SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

June 2026, Vol. 69, Iss. 6, 162501:1–162501:11
https://doi.org/10.1007/s11432-025-4660-1

Highly integrated broadband entropy source for quantum random number generators based on vacuum fluctuations

Xuyang WANG[1,2,3*], Yuqi SHI[1], Ning WANG[2,4], Jie YUN[1], Jiaxu LI[4], Yanxiang JIA[1], Shuaishuai LIU[1], Zhenguo LU[1,2], Jun ZOU[5] & Yongmin LI[1,2,3*]

[1]*State Key Laboratory of Quantum Optics Technologies and Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China*
[2]*Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, China*
[3]*Hefei National Laboratory, Hefei 230088, China*
[4]*College of Physics and Electronic Engineering, Shanxi University, Taiyuan 030006, China*
[5]*ZJU-Hangzhou Global Scientific and Technological Innovation Center, Zhejiang University, Hangzhou 311215, China*

Received 30 April 2025/Revised 13 August 2025/Accepted 31 October 2025/Published online 9 February 2026

Abstract In this work, we designed and experimentally verified a highly integrated broadband entropy source for a quantum random number generator (QRNG) based on vacuum fluctuations. The core of the entropy source is a hybrid laser-and-silicon-photonics chip, which is only 6.3 mm × 2.6 mm × 1.5 mm in size. A balanced homodyne detector based on cascaded radio-frequency amplifiers in the entropy source achieves a 3-dB bandwidth of 2.4 GHz and a common-mode rejection ratio above 25 dB. The quantum-to-classical-noise ratio is 9.51 dB at a photoelectron current of 1 mA. The noise equivalent power and equivalent transimpedance at 0.1 GHz are 8.85 pW/$\sqrt{\text{Hz}}$, and 22.8 kΩ, respectively. A trusted-device-dependent security framework that takes into account both classical and quantum side information is employed to calculate the minimum entropy. The equalization technology is used to extend the bandwidth and minimize the correlations between adjacent samples. The quantum random number generation rate reaches 58.24 Gbps. The developed hybrid chip enhances the integrability and speed of QRNG entropy sources based on vacuum fluctuations.

Keywords quantum random number generator, integrated entropy source, equalizer, balanced homodyne detector

Citation Wang X Y, Shi Y Q, Wang N, et al. Highly integrated broadband entropy source for quantum random number generators based on vacuum fluctuations. Sci China Inf Sci, 2026, 69(6): 162501, https://doi.org/10.1007/s11432-025-4660-1

1 Introduction

Quantum random number generators (QRNGs), which can produce true random numbers with high unpredictability, irreproducibility, and unbiasedness, are guaranteed by the basic principles of quantum physics [1,2]. QRNGs play an essential role in various applications, such as quantum communication, quantum simulations, and many fundamental physical experiments [3–17]. As a crucial element of quantum networks, quantum communication enables the global deployment of a wide range of quantum technologies and protocols, such as QRNGs, quantum repeaters [18, 19], multiparty quantum conferencing [20, 21]. It is anticipated that the number of quantum devices in a quantum network and corresponding energy consumption will increase exponentially over time [18]. Chip-level QRNGs can significantly reduce cost and energy consumption. However, a major challenge is the integration of light sources, waveguides, photodiodes, and transimpedance amplifiers (TIAs) in a single material simultaneously. The silicon photonics (SiPh) technology, which employs silicon-on-insulator (SOI) wafers as semiconductor substrate materials, is compatible with complementary metal-oxide-semiconductor (CMOS) fabrication. This means that most standard CMOS manufacturing processes can be used for SiPh device production, and the technology can monolithically integrate silicon electronics and photonics into the same platform [22]. Although the indirect bandgap of silicon prevents the direct generation of laser beams in SiPh chips, a hybrid or heterogeneous integration method can incorporate the laser and SiPh chips into a monolithically integrated entropy source [23, 24]. Therefore, the overall entropy source is feasible to be highly integrated. The SiPh technology combined with hybrid or heterogeneous integration technologies can enable high-rate QRNG entropy sources with small size, low power consumption, and low cost [25].

* Corresponding author (email: wangxuyang@sxu.edu.cn, yongmin@sxu.edu.cn)

Table 1 Brief summary of integrated trusted-device QRNGs and BHDs.

Year	QRNG or BHD	3-dB bandwidth	Rate (Gbps)	Stage	Integrated chip
2018	QRNG [55]	150 MHz	1.2	1	SiPh chip
2021	QRNG [56]	3.5 GHz	18.8	1	SiPh chip
2021	BHD [57]	1.5 GHz	–	1	SiPh chip
2021	BHD [61]	1.7 GHz	–	1	SiPh chip
2023	QRNG [58]	1.5 GHz	100	1	SiPh chip
2024	QRNG [59]	4.75 GHz	240	1	SiPh chip
2024	BHD [60]	1.5 GHz	–	1	SiPh chip
2024	BHD [62]	15.3 GHz	–	2	SiPh chip & TIA (monolithic electronic-photonic integration)
2025	QRNG(current work)	2.4 GHz	58.24	2	Laser chip & SiPh chip (hybrid integration)

In the past two decades, there has been tremendous development for QRNGs: trusted device, device independent (DI), and semi-DI. DI-QRNGs achieve robustness against general classical and quantum side information through the loophole-free violation of a Bell inequality. This implementation requires a high-quality entanglement source and high-efficiency detectors, and currently limits the generation rate to only hundreds of bits per second [26–28]. In semi-DI QRNGs, either the source or the measurement device is untrusted while the other part remains trusted. Techniques including the entropic uncertainty principle [29], tomography, and semi-definite programming have been employed to analyze side information leakage from untrusted components [30,31]. However, these protocols exhibit a security-rate trade-off, typically achieving rates about one order of magnitude lower than those achieved by fully trusted counterparts. Trusted-device QRNGs prioritize high-speed and easy implementation, and they target applications where speed and integration are critical, such as exponentially growing quantum networks.

In this study, we focused on trusted-device QRNGs. Our certification model relies on a trusted vacuum state, a characterized homodyne detector, and the specific Gaussian classical noise (also called side information) [32]. Among various ways for quantum random number generation [33–48]—such as photon counting, amplified spontaneous emission, phase noise, vacuum fluctuations, and others—vacuum fluctuations offer several advantages [32–34]. First, vacuum noise is a readily available source of entropy, avoiding the need for bulky external components. Second, the excess noise in a local oscillator is inherently canceled using balanced detection, relaxing requirements on the laser and increasing the system's resilience against external perturbations. Furthermore, the bandwidth of a balanced homodyne detector (BHD) can be extended to tens of gigahertz. Third, all optic devices can be integrated into chips. Hence, high-performance trusted device QRNGs based on vacuum fluctuations have been extensively explored [25, 49–54].

