https://doi.org/10.1140/epjqt/s40507-023-00206-w

EPJ.org

EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

Effect of external magnetic fields on practical quantum random number generator

Yuan-Hao Li[1], Yang-Yang Fei[1*], Wei-Long Wang[1*], Xiang-Dong Meng[1], Hong Wang[1], Qian-Heng Duan[1], Yu Han[1] and Zhi Ma[1]

*Correspondence:
fei_yy@foxmail.com;
wangwl19888@163.com
[1] Henan Key Laboratory of Network Cryptography Technology, Zhengzhou, Henan, 450001, China

Abstract

Quantum random number generator (QRNG) based on the inherent randomness of fundamental quantum processes can provide provable true random numbers which play an important role in many fields. However, the security of practical QRNGs is linked to the performance of realistic devices. In particular, devices based on the Faraday effect in a QRNG system may be affected by external magnetic fields, which will inevitably open a loophole that an eavesdropper can exploit to steal the information of generated random numbers. In this work, the effects of external magnetic fields on the security of practical QRNGs are analyzed. Taking the quantum phase fluctuation based QRNG with unbalanced Michelson interferometer as an example, we experimentally demonstrate the rotation angle of the Faraday rotation mirror (FRM) is influenced by external magnetic fields. Then, we develop a theoretical model between the rotation angle deviation of FRM and conditional min-entropy. Simulation results show that the imperfect FRM leads to a reduction in the variance of measured signal and extractable randomness. Furthermore, the impacts of practical sampling device on the extractable randomness are analyzed in the presence of imperfect FRM, which indicates suitable parameters of the sampling device can improve the security of practical QRNGs. Potential countermeasures are also proposed. Our work reveals that external magnetic fields should be carefully considered in the application of practical QRNGs.

Keywords: Quantum random number generator; Faraday rotator; External magnetic field

1 Introduction

Random numbers play an important role and have vast applications in a variety of tasks, such as cryptography [1], numerical simulation [2] and lottery [3]. The randomness of random numbers has a direct impact on the performance of the application. Quantum random number generators (QRNGs) based on the intrinsic uncertainty principle of quantum mechanics can produce true random numbers [4, 5], which has attracted a lot of attention. Over the past two decades, varieties of practical QRNG schemes have been proposed and implemented. According to different quantum random sources, QRNGs can be divided into discrete variable QRNGs and continuous variable QRNGs. Discrete variable QRNGs

Springer

mainly utilize photon path [6], photon arrival time [7–9] and photon number distribution [10, 11] to generate random numbers. However, similar to the discrete variable quantum key distribution (QKD), which is limited by some drawbacks with regards to single photon detectors, such as dark count rates, low quantum efficiencies, after-pulse effects and dead times, the generation rates of discrete variable QRNGs are so slow that the random numbers cannot be used to satisfy most practical applications [12–16]. In contrast to discrete variable QRNGs, continuous variable QRNGs use a traditional high-bandwidth photodetector (PD) with higher speed and lower cost, which exploits vacuum fluctuation [17–20], quantum phase fluctuation [21–32] and amplified spontaneous emission noise [33–38], to generate random numbers, and the random number generation rates of continuous variable QRNGs are significantly increased. Moreover, continuous variable QRNG can be well compatible with classical optical communication systems.

Among the continuous variable QRNGs, the one based on quantum phase fluctuation is a more promising and valuable scheme due to its high generation rate and simple structure. For example, the related generation rate has reached tens of Gbps [27, 29] and on-chip integration has been realized [30]. Since it is difficult to directly measure the phase fluctuations, an interferometer is commonly used to convert phase fluctuations into intensity fluctuations. Nevertheless, the performance of the interference is sensitive to the polarization and phase drift in optical fibers. To reduce the impact of polarization and phase drift, the unbalanced Michelson interferometer with two Faraday rotation mirrors (FRMs) is proposed and widely used in the continuous mode [24–27] or gain-switched mode [31, 32]of semiconductor lasers.

