 80 \mu\text{m}^2$: Driven by 20, 30, 40, 50, 60, 64, 70 mA DC
- g) $100 \times 100 \mu\text{m}^2$: Driven by 40, 50, 60, 70, 80, 90, 100 mA DC

For larger sizes of micro-LEDs, with higher output power at the same injection current density, they can obtain larger intensity fluctuations and successfully pass NIST test suits. However, the quantum random number generation rates of all micro-LED devices under different injection current are limited to 9.375 Gb/s due to the constrained 400 MHz bandwidth of APD implemented in the experiment. A higher RNG rate is expected to be achieved with high-speed PD, which can be evaluated in the future work.

During the experiment, another post-processing method, including self-delayed exclusive-or (XOR) and LSB retention, is also evaluated to confirm the micro-LED as an effective entropy source for QRNG. We found that self-delayed XOR enables a higher generation rate of 600 Gb/s. However, it compromises the inherent quantum randomness of the optical noise. To validate the quantum randomness of the collected optical signal, BG noise was subjected to two post-processing methods for comparison. In the first method involving subtraction followed by retaining LSBs, the BG noise failed to pass the NIST test suite. In contrast, the second method, which combined LSB retention with self-delayed XOR, enabled the BG noise to successfully pass the NIST test suite. These results indicate that self-delayed XOR can independently introduce randomness, thereby diluting the quantum randomness originating from the micro-LED's spontaneous emission. Therefore, the post-processing method, including subtraction and LSB retention, was finally chosen to be implemented in our system.

Beyond the post-processing algorithms discussed earlier, future work could further enhance our system by incorporating advanced randomness extractors such as the Toeplitz and Trevisan hash functions. The Toeplitz extractor, with its inherent structure based on Toeplitz matrices, offers significant advantages in terms of extraction efficiency and the ability to leverage parallel computation [40–42]. This makes it particularly attractive for high-throughput applications where real-time processing is crucial. In contrast, Trevisan's extractor is renowned for its strong security guarantees—it provides information-theoretic security even against quantum adversaries, making it an ideal choice for applications with stringent security requirements [43]. By integrating these two approaches, our micro-LED-based QRNG system can not only achieve high-speed performance but also meet the robust security standards required for broader applications, such as quantum key distribution and other advanced cryptographic systems.

In our experiment of micro-LED-based QRNG, the quantum random number generation rate is limited by the responsivity and bandwidth of the PD. With a low responsivity of around 23

A/W for APD430 at the wavelength of 400 nm, it is difficult for micro-LEDs to obtain higher bits and suppress classical noise, which dilutes the quantum noise. Also, the -3 dB bandwidth of 400 MHz limits the detection of the high-speed intensity fluctuation and finally limits the RNG rates.

Compared to other QRNG works, micro-LEDs offer a unique advantage due to their dual functionality as light emitters and high-speed PDs. Previous studies have demonstrated that micro-LEDs operating at wavelengths around 400 nm can achieve bandwidths exceeding 1 GHz, making them suitable for high-speed optoelectronic applications [44]. Furthermore, the surface-emitting nature of micro-LEDs facilitates the straightforward formation of two-dimensional arrays, enabling parallel multi-channel QRNG to significantly boost generation rates. For example, in this study, a single micro-LED achieves a quantum bit generation rate of 9.375 Gb/s. Extending this to a 2×2 array results in a combined rate of 37.5 Gb/s, with scalability to larger arrays offering virtually limitless potential for speed enhancement. Additionally, micro-LEDs and PDs can be vertically integrated. It is simply realized by depositing ZnO PD on the backside of sapphire substrate [45]. Based on this scheme, it is possible to monolithically integrate a multi-channel QRNG on a single chip. Because of the transparency of sapphire and back emission of micro-LED, the emitted optical signals from the micro-LEDs are directly received by the integrated PDs, where they are converted into electrical signals. These electrical signals can then undergo post-processing to yield stable quantum random bits. This integrated design not only simplifies the system architecture but also overcomes the bandwidth limitations of external PD used in this experiment. As a result, each channel's generation rate could be further increased, limited only by the electronic device response time rather than the intrinsic quantum processes. This capability underscores the vast potential of micro-LED-based QRNG systems to meet future demands for high-speed, scalable, and compact quantum random number generation solutions.

4. Conclusions

In summary, our study establishes micro-LEDs as a highly efficient and scalable platform for quantum random number generation. By leveraging subtraction techniques and 6-LSB retention, we demonstrate that individual micro-LEDs, with sizes ranging from $5 \times 5 \mu\text{m}^2$ to $100 \times 100 \mu\text{m}^2$, consistently achieve a remarkable bit generation rate of 9.375 Gb/s. The micro-LEDs' compact footprint, exceptional efficiency, and compatibility with scalable chip-based architectures position them as an ideal solution for high-throughput QRNG systems. Furthermore, their ability to form 2D arrays enables parallel QRNG implementations, significantly enhancing potential throughput and scalability. This capability underscores their transformative potential in secure communication and quantum computing applications. These findings highlight the remarkable versatility, performance, and scalability of micro-LED-based QRNGs, potentially establishing them as a cornerstone technology for future adoption of LEDs as random number generators in a plethora of application scenarios.