In recent years, SiPh-based vacuum fluctuation entropy sources have made significant progress, and their performance has steadily improved. In 2018, a QRNG with a generation rate of 1.2 Gbps was realized with a 150 MHz (3-dB bandwidth) homodyne detector on a SiPh chip [55]. In 2021, a QRNG with a generation rate of 18.8 Gbps based on an integrated 3.5 GHz homodyne detector was reported [56]. In the same year, an integrated 1.5 GHz homodyne detector with improved TIA circuits was designed [57]. The shot noise limited whole bandwidth of the BHD was 20 GHz. Later, the researchers achieved a quantum random number generation rate of 100 Gbps using the equalizer technology in 2023 [58]. In 2024, the generation rate was boosted to 240 Gbps [59]. For SiPh integration of BHDs, 3-dB bandwidths of 1.5 GHz [60], 1.7 GHz [61], and 15.3 GHz [62] were also reported. The BHD with 3-dB bandwidth of 15.3 GHz was enabled by monolithic electronic-photonic integration, which goes below the capacitance limits of devices made up of separate integrated chips or discrete components. It exceeds the bandwidth of quantum detectors with macroscopic electronic interconnects, including wire and flip-chip bonding.

Table 1 summarizes existing high-speed integrated QRNGs or BHDs at different integration stages. Here, we define the integration of a 50/50 coupler, two series-connected photodiodes, and connected waveguides into a SiPh chip as "Stage 1"; integration of any two of the three parts of the entropy sources (which are typically a laser chip, a SiPh chip, and an amplifier chip) as "Stage 2"; and integration of the overall entropy source into a single chip as "Stage 3". In the above work, simple wire bonding between the SiPh chip and TIA chips or other amplifier chips is not defined as an integration stage. Obviously, when the stage is higher, the volume of entropy is smaller, cost and power consumption are lower, and the quantum generation rate will have the potential to achieve a higher level.

Notably, the entropy sources of the previous high-speed on-chip QRNGs lacked integrated laser sources, and the laser beam was guided into SiPh chips through a fiber with a grating or edge coupler. Integrating the laser chip with the SiPh chip eliminates a bulky laser source and greatly reduces the size, power consumption, and cost of

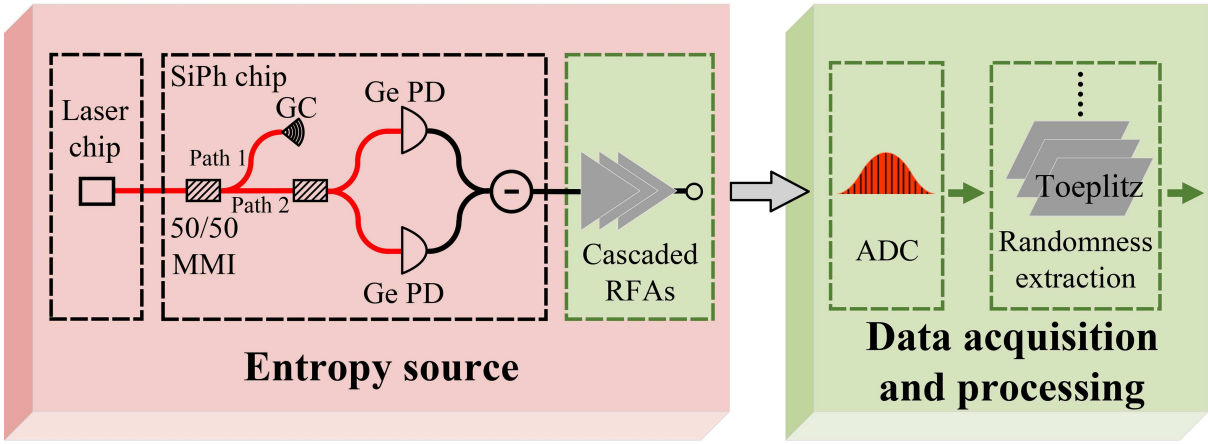

Figure 1 (Color online) Structure of our QRNG based on vacuum fluctuations. GC: grating coupler; PD: photodiode; MMI: multimode interferometer; RFAs: radio-frequency amplifiers; ADC: analog to digital converter.

QRNG entropy source.

In this study, we presented a highly integrated broadband QRNG entropy source based on vacuum fluctuations. The overall size of the hybrid chip, which comprised an indium phosphide (InP) distributed feedback (DFB) laser chip and a SiPh chip, was 6.3 mm × 2.6 mm × 1.5 mm. With cascaded radio-frequency amplifiers, the BHD with a 3-dB bandwidth of 2.4 GHz and a common-mode rejection ratio (CMRR) above 25 dB was achieved. The observed quantum-to-classical-noise ratio (QCNR) was 9.51 dB at a photoelectron current of 1 mA. To achieve a tighter minimum entropy, a trusted-device-dependent security framework that takes into account both classical and quantum side information is employed. Especially, the nonlinear behavior of the analog to digital converter (ADC) is accounted for to obtain an accurate estimate of the generation rate. An effective method to calculate the minimum entropy in the non-independent and identically distributed (non-IID) case is used. The limited bandwidth is augmented digitally by applying detector equalization, which can also minimize correlations between adjacent samples. Finally, we demonstrated an integrated QRNG with an ultrafast generation rate of 58.24 Gbps, representing the highest speed for an integrated QRNG at integration Stage 2.

2 Structure and packaging of the integrated entropy source

Figure 1 shows the structure of our QRNG based on vacuum fluctuations. The main components are the entropy source and the data acquisition and processing module. The entropy source (the core of the QRNG) comprised a laser chip, a SiPh chip, and radio-frequency amplifiers (RFAs). The entropy source outputs Gaussian white noise signals composed of shot noise (quantum noise) and electronic noise (classical noise), which are acquired by the data acquisition module through an ADC. Then, the data processing module estimates the minimum entropy and extracts the random numbers using a Toeplitz matrix.

The SiPh chip, which consists of a butt coupler, two 1× 2 multimode interferometer (MMI) couplers with a 50/50 splitting ratio, two series-connected germanium (Ge) photodiodes, and their connected waveguides, was fabricated using the industry-standard active flow SOI technology of CUMEC. The SiPh chip is 2.5 mm × 2.5 mm × 0.8 mm in size. The 1550 nm laser beam emitted by the InP edge-emitting DFB laser chip is coupled into the SiPh chip using the butt coupler with an insertion loss of 2.5 dB. The polarization of the laser beam is parallel to the plane of the SiPh chip and transformed into a transverse electric mode beam in the waveguide. The beam was then split by the 1 × 2 MMI coupler. In the SiPh chip, path 1 is connected to the grating coupler for aligning in package and path 2 is used to generate shot noise. To simplify the structure, a 1 × 2 MMI coupler with a high degree of balance is used instead of a 2 × 2 MMI coupler, and no balance structures at the coupler outputs are required. The two output beams are directly injected into the two series-connected Ge photodiodes, each with a response of 0.9 A/W.