In general, practical QRNGs can produce secure true random numbers only if the physical devices are trusted and fulfill with the model assumptions, which usually fails in the presence of an eavesdropper or the imperfections of physical devices. This leads to information leakage of the generated random numbers of practical QRNGs. To solve this problem, device-independent QRNG (DI-QRNG) protocols without assumptions on the physical devices are proposed [39–41], but the realistic implementations are difficult and the generation rate is relatively slow. To trade off between generation rate and practical security, the semi-device-independent QRNG (SDI-QRNG) protocols are proposed, which mainly include source-device-independent [42–44], measurement-device-independent [45, 46] and dimension witness violation based QRNG protocols [15, 47–49]. Though the generation rate of SDI-QRNG has been improved, its security is still dependent on partially imperfect devices. Compared to the DI-QRNG and SDI-QRNG schemes, practical QRNGs are still more popular due to their relatively low cost, ease of implementation and high generation rates. Therefore, the security of practical QRNGs is a major and essential issue that must be considered.

There are already some excellent researches on the security of practical QRNGs, such as the influence of postprocessing method [50], local oscillator fluctuation [51], phase randomness in laser source [52], sampling settings [18, 53] and variations in laser source temperature [36, 54]. In previous works, it is generally assumed that the operating environment is stable. Unfortunately, practical QRNGs may be subjected to complex electromagnetic environments [16, 55–57] or electromagnetic disturbance from an eavesdropper [58]. Ref. [59] analyze the variations on the performance of optical isolator and optical circulator caused by external magnetic fields. Ref. [58] presents an attacker who actively exploits an electromagnetic side channel to control the output of a kind of homodyne-based

QRNGs. At present, the Faraday effect based optical devices, such as the FRM, are widely used in the QRNG systems. The performance of FRM is sensitive to the variations in surrounding magnetic field strength which may result in overestimating the min-entropy. Nevertheless, there is still a lack of study on the effect of external magnetic fields on the security of practical QRNG.

In this paper, taking the quantum phase fluctuation based QRNG with unbalanced Michelson interferometer as an example, the effect of external magnetic fields on the security of practical QRNG is studied. We experimentally demonstrate the rotation angle of the FRM significantly deviates from the ideal value under the influence of external magnetic fields, which directly affects the performance of unbalanced Michelson interferometer. Then we analyze the impacts of imperfect FRM on the security of practical quantum phase fluctuation based QRNG. Simulation results show that the imperfect FRM leads to a reduction in extractable randomness. Furthermore, the influences of practical sampling devices are also quantitatively studied. Finally, we propose some countermeasures to defend against variation in the magnetic field strength.

The rest of this paper is organized as follows. In Sect. 2.1, we briefly review the protocol of quantum phase fluctuation based QRNG with unbalanced Michelson interferometer. In Sect. 2.2, the influence of external magnetic fields on FRM is briefly introduced and experimentally demonstrated. In Sect. 3.1, the security of practical QRNG based on quantum fluctuation is analyzed under the external magnetic fields, including the impacts on the variance of measured signal and the extractable randomness. Moreover, the impacts of sampling devices on the extractable randomness are investigated with imperfect FRM. Corresponding countermeasures are proposed in Sect. 3.2. Finally, we conclude this paper in Sect. 4.

2 Methods

2.1 Quantum phase fluctuation based QRNG with unbalanced Michelson interferometer

In this section, we review a typical quantum phase fluctuation based QRNG with unbalanced Michelson interferometer. Phase fluctuations of photons emitted from a laser originate from spontaneous emissions, which can be used as a quantum entropy source to generate random numbers [60, 61]. When the laser current is operated around its threshold value, spontaneous emissions will dominate. Because the phase fluctuation is difficult to measure directly, the phase fluctuation can be converted into a measurable intensity via an interferometer. The structure of the QRNG scheme is shown in Fig. 1.

As shown in Fig. 1, a semiconductor laser is operated slightly above its threshold and emits a continuous beam. Then the continuous beam passes through Port 1 of a circulator into the Michelson interferometer, which is mainly composed of a 50/50 beam splitter (BS), a phase shifter (PS), two FRMs and a delay line. The circulator is a three-port device that redirects incoming optical signals to special output ports [13, 14, 62]. Port 1 is coupled to the input of semiconductor laser with Port 2 connected to the BS. After entering the BS from Port 2, the continuous beam is divided into a signal beam and a reference beam. Two FRMs reflect the signal beam and reference beam, which then pass through the BS again and interfere. In the Michelson interferometer, two ideal FRMs make the interferometer polarization-insensitive. One output port of the interferometer is monitored by a power meter (PM). By analyzing the measured results of the PM, a proportional-integral-derivative (PID) program sends feedback signals to an open-loop piezo controller (PC) to