Funding. King Abdullah University of Science and Technology (FCC/1/5939, RFS-OPF2023-5534, FCC/1/5937, ORFS-2022-CRG11-5079, BAS/1/1614-01-01, ORA-2022-5313); KACST-UCSB Center of Excellence.

Disclosures. The authors declare no conflicts of interest.

Data availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

References

1. J. Y. Haw, S. M. Assad, and P. K. Lam, "Secure random number generation in continuous variable systems," in *Quantum Random Number Generation* (Springer, 2020), pp. 85–112.
2. W. Schindler, "Random number generators for cryptographic applications," in *Cryptographic Engineering* (Springer, 2009), pp. 5–23.
3. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science* **560**, 7–11 (2014).
4. P. L'Ecuyer, "Random numbers for simulation," *Commun. ACM* **33**(10), 85–97 (1990).

5. N. Metropolis and S. Ulam, "The Monte Carlo method," *J. Am. Stat. Assoc.* **44**(247), 335–341 (1949).
6. D. J. Gauthier, E. Bollt, A. Griffith, *et al.*, "Next generation reservoir computing," *Nat. Commun.* **12**(1), 5564 (2021).
7. F. James, "A review of pseudorandom number generators," *Comput. Phys. Commun.* **60**(3), 329–344 (1990).
8. M. Drutarovsky and P. Galajda, "A Robust Chaos-Based True Random Number Generator Embedded in Reconfigurable Switched-Capacitor Hardware," in *2007 17th International Conference Radioelektronika* (IEEE, 2007), pp. 1–6.
9. Y. Yang, G. Bai, and H. Chen, "A 200Mbps random number generator with jitter-amplified oscillator," in *Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT)* (2014), pp. 1–5.
10. A. Uchida, K. Amano, M. Inoue, *et al.*, "Fast physical random bit generation with chaotic semiconductor lasers," *Nature Photonics* **2**(12), 728–732 (2008).
11. H. Lu, O. Alkhazragi, Y. Wang, *et al.*, "Parallel On-Chip Physical Random Number Generator Based on Self-Chaotic Dynamics of Free-Running Broad-Area VCSEL Array," *IEEE J. Select. Topics Quantum Electron.* **31**(2: Pwr. and Effic. Scaling in), 1–11 (2025).
12. H. Schmidt, "Quantum-mechanical random-number Generator," *J. Appl. Phys.* **41**(2), 462–468 (1970).
13. Y.-Q. Nie, H.-F. Zhang, Z. Zhang, *et al.*, "Practical and fast quantum random number generation based on photon arrival time relative to external reference," *Appl. Phys. Lett.* **104**(5), 051110 (2014).
14. Q. Yan, B. Zhao, Q. Liao, *et al.*, "Multi-bit quantum random number generation by measuring positions of arrival photons," *Rev. Sci. Instrum.* **85**(10), 103116 (2014).
15. B. Qi, Y.-M. Chi, H.-K. Lo, *et al.*, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," *Opt. Lett.* **35**(3), 312–314 (2010).
16. Y. Shen, L. Tian, and H. Zou, "Practical quantum random number generator based on measuring the shot noise of vacuum states," *Phys. Rev. A* **81**(6), 063814 (2010).
17. J. Yang, F. Fan, J. Liu, *et al.*, "Randomness quantification for quantum random number generation based on detection of amplified spontaneous emission noise," *Quantum Sci. Technol.* **6**(1), 015002 (2021).
18. B. Sanguinetti, A. Martin, H. Zbinden, *et al.*, "Quantum Random Number Generation on a Mobile Phone," *Phys. Rev. X* **4**(3), 031056 (2014).
19. S. Tisa, F. Villa, A. Giudice, *et al.*, "High-Speed Quantum Random Number Generation Using CMOS Photon Counting Detectors," *IEEE J. Select. Topics Quantum Electron.* **21**(3), 23–29 (2015).
20. A. Khanmohammadi, R. Enne, M. Hofbauer, *et al.*, "A Monolithic Silicon Quantum Random Number Generator Based on Measurement of Photon Detection Time," *IEEE Photonics J.* **7**(5), 1–13 (2015).
21. Z. Bisadi, G. Fontana, E. Moser, *et al.*, "Robust Quantum Random Number Generation With Silicon Nanocrystals Light Source," *J. Lightwave Technol.* **35**(9), 1588–1594 (2017).
22. Z. Bisadi, F. Acerbi, G. Fontana, *et al.*, "Compact quantum random number generator with silicon nanocrystals light emitting device coupled to a silicon photomultiplier," *Front. Phys.* **6**, 314963 (2018).
23. Y.-Y. Hu, Y.-Y. Ding, S. Wang, *et al.*, "Compact quantum random number generation using a linear optocoupler," *Opt. Lett.* **46**(13), 3175 (2021).
24. F. Regazzoni, E. Amri, S. Burri, *et al.*, "A High Speed Integrated Quantum Random Number Generator with on-Chip Real-Time Randomness Extraction," *arXiv* (2021).
25. J. Argillander, A. Alarcón, C. Bao, *et al.*, "Quantum random number generation based on a perovskite light emitting diode," *Commun. Phys.* **6**(1), 157 (2023).
26. M. Moeni, M. Akbari, M. Mirsadeghi, *et al.*, "Quantum random number generator based on LED," *J. Appl. Phys.* **135**(8), 084402 (2024).
27. J. J. Bird, A. Ekárt, and D. R. Faria, "On the effects of pseudorandom and quantum-random number generators in soft computing," *Soft Comput.* **24**(12), 9243–9256 (2020).
28. D. Cirauqui, M. Á. García-March, G. G. Corominas, *et al.*, "Comparing pseudo- and quantum-random number generators with Monte Carlo simulations," *APL Quantum* **1**(3), 036125 (2024).
29. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, *et al.*, "The security of practical quantum key distribution," *Rev. Mod. Phys.* **81**(3), 1301–1350 (2009).
30. Y. Guo, Q. Cai, P. Li, *et al.*, "40 Gb/s quantum random number generation based on optically sampled amplified spontaneous emission," *APL Photonics* **6**(6), 066105 (2021).
31. C. R. S. Williams, J. C. Salevan, X. Li, *et al.*, "Fast physical random number generator using amplified spontaneous emission," *Opt. Express* **18**(23), 23584–23597 (2010).
32. L. Allen and G. I. Peters, "Spectral distribution of amplified spontaneous emission," *J. Phys. A: Gen. Phys.* **5**(5), 695–704 (1972).
33. A. Pandey, M. Reddeppa, and Z. Mi, "Recent progress on micro-LEDs," *Light: Advanced Manufacturing* **4**(4), 519–542 (2024).
34. M. S. Wong, S. Nakamura, and S. P. DenBaars, "High external quantum efficiency III-nitride micro-light-emitting diodes," in *Semiconductors and Semimetals* (Elsevier, 2021), 106, pp. 95–121.
35. I. Reidler, Y. Aviad, M. Rosenbluh, *et al.*, "Ultrahigh-speed random number generation based on a chaotic semiconductor laser," *Phys. Rev. Lett.* **103**(2), 024102 (2009).
36. T. Takeuchi, S. Sota, M. Katsuragawa, *et al.*, "Quantum-confined Stark effect due to piezoelectric fields in GaInN strained quantum wells," *Jpn. J. Appl. Phys.* **36**(4A), L382 (1997).
37. B.-J. Pong, C.-H. Chen, S.-H. Yen, *et al.*, "Abnormal blue shift of InGaN micro-size light emitting diodes," *Solid-State Electron.* **50**(9–10), 1588–1594 (2006).