To integrate the laser chip into the entropy source, we designed an aluminum nitride ceramic mount (Mount A) with good heat conduction. As shown in Figure 2(a). Au pads 1 and 4 connected the DFB laser chip to the constant current sources of outside circuits and pads 2 and 3 were used to connect a thermal resistor (which was unused here because the low heat generated by the laser chip required no temperature control). The cathode side of the laser chip was soldered to pad 1 using the flip-chip method and the anode side was connected to pad 4 via wire bonding (Figure 2(b)). The laser chip has a size of 1 mm × 0.25 mm × 0.12 mm and protrudes 40 μm from

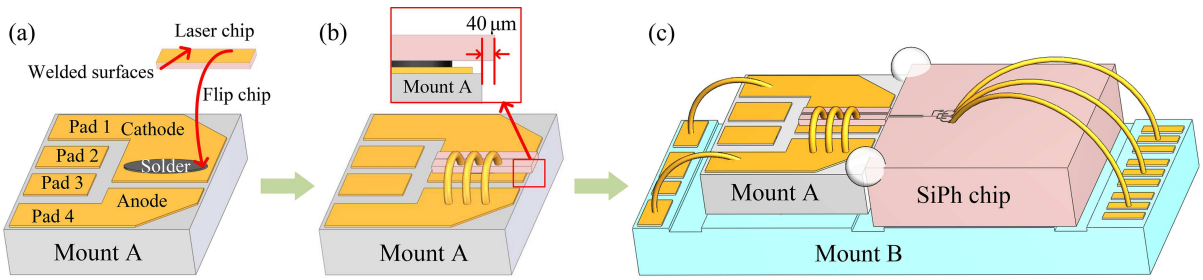

Figure 2 (Color online) Integration of the laser and SiPh chips. (a) Mount A; (b) mount A with a flip-chipped laser chip; (c) the packaged hybrid chip.

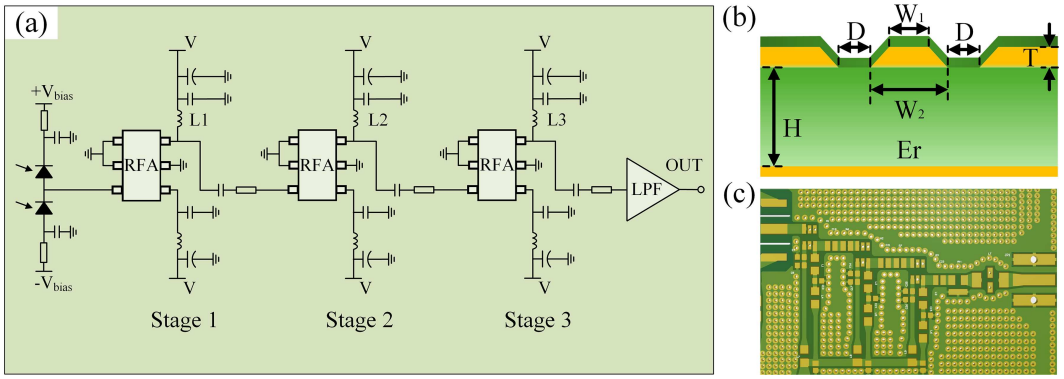

Figure 3 (Color online) Circuit diagram and the layout of cascaded RFAs circuits. (a) Circuit diagram; (b) the structure of the high-frequency transmission lines; (c) the layout of RFAs circuits. LPF: low-pass filter.

the edge of Mount A along the laser-emitting direction, facilitating the alignment and packaging of the hybrid chip (Figure 2(b), inset).

During packaging, Mount A and the SiPh chip were adhered by applying ultraviolet (UV) glue at the corners of both components, as shown in Figure 2(c). The UV glue seeped into the gap between Mount A and the SiPh chip, ensuring tight bonding. Heat-conducting silver glue was overlaid on the surface of Mount B, fastening the conglutination of Mount A and the SiPh chip as well as enhancing the anti-shaking and durability of the entropy source. After packing, the insertion loss increased to 3.1 dB. Gold-plated welding pads on Mount B connected the SiPh and laser chips to a printed circuit board (PCB).

Figure 3 presents the analog circuits of the BHD in the entropy source. The photoelectron current difference of the two Ge photodiodes is amplified by three-stage cascaded low-noise RFAs ABA52563, fabricated with Avago's HP25 silicon bipolar process. These monolithic silicon amplifiers are internally matched to 50 Ω, and provide excellent gain with a flat broadband response from direct current (DC) up to 3.5 GHz. The cascaded RFAs are connected by capacitors, which block the DC voltage source V and transmit high-frequency signals, and resistors, which act as attenuators to stabilize the analog circuits. Finally, a low-pass filter (LPF) with a 3-dB bandwidth of 3.5 GHz filters the high-frequency interference noises.

Obeying the PCB layout rules is essential for obtaining well-performing high-frequency amplifier circuits. The main considerations are impedance matching and parasitic capacitance and inductance. A good impedance circuit ensures the flatness of high-frequency noise signals. Herein, the sizes of transmission lines and spaces between the lines and copper coatings on the PCB board were designed using the Si9000 software. The structure and parameters of the high-frequency transmission lines are shown in Figure 3(b) and Table 2, respectively.

Figure 3(c) presents the layout of cascaded RFAs circuits on the PCB. Small-sized electronic components were exploited to minimize parasitic inductance and optimize impedance matching. Because the sizes of many electronic devices (e.g., an LPF and a SubMiniature version A connector) did not match the width of the transmission lines, the transmission line widths were gradually varied to fit these devices while avoiding the reflection of high-frequency signals caused by a drastic change. Furthermore, the space between the bias voltage pads and the common pad was hollowed to reduce the parasitic capacitance parallel to the junction capacitance of the photodiodes. The inductors L1, L2, and L3 were carefully selected as they are sensitive to parasitic capacitance. The spaces between these inductors and the copper coating were enlarged to reduce parasitic capacitance as much as possible.

Figure 4(a) shows the overall integrated hybrid entropy source and its peripheral circuits. Figure 4(b) shows

Table 2 Parameters of the high-frequency transmission lines. 1 mil = 0.0254 mm.