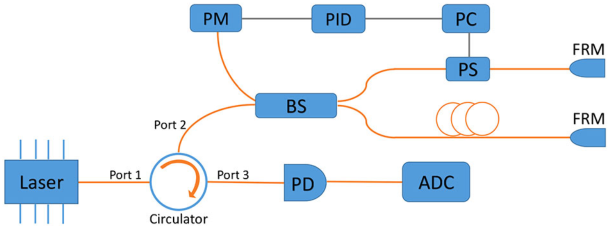

Figure 1 The architecture of the QRNG is based on quantum phase fluctuation. A laser emits a continuous beam that enters the Michelson interferometer through the circulator. One output port of the interferometer is monitored by a PM. A PID program analyzes the measured results of the PM and sends a signal to the PC. The PC could adjust the PS in real-time. The other output port of the interferometer is measured by a PD. And the measured voltage signal of the PD is digitized by an ADC. BS: beam splitter, PS: phase shifter, PM: power meter, PC: piezo controller, FRM: Faraday rotator mirror, PID: proportional-integral-derivative control, PD: photodetector, ADC: analog-to-digital converter

precisely adjust the PS in real time. In this way, the phase difference between two arms of the interferometer could be maintained. The other output port of the interferometer re-enters the circulator in Port 2 and finally reaches Port 3. The interference beam output from Port 3 is converted to electrical signal by a PD. Subsequently, an n-bit analog-to-digital converter (ADC) samples the voltage output of the PD to obtain the raw bits. Due to the presence of classical noise, the raw bits should be post-processed to extract secure random bits. In practical QRNG systems, the min-entropy is commonly used to quantify the random bits that can be extracted [18, 27–29, 63–66].

2.2 Influence of external magnetic fields on FRM

In practical QRNG schemes, many core optical devices are based on the magneto-optical effect, which are sensitive to external magnetic fields. For example, the FRM is an important optical device in the quantum phase fluctuation based QRNG with unbalanced Michelson interferometer, whose performance can also be affected by external magnetic field. In this work, we focus on the analysis and discussion of the influence of external magnetic fields on FRMs.

The FRM is a combination of a Faraday rotator and an ordinary mirror. The Faraday rotator is based on Faraday effect, which is also a kind of magneto-optical effect, i.e., an interaction between the light field and magnetic field in a medium. When a static magnetic field is applied to the medium in a direction parallel to the propagation direction of light field, the polarization plane of the light field will rotate and is only related to the direction of the magnetic field. The Faraday rotator is a non-reciprocal optical device composed of a magneto-optical crystal and a permanent magnet. Under the magnetic field, the rotation angle of the polarization plane of light field is proportional to the path length L of light through the material and the component of magnetic field strength B around the magneto-optical crystal in the direction of light propagation, which can be expressed as

$$\theta = VBL, \tag{1}$$

where V denotes the Verdet constant of the material, i.e., characterizes the magneto-optical properties of the material.

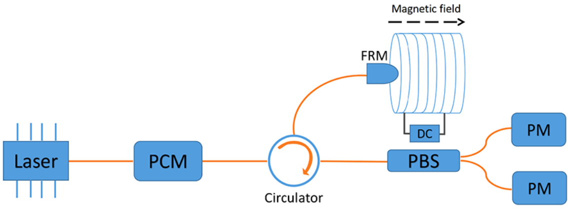

Figure 2 Simplified diagram of the experimental setup to study the effect of an external magnetic field on FRM. PCM: polarization control module, PBS: polarization beam splitter, DC: DC power supply

In the ideal case, the rotation angle of Faraday rotator is 45° and its Jones matrix can be written as

$$\mathrm{FM}(45^\circ) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} = -\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{2}$$

Therefore, a perfect FRM can rotate the original polarization state of a photon to its orthogonal state. However, the rotation angle of the Faraday rotator may not be exactly 45° under an external magnetic field disturbance. To further investigate the influence of external magnetic fields on FRM, we perform a relevant experiment.

Figure 2 shows the simplified diagram of the experimental setup to study the effect of external magnetic fields on FRM. A 1550 nm laser diode is operated at continuous wave mode and its output light is transmitted to the polarization control module (PCM). PCM is used to control the polarization state of the input light. Then the light passes through a circulator to an FRM which is placed in the middle of the solenoid. The magnetic field in the middle of the solenoid is uniformly distributed, and the strength of the magnetic field can be adjusted by changing the current loaded onto the solenoid. The magnetic field strength is measured by a Gauss meter and the current is provided by a DC power supply. After passing through FRM, the polarization state of the light can be changed. Then, the light signal reflected by the FRM is transmitted through the circulator to a polarization BS (PBS), which divides light into two paths whose polarization states are orthogonal to each other. Finally, the light intensities of the two paths are individually measured with two PMs. Based on the measured values, the rotation angle deviation of FRM caused by external magnetic fields can be calculated.