38. V. N. Chizhevsky, "Symmetrization of single-sided or nonsymmetrical distributions: The way to enhance a generation rate of random bits from a physical source of randomness," *Phys. Rev. E* **82**(5), 050101 (2010).
39. S.-J. Kim, K. Umeno, and A. Hasegawa, "Corrections of the NIST Statistical Test Suite for Randomness," *arXiv* (2004).
40. X. Guo, F. Lin, J. Lin, *et al.*, "Parallel and real-time post-processing for quantum random number generators," *arXiv* (2024).
41. F. Lin, W. Ge, Z. Song, *et al.*, "Seed Renewable Parallel and Real-Time Toeplitz Post-Processing for QRNG," *J. Lightwave Technol.* **42**(24), 8606–8615 (2024).
42. A. K S V, G. Raghavan, and K. R. P. "High-efficiency implementation of Toeplitz Strong Extractor for PRNG and QRNG output on CPU/GPU hardware systems," *Phys. Scr.* **99**(7), 075115 (2024).
43. X. Ma, F. Xu, H. Xu, *et al.*, "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction," *Phys. Rev. A* **87**(6), 062327 (2013).
44. J. Shi, Z. Xu, W. Niu, *et al.*, "Si-substrate vertical-structure InGaN/GaN micro-LED-based photodetector for beyond 10 Gbps visible light communication," *Photonics Res.* **10**(10), 2394–2404 (2022).
45. H. Yu, J. Yao, M. H. Memon, *et al.*, "Vertically integrated self-monitoring AlGaIn-based deep ultraviolet micro-LED array with photodetector via a transparent sapphire substrate toward stable and compact maskless photolithography application," *Laser Photonics Rev.* **19**(2), 2401220 (2025).