Parameter	Value
Substrate height (H)	57.66 mil
Substrate dielectric (Er)	4.2
Upper trace width (W_1)	47.08 mil
Lower trace width (W_2)	47.08 mil
Ground strip separation (D)	10 mil
Trace thickness (T)	1.4 mil
Impedance (Z)	50 Ω

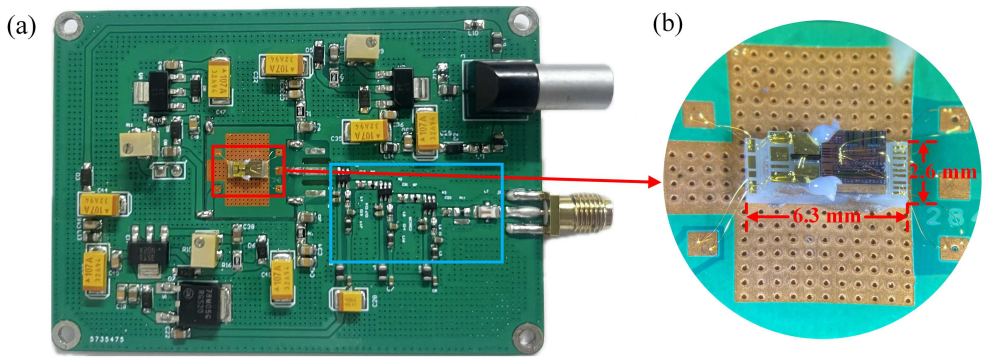

Figure 4 (Color online) (a) Photograph of the integrated entropy source and its peripheral circuits; (b) microphotograph of the hybrid chip.

a micrograph detailing the hybrid chip composed of the laser and SiPh chips (the red rectangle in Figure 4(a)). The hybrid chip, with a size of 6.3 mm × 2.6 mm × 1.5 mm, was fixed on the copper surface of the PCB using silver glue to disperse the generated heat. The hybrid chip was connected to the PCB via wire bonding using 25-μm-diameter golden wires. As the laser power was low (9 mW), no temperature controller was needed. The cascaded RFAs are marked by a blue rectangle. The other circuits involved a voltage source that powered the RFAs and supplied the bias voltage to the photodiodes and a constant current source that powered the laser chip. The electronic components were soldered on the PCB using the reflow soldering technology, ensuring stable and good high-frequency performance. The whole entropy source was enclosed in a metal box to shield it from electromagnetic interference.

3 Characterization of the integrated entropy source

The noise power spectrum of the entropy source at different photoelectron currents from 0 to 4 GHz is presented in Figure 5. The black line represents the inherent noise power of the RF spectrum analyzer. The green line represents the electronic (classical) noise power of the BHD, and the red and blue lines represent the noise powers at photoelectron currents of 0.5 and 1 mA. The measured shot noise was 10.5 dB above the electronic noise when the photoelectron current was 1 mA at 0.1 GHz. The 3-dB bandwidth of the BHD was found to be 2.4 GHz indicated by the blue dotted line.

As shown in Figure 5, the noise power at 0.1 GHz and 1 mA was $P_{\mathrm{M}} = -48.35\,\mathrm{dBm}$. Using the following equation:

$$P\,(\mathrm{dBm}) = 10 \cdot \log_{10}\left(\frac{u^2}{R_{\mathrm{Z}}} \cdot R_{\mathrm{BW}}/10^{-3}\right), \tag{1}$$

where P is the noise power at a specified frequency, u is the output-voltage noise density, and R_{Z} is the input impedance 50 Ω of the RF spectrum analyzer, the output-voltage noise density at 0.1 GHz was calculated to be $u_{\mathrm{M}} = 6.05 \times 10^{-7}\,\mathrm{V}/\sqrt{\mathrm{Hz}}$. Similarly, we obtained the output-voltage noise density of the electronic noise $u_{\mathrm{E}} = 1.82 \times 10^{-7}\,\mathrm{V}/\sqrt{\mathrm{Hz}}$ using $P_{\mathrm{E}} = -58.8\,\mathrm{dBm}$ at 0.1 GHz.

The input-current noise density at photoelectron current of $I_{\mathrm{Q}} = 1$ mA is given by

$$i_{\mathrm{Q}} = \sqrt{2 \cdot q \cdot (2I_{\mathrm{Q}})} = 2.53 \times 10^{-11}\,\mathrm{A}/\sqrt{\mathrm{Hz}}, \tag{2}$$

where q is the charge of a single electron and $2I_{\mathrm{Q}}$ is the photoelectron current generated by two Ge photodiodes.

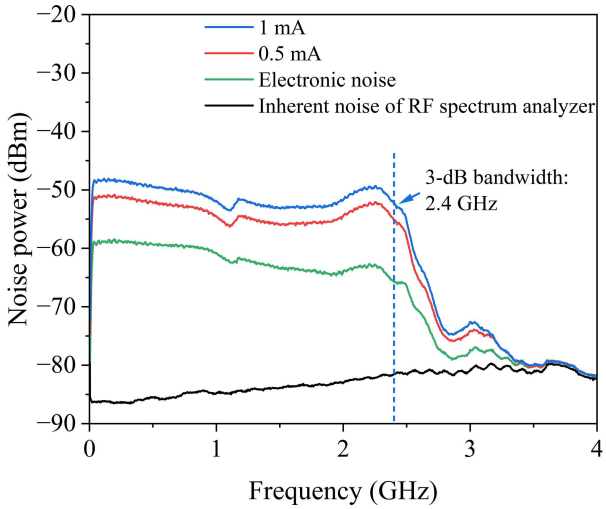

Figure 5 (Color online) Noise power spectra of the integrated BHD. The resolution bandwidth is $R_{\mathrm{BW}} = 2$ MHz.

The equivalent transimpedance at 0.1 GHz was computed as follows:

$$R_{\mathrm{F}} = \sqrt{u_{\mathrm{M}}^2 - u_{\mathrm{E}}^2}/i_{\mathrm{Q}} = u_{\mathrm{Q}}/i_{\mathrm{Q}} = 2.28 \times 10^4\,\Omega, \tag{3}$$

where u_{Q} is the noise density of shot noise.

The QCNR at 0.1 GHz was then determined as follows:

$$\mathrm{QCNR} = 10 \cdot \log_{10}\left(u_{\mathrm{Q}}^2/u_{\mathrm{E}}^2\right) = 9.51\,\mathrm{dB}. \tag{4}$$

From (2)–(4), it was concluded that the electronic noise was equivalent to the shot noise generated by a photoelectron current of $I_{\mathrm{E}} \approx 0.1$ mA. The noise equivalent power at 0.1 GHz was calculated as

$$\mathrm{NEP} = i_{\mathrm{E}}/R(\lambda) = \sqrt{2q \cdot (2I_{\mathrm{E}})}/R(\lambda) = 8.85\ \ \mathrm{pW}/\sqrt{\mathrm{Hz}}, \tag{5}$$

where i_{E} is the current noise density of the equivalent photoelectron current I_{E} at 0.1 GHz, and $R(\lambda)$ is the responsivity of the Ge photodiode (0.9 A/W) at 1550 nm.