The experimental results of the rotation angle deviation of the FRM in the presence of an external magnetic field are shown in Fig. 3. Specifically, by changing the direction of the FRM in the solenoid, we can investigate the effect of external magnetic fields on the deviation of the rotation angle of the Faraday rotator under different magnetic field directions. Figure 3(a) shows the experimental results under the condition that the external and internal magnetic fields are in the same direction. It is shown that external magnetic fields can hardly change the deviation of rotation angle, even though the external magnetic field strength reaches 900 GS. This is due to the magnetic saturation effect of the permanent magnets [67, 68], where an increase in the strength of the magnetic field does not change the rotation angle of FRM. The experimental results under the condition that the external and internal magnetic fields are in the opposite direction are shown in Fig. 3(b). Similarly, because of the magnetic saturation effect, when the external magnetic field strength is less than 350 Gs, the deviation of rotation angle remains almost constant. With continuously

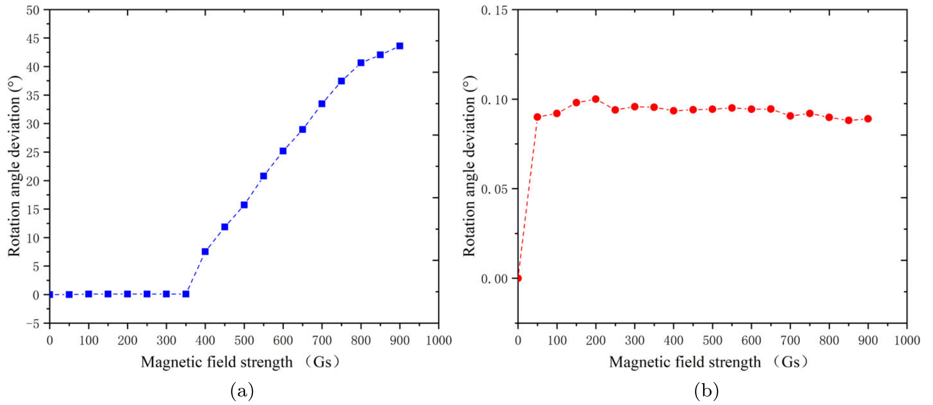

Figure 3 Experimental results on the rotation angle deviation of FRM versus external magnetic field strength. (a) Variation in the rotation angle deviation of FRM when the external and internal magnetic fields are in the same direction. (b)Variation in the rotation angle deviation of FRM when the external and internal magnetic fields are in opposite directions

increasing the strength of reverse external magnetic field, the rotation angle deviation varies significantly and approximately linearly.

Therefore, the rotation angle of the Faraday rotator would be significantly changed when the directions of the external and internal magnetic fields are opposite as well as the strength of external magnetic field exceeds a certain threshold value. In this case, the Jones matrix of practical FRM should be written as

$$\begin{aligned} \mathrm{FM}\left(45^\circ - \theta\right) &= \begin{bmatrix} \cos(45^\circ - \theta) & \sin(45^\circ - \theta) \\ -\sin(45^\circ - \theta) & \cos(45^\circ - \theta) \end{bmatrix} \\ &\quad \times \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \cos(45^\circ - \theta) & -\sin(45^\circ - \theta) \\ \sin(45^\circ - \theta) & \cos(45^\circ - \theta) \end{bmatrix} \\ &= \begin{bmatrix} \sin(2\theta) & -\cos(2\theta) \\ -\cos(2\theta) & -\sin(2\theta) \end{bmatrix}, \end{aligned} \tag{3}$$

where θ represents the rotation angle deviation caused by the external magnetic field and the true rotation angle in every step is $45^\circ - \theta$. Hence, the magnetic field around the FRM directly affects the rotation angle of the light field polarization plane, and thus impacts the performances of the FRM and Michelson interferometer. By remotely controlling the external magnetic field around the FRM, the rotation angle of FRM will be changed, which opens a security loophole for a malicious eavesdropper.