A BHD with a high CMRR is crucial to minimize the classical intensity noise of the laser [63]. SiPh-chip-based BHDs usually use Mach Zehnder interferometer structures or p-i-n phase modulators to balance the two output ports of a 50/50 MMI coupler [64]. The additional balance structures require extra balance control, which complicates the BHD structure and QRNG. In our design, an optimized symmetrical 1 × 2 MMI structure is employed to achieve high balance degree. The balance of the two output beams of the 1 × 2 MMI structure is less sensitive to the structure size and beam wavelength than that of the 2 × 2 MMI structure. Furthermore, the 1 × 2 MMI is smaller and introduces lower loss than the 2 × 2 MMI. If a fabrication error alters the size of the 1 × 2 MMI or the laser wavelength changes, the balance will be less affected.

For CMRR measurements, we directed the laser beam emitted by the DFB laser chip into an amplitude modulator and then injected the modulated beam into the integrated homodyne detector. When the photoelectron current was 0.5 mA, the CMRR exceeded 35 dB at 500 MHz (Figure 6(a)) and 25 dB at 2 GHz (Figure 6(b)).

4 Generation and analysis of quantum random numbers

To generate quantum random numbers, a trusted-device-dependent security framework that takes into account both the classical and quantum side information is employed. The minimum entropy is given by [51, 58]

$$H_{\min} \geqslant -\min_{\delta>0} \log_2 \left[\frac{(n+\delta)(1+n+\delta)}{\delta} \cdot B\right], \tag{6}$$

where δ is a parameter that is employed to improve the bound. Its value can be determined as

$$\frac{(n+\delta)(1+n+\delta)}{\delta} = \Gamma(n) = \left(\sqrt{n} + \sqrt{n+1}\right)^2, \tag{7}$$

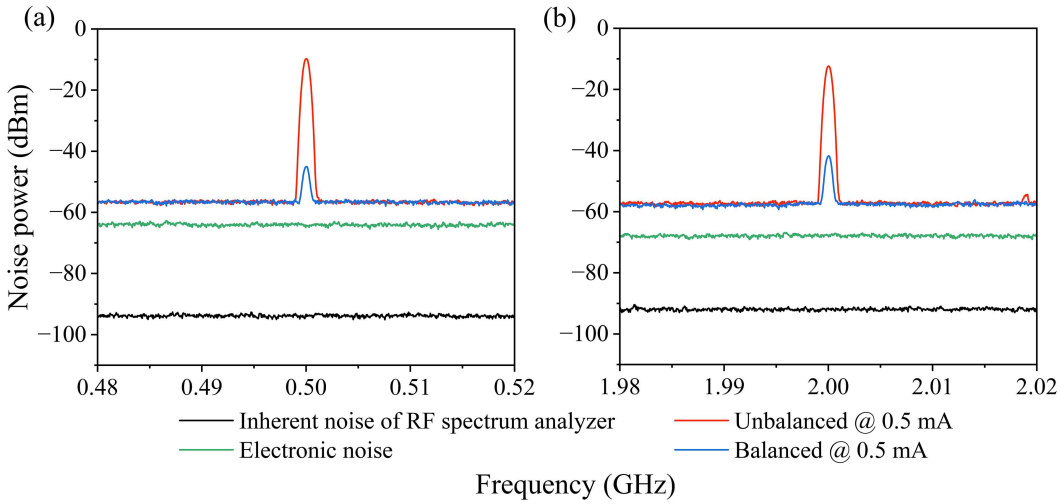

Figure 6 (Color online) CMRR of the BHD measured at (a) 500 MHz and (b) 2 GHz.

where n is the mean photon number of the thermal state used to characterize the vacuum state measurement by BHD with excess noise [51]. B is defined as

$$\begin{aligned} B &= \max\left\{\operatorname{erf}\left(\frac{\Delta x}{2u}\right), \frac{1}{2}\operatorname{erfc}\left(\frac{R}{u}\right)\right\}, \\ u &= g\sqrt{\frac{4n(n+1+\delta)+2\delta}{n}}. \end{aligned} \tag{8}$$

The term $\Delta x = R/2^N$, which can be determined by the range R and resolution N of the ADC, is the bin size of the ADC. The parameter g is the gain of the BHD when the shot noise is normalized to 1. The optimal values of R and B can be determined by

$$\operatorname{erf}\left(\frac{\Delta x}{2u}\right) = \frac{1}{2}\operatorname{erfc}\left(\frac{R}{u}\right). \tag{9}$$

Due to the finite bandwidth of the detector, the measurement process cannot be considered as an IID stationary Gaussian process. To extend the framework to non-IID measurement, the conditional variances $\sigma^2_{\mathrm{M,c}}, \sigma^2_{\mathrm{Q,c}}$, and $\sigma^2_{\mathrm{E,c}}$ for the homodyne measurement M, quantum signal Q, and excess noise E should be calculated based on the power spectral density, which can be obtained using the fast Fourier transform (FFT) [65]. The relationship of the variance σ^2_{M}, which is calculated directly using data samples, and the conditional variance $\sigma^2_{\mathrm{M,c}}$ is

$$\sigma^2_{\mathrm{M}} = \sigma^2_{\mathrm{M,c}} + \varsigma, \tag{10}$$

where ς is a factor that contains all the fluctuation of past measurement. The gain g of BHD and the mean photon number n of the thermal state are determined by

$$\begin{aligned} g^2 &= \sigma^2_{\mathrm{Q,c}}, \\ 2g^2 n &= \sigma^2_{\mathrm{M}} - \sigma^2_{\mathrm{Q,c}}. \end{aligned} \tag{11}$$

To characterize the side-information leakage due to the imperfect ADC, the differential nonlinearity (DNL) $D_{\max}$, which represents the maximum deviation from the ideal bin size Δx, should be characterized [66, 67]. Then, the minimum entropy can be calculated as

$$H_{\min} \geqslant -\log_2\left[\Gamma(n)\cdot\operatorname{erf}\left(\frac{\Delta x + \Delta x\cdot D_{\max}}{2u}\right)\right]. \tag{12}$$

In our experiment, data were acquired using an oscilloscope with a sampling rate of 6.25 GSample/s and a 12-bit resolution ADC. An equalizer was designed to minimize correlations of adjacent samples and increase the data acquisition rate [68]. Various parameters and the minimum entropy before and after equalization were determined, as listed in Tables 3 and 4.

Table 3 Minimum entropy and related parameters before equalization.

n	g (V)	δ	R (V)	u (V)	ς (V^2)	Δx (V)	$H_{\min}$ (bit)
0.4891	0.0202	0.8500	0.1321	0.0549	3.5361×10^{-4}	3.2251×10^{-5}	9.4140
σ^2_{M} (V^2)	$\sigma^2_{\mathrm{M,c}}$ (V^2)	$\sigma^2_{\mathrm{Q,c}}$ (V^2)	$\sigma^2_{\mathrm{E,c}}$ (V^2)	K_{M}	S_{M}	K_{E}	S_{E}
8.0583×10^{-4}	4.5220×10^{-4}	4.0736×10^{-4}	4.4853×10^{-5}	2.9929	−0.0161	2.9931	−0.0039

Table 4 Minimum entropy and related parameters after equalization.

n	g (V)	δ	R (V)	u (V)	ς (V^2)	Δx (V)	$H_{\min}$ (bit)
0.5479	0.0196	0.9200	0.1324	0.0550	3.6184×10^{-4}	3.2324×10^{-5}	9.3184
σ^2_{M} (V^2)	$\sigma^2_{\mathrm{M,c}}$ (V^2)	$\sigma^2_{\mathrm{Q,c}}$ (V^2)	$\sigma^2_{\mathrm{E,c}}$ (V^2)	K_{M}	S_{M}	K_{E}	S_{E}
8.0583×10^{-4}	4.4399×10^{-4}	3.8450×10^{-4}	5.9488×10^{-5}	2.9836	−0.0074	2.9778	0.0093

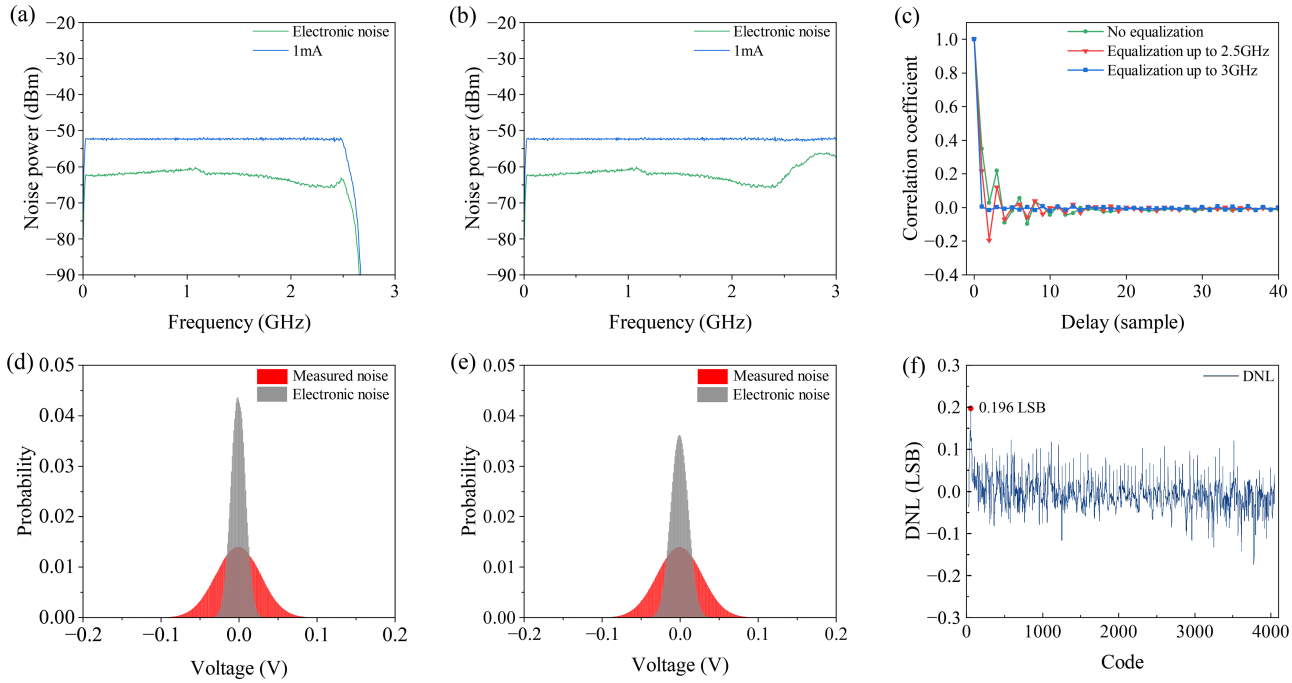

Figure 7 (Color online) Equalization, correlation, and probability distribution of data, and measurement results of DNL. Noise power spectra when the frequency was equalized (a) up to 2.5 GHz and (b) up to 3 GHz. (c) Effect of the equalizer on the correlation coefficients of the raw data. Histograms of measured and electronic noises before (d) and after (e) equalization. (f) Measurement results of DNL.

In the equalization process, we tune the gain factor of the equalizer to make sure that the energy of signals does not increase. It means that the variance σ^2_{M} of the measured noise signal does not change after adding the equalization filter. In this case, the value of the minimum entropy and related parameters changed slightly. The skewness S_{M} and S_{E} of the measured noise data and electronic noise data were nearly zero, and kurtosis K_{M} and K_{E} were nearly 3, confirming that the raw data closely followed a Gaussian distribution before and after the equalization.

Figures 7(a) and (b) show the power spectrum when the frequency was equalized up to 2.5 and 3 GHz, respectively. After equalization, flat white noises were obtained. Figure 7(c) shows the effect of equalization on the correlations between adjacent samples. In the absence of equalization, the adjacent samples were obviously correlated. The correlation coefficients, which were calculated from 1.25×10^8 samples, decreased when the frequency was equalized up to 2.5 GHz and nearly became zero when the frequency was equalized up to 3 GHz. The weak correlations indicated that the raw samples were close to IID. Panels (d) and (e) in Figure 7 display histograms of the acquired data before and after equalization, respectively. The data closely followed a perfect Gaussian distribution. Figure 7(f) shows the measurement result of DNL and a maximum deviation $D_{\max}=0.196$ LSB was measured.

For the equalization up to 3 GHz, our QRNG promises a generation rate of 58.24 Gbps (6.25 GSample/s $\times$ 9.3184 bits/sample). Using the raw sample and a Toeplitz matrix, the random numbers were extracted according to the estimated minimum entropy. The randomness of the extracted random numbers was evaluated using the NIST SP 800-22 suite [69, 70]. The randomness test results shown in Table 5 indicate good statistical characteristics of

Table 5 NIST SP 800-22 randomness test results.

Statistical test	P-value	Result	Statistical test	P-value	Result
Frequency	0.8036	Success	Overlapping template	0.0432	Success
Block frequency	0.8021	Success	Universal	0.6861	Success
Cumulative sums	0.9162	Success	Approximate entropy	0.4180	Success
Runs	0.1047	Success	Random excursions	0.9755	Success
Longest run	0.8857	Success	Random excursions variant	0.9643	Success
Rank	0.5219	Success	Serial	0.8707	Success
FFT	0.1892	Success	Linear complexity	0.3879	Success
Non-overlapping template	0.9460	Success			

the generated random number sequence containing one gigabit of random numbers.

5 Conclusion

We have designed and investigated a highly integrated broadband entropy source for QRNGs based on vacuum fluctuations. The entropy source comprises a hybrid chip and three cascaded RFAs. The hybrid chip, comprising an InP DFB laser chip (1550 nm) and a SiPh chip, is only 6.3 mm × 2.6 mm × 1.5 mm in size. The QCNR reaches 9.51 dB at a photoelectron current of 1 mA and no temperature controller is needed. The noise equivalent power and equivalent transimpedance are 8.85 $\mathrm{pW}/\sqrt{\mathrm{Hz}}$ and 22.8 kΩ, respectively. Although no balancing structure is utilized, the CMRR of the BHD exceeds 25 dB. By optimizing the analog circuits, the 3-dB bandwidth of the BHD reaches 2.4 GHz. The equalization technique is employed to increase the data acquisition rate and minimize correlations between adjacent samples. The DNL of the ADC is measured to achieve a tighter minimum entropy. At last, a quantum random number generation rate of 58.24 Gbps is achieved in a trusted-device-dependent and non-IID security framework, which takes into account both classical and quantum side information. The randomness test results confirm the good statistical characteristics of the generated random sequence.

In future work, we will develop a hybrid chip with stage 3 integration. Through monolithic electronic-photonic integration and the hybrid integration of a laser chip, the size of the whole entropy source will be reduced to 5 mm × 2 mm × 1.5 mm. By improving the bandwidth of the BHD, an ultrafast, compact, cost-effective, and lower-power-consumption QRNG can be realized. We envisage that such devices will play an important role in the quantum information field.

Acknowledgements This work was supported in part by National Natural Science Foundation of China (Grant Nos. 11504219, 62175138, 62205188, 11904219), Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0300703), and Shanxi Provincial Foundation for Returned Scholars, China (Grant No. 2022-016).

References

1 Herrero-Collantes M, Garcia-Escartin J C. Quantum random number generators. Rev Mod Phys, 2017, 89: 015004
2 Ma X, Yuan X, Cao Z, et al. Quantum random number generation. npj Quantum Inf, 2016, 2: 1–9
3 Bauke H, Mertens S. Random numbers for large-scale distributed monte carlo simulations. Phys Rev E, 2007, 75: 066701
4 Martin A, Sanguinetti B, Lim C C W, et al. Quantum random number generation for 1.25-GHz quantum key distribution systems. J Lightwave Technol, 2015, 33: 2855–2859
5 Liu S, Lu Z, Wang P, et al. Experimental demonstration of multiparty quantum secret sharing and conference key agreement. npj Quantum Inf, 2023, 9: 92
6 Tian Y, Zhang Y, Liu S, et al. High-performance long-distance discrete-modulation continuous-variable quantum key distribution. Opt Lett, 2023, 48: 2953–2956
7 Liu S, Tian Y, Zhang Y, et al. Integrated quantum communication network and vibration sensing in optical fibers. Optica, 2024, 11: 1762–1772
8 Tian Y, Wang P, Liu J, et al. Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over optical fiber. Optica, 2022, 9: 492–500
9 Ren M Z, Zhou L, Yuan Z L. Low-loss, dual-polarization asymmetric Mach-Zehnder interferometer chips for quantum key distribution. Sci China Inf Sci, 2023, 66: 180503
10 Ma L, Yang J, Zhang T, et al. Practical continuous-variable quantum key distribution with feasible optimization parameters. Sci China Inf Sci, 2023, 66: 180507
11 Feng Y, Qiu R H, Zhang K, et al. Secret key rate of continuous-variable quantum key distribution with finite codeword length. Sci China Inf Sci, 2023, 66: 180511
12 Lu Q H, Wang F X, Chen W, et al. Quantum key distribution over a mimicked dynamic-scattering channel. Sci China Inf Sci, 2024, 67: 142503
13 Li C, Ren S Y, Yan Y R, et al. Distribution of polarization squeezed light through a 20 km fiber channel. Sci China Inf Sci, 2024, 67: 159501

14 Zhang K, Hou J, Jiang X-Q, et al. Effective rate-adaptive reconciliation for CV-QKD using QC-MET-LDPC codes. Sci China Inf Sci, 2025, 68: 082002
15 Guo M X, Huang P, Wang T, et al. Reverse-encoded quantum key distribution with Gaussian-modulated coherent states. Sci China Inf Sci, 2025, 68: 082003
16 Ren S Y, Han D M, Wang M H, et al. Continuous variable quantum teleportation and remote state preparation between two space-separated local networks. Sci China Inf Sci, 2024, 67: 042002
17 Wang P, Tian Y, Li Y M. Advances in continuous variable measurement-device-independent quantum key distribution. Sci China Inf Sci, 2025, 68: 082004
18 Azuma K, Economou S E, Elkouss D, et al. Quantum repeaters: from quantum networks to the quantum internet. Rev Mod Phys, 2023, 95: 045006
19 Li C L, Yin H L, Chen Z B. Asynchronous quantum repeater using multiple quantum memory. Rep Prog Phys, 2024, 87: 127901
20 Lu Y S, Yin H L, Xie Y M, et al. Repeater-like asynchronous measurement-device-independent quantum conference key agreement. Rep Prog Phys, 2025, 88: 067901
21 Dolphin J A, Taofiq K, Han D, et al. A hybrid integrated quantum key distribution transceiver chip. npj Quantum Inf, 2023, 9: 1–8
22 Siew S Y, Li B, Gao F, et al. Review of silicon photonics technology and platform development. J Lightwave Technol, 2021, 39: 4374–4389
23 Marinins A, Hänsch S, Sar H, et al. Wafer-scale hybrid integration of InP DFB lasers on Si photonics by flip-chip bonding with sub-300 nm alignment precision. IEEE J Sel Top Quantum Electron, 2022, 29: 1–11
24 Li N, Chen G, Ng D K T, et al. Integrated lasers on silicon at communication wavelength: a progress review. Adv Opt Mater, 2022, 10: 2201008
25 Zhang X, Zhang Y, Li Z, et al. 1.2-GHz balanced homodyne detector for continuous-variable quantum information technology. IEEE Photonics J, 2018, 10: 1–10
26 Liu Y, Zhao Q, Li M H, et al. Device-independent quantum random-number generation. Nature, 2018, 562: 548–551
27 Liu W Z, Li M H, Ragy S, et al. Device-independent randomness expansion against quantum side information. Nat Phys, 2021, 17: 448–451
28 Shalm L K, Zhang Y, Bienfang J C, et al. Device-independent randomness expansion with entangled photons. Nat Phys, 2021, 17: 452–456
29 Marangon D G, Vallone G, Villoresi P. Source-device-independent ultrafast quantum random number generation. Phys Rev Lett, 2017, 118: 060503
30 Cao Z, Zhou H, Ma X. Loss-tolerant measurement-device-independent quantum random number generation. New J Phys, 2015, 17: 125011
31 Wang C, Primaatmaja I W, Ng H J, et al. Provably-secure quantum randomness expansion with uncharacterised homodyne detection. Nat Commun, 2023, 14: 316
32 Haw J Y, Assad S M, Lance A M, et al. Maximization of extractable randomness in a quantum random-number generator. Phys Rev Appl, 2015, 3: 054004
33 Jennewein T, Achleitner U, Weihs G, et al. A fast and compact quantum random number generator. Rev Sci Instruments, 2000, 71: 1675–1680
34 Stipčević M, Rogina B M. Quantum random number generator based on photonic emission in semiconductors. Rev Sci Instruments, 2007, 78: 045104
35 Wayne M A, Jeffrey E R, Akselrod G M, et al. Photon arrival time quantum random number generation. J Modern Opt, 2009, 56: 516–522
36 Wahl M, Leifgen M, Berlin M, et al. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements. Appl Phys Lett, 2011, 98: 171105–171105
37 Fürst H, Weier H, Nauerth S, et al. High speed optical quantum random number generation. Opt Express, 2010, 18: 13029–13037
38 Ren M, Wu E, Liang Y, et al. Quantum random-number generator based on a photon-number-resolving detector. Phys Rev A, 2011, 83: 023820
39 Wei W, Guo H. Bias-free true random-number generator. Opt Lett, 2009, 34: 1876–1878
40 Gabriel C, Wittmann C, Sych D, et al. A generator for unique quantum random numbers based on vacuum states. Nat Photon, 2010, 4: 711–715
41 Shen Y, Tian L, Zou H. Practical quantum random number generator based on measuring the shot noise of vacuum states. Phys Rev A, 2010, 81: 063814
42 Symul T, Assad S M, Lam P K. Real time demonstration of high bitrate quantum random number generation with coherent laser light. Appl Phys Lett, 2011, 98: 231103–231103
43 Guo H, Tang W, Liu Y, et al. Truly random number generation based on measurement of phase noise of a laser. Phys Rev E, 2010, 81: 051137
44 Qi B, Chi Y M, Lo H K, et al. High-speed quantum random number generation by measuring phase noise of a single-mode laser. Opt Lett, 2010, 35: 312–314
45 Jofre M, Curty M, Steinlechner F, et al. True random numbers from amplified quantum vacuum. Opt Express, 2011, 19: 20665–20672
46 Williams C R S, Salevan J C, Li X, et al. Fast physical random number generator using amplified spontaneous emission. Opt Express, 2010, 18: 23584–23597
47 Bustard P J, Moffatt D, Lausten R, et al. Quantum random bit generation using stimulated Raman scattering. Opt Express, 2011, 19: 25173–25180
48 Marandi A, Leindecker N C, Vodopyanov K L, et al. Twin degenerate OPO for quantum random bit generation. In: Proceedings of Nonlinear Optics: Materials, Fundamentals and Applications, 2011

49 Abellan C, Amaya W, Domenech D, et al. Quantum entropy source on an InP photonic integrated circuit for random number generation. Optica, 2016, 3: 989–994

50 Zheng Z, Zhang Y C, Huang W, et al. 6 Gbps real-time optical quantum random number generator based on vacuum fluctuation. Rev Sci Instruments, 2019, 90: 043105

51 Gehring T, Lupo C, Kordts A, et al. Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information. Nat Commun, 2021, 12: 605

52 Avesani M, Marangon D G, Vallone G, et al. Source-device-independent heterodyne-based quantum random number generator at 17 Gbps. Nat Commun, 2018, 9: 5365

53 Xu B, Chen Z, Li Z, et al. High speed continuous variable source-independent quantum random number generation. Quantum Sci Technol, 2019, 4: 025013

54 Li L, Cai M, Wang T, et al. On-chip source-device-independent quantum random number generator. Photon Res, 2024, 12: 1379–1394

55 Raffaelli F, Ferranti G, Mahler D H, et al. A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers. Quantum Sci Technol, 2018, 3: 025003

56 Bai B, Huang J Y, Qiao G R, et al. 18.8 Gbps real-time quantum random number generator with a photonic integrated chip. Appl Phys Lett, 2021, 118: 264001

57 Bruynsteen C, Vanhoecke M, Bauwelinck J, et al. Integrated balanced homodyne photonic-electronic detector for beyond 20 GHz shot-noise-limited measurements. Optica, 2021, 8: 1146–1152

58 Bruynsteen C, Gehring T, Lupo C, et al. 100-Gbit/s integrated quantum random number generator based on vacuum fluctuations. PRX Quantum, 2023, 4: 010330

59 Ng S Q, Zhang G, Lim C, et al. A chip-integrated homodyne detection system with enhanced bandwidth performance for quantum applications. Quantum Sci Technol, 2024, 9: 045010

60 Bian Y M, Pan Y, Xu X S, et al. Continuous-variable quantum key distribution over 28.6 km fiber with an integrated silicon photonic receiver chip. Appl Phys Lett, 2024, 124: 174001

61 Tasker J F, Frazer J, Ferranti G, et al. Silicon photonics interfaced with integrated electronics for 9 GHz measurement of squeezed light. Nat Photonics, 2021, 15: 11–15

62 Tasker J F, Frazer J, Ferranti G, et al. A Bi-CMOS electronic photonic integrated circuit quantum light detector. Sci Adv, 2024, 10: eadk6890

63 Wang X Y, Guo X B, Jia Y X, et al. Accurate shot-noise-limited calibration of a time-domain balanced homodyne detector for continuous-variable quantum key distribution. J Lightwave Technol, 2023, 41: 5518–5528

64 Jia Y, Wang X, Hu X, et al. Silicon photonics-integrated time-domain balanced homodyne detector for quantum tomography and quantum key distribution. New J Phys, 2023, 25: 103030

65 Cover T M, Thomas J A. Elements of Information Theory. Hoboken: Wiley-Interscience, 2006

66 Plassche R. CMOS Integrated Analog-To-Digital and Digital-To-Analog Converters. New York: Springer U.S., 2003

67 Zhu Z M, Song J J, Liang Y H. A 10-kHz 12-16-bit reconfigurable zoom ADC with pole optimization technique and floating current-starved amplifier. Sci China Inf Sci, 2024, 67: 229403

68 Kordts A, Lupo C, Nikolic D S, et al. Security verification for vacuum fluctuation based quantum random number generator. In: Proceedings of 2018 Conference on Lasers and Electro-Optics (CLEO), San Jose, 2018. 1–2

69 Lu Z, Liu J, Wang X, et al. Quantum random number generator with discarding-boundary-bin measurement and multi-interval sampling. Opt Express, 2021, 29: 12440–12453

70 Wang J J, Cai Q, Zhang J G, et al. Photonic reservoir computing based min-entropy evaluation for random number generators. Sci China Inf Sci, 2025, 68: 082001