3 Results and discussion

3.1 Security of practical QRNG under external magnetic fields

We have demonstrated that the rotation angle of the FRM can be deviated from ideal value by external magnetic fields, which would lead to the imperfect performance of Michelson interferometer. In this section, we specifically analyze the effect of imperfect FRM under external magnetic fields on the security of practical QRNGs. By numerical simulation, the influences of imperfect FRM on the variance of measured signal and the estimation of the extractable randomness are analyzed. Furthermore, the impacts of sampling device on the security of practical QRNG with imperfect FRM are evaluated.

3.1.1 Influence of imperfect FRM on the extractable randomness

The electric field intensity of the semiconductor laser can be modeled as

$$E(t) = E_0 \exp\bigl[i\omega t + \phi(t)\bigr], \tag{4}$$

where E_0 is the amplitude of electric field, ω is the angular frequency of the electromagnetic field and $\phi(t)$ represents the random phase fluctuations due to the contribution of the spontaneous emission to the emitted light. Without loss of generality, the laser pulses are assumed to be horizontally polarized. That is, the emitted light can be written as $E_{\text{in}} = [E(t), 0]^T$. After passing an ideal BS, the output electric fields become

$$\begin{bmatrix} E_1 \\ E_2 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} E(t) \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} E(t) \\ E(t) \end{bmatrix}, \tag{5}$$

and the polarization of lights is still horizontally polarized, where the electric field intensities of signals in the long arm and the short arm of the Michelson interferometer are E_1 and E_2, respectively.

In the Michelson interferometer, a single mode fiber (SMF), which has a birefringence effect, is used. The Jones matrix of SMF, which can be equivalent to the one of an ellipse delayer, is given by

$$\overrightarrow{R} = \begin{bmatrix} a & -b^* \\ b & a^* \end{bmatrix} = \begin{bmatrix} \cos(\delta/2) + i\cos 2\alpha \sin(\delta/2) & i\sin(2\alpha)\sin(\delta/2) \\ i\sin(2\alpha)\sin(\delta/2) & \cos(\delta/2) - i\cos 2\alpha \sin(\delta/2) \end{bmatrix}, \tag{6}$$

where $\overrightarrow{R}$ means the Jones matrix in the forward direction, α represents the rotation angle between the equivalent fast axis and the x axis of the reference frame, δ is the phase difference between the equivalent fast and slow axes of the SMF. The Jones matrix of the SMF in the inverse direction is given by

$$\overleftarrow{R} = \begin{bmatrix} a & -b \\ b^* & a^* \end{bmatrix}. \tag{7}$$

For simplicity, the short arm coordinate system is selected as the equivalent fast axis and the rotation angle between the short arm and the long arm is the same, i.e., $\alpha = 0$. Then, the input signals of the long arm and short arm pass through the corresponding imperfect FRMs and are reflected to the BS. According to Eq. (1), the rotation angle of FRM is related to the properties of the magneto-optical crystals and the magnetic field strength. Therefore, the rotation angle deviations of the two FRMs may not be the same. Moreover, the rotation angle deviation of the two FRMs are denoted as θ_1 and θ_2, respectively.

Based on the above analysis, the electric fields of the two path signals after the FRM reflection can be obtained. For the long arm, the electric field is

$$E_3 = \overleftarrow{R}(\delta_1) \cdot \mathrm{FM}\bigl(45^\circ + \theta_1\bigr) \cdot \overrightarrow{R}(\delta_1) \cdot E_1(t + \tau)$$

$$= \frac{1}{\sqrt{2}} \overleftarrow{R}(\delta_1) \cdot \mathrm{FM}\big(45^\circ + \theta_1\big) \cdot \overrightarrow{R}(\delta_1) \cdot E(t+\tau), \tag{8}$$

where τ is the time delay between the two arms of the Michelson interferometer. For the short arm, the electric field is

$$\begin{aligned} E_4 &= \overleftarrow{R}(\delta_2) \cdot \mathrm{FM}\big(45^\circ + \theta_2\big) \cdot \overrightarrow{R}(\delta_2) \cdot E_2(t) \cdot e^{i\varphi} \\ &= \frac{1}{\sqrt{2}} \overleftarrow{R}(\delta_2) \cdot \mathrm{FM}\big(45^\circ + \theta_2\big) \cdot \overrightarrow{R}(\delta_2) \cdot E(t) \cdot e^{i\varphi}, \end{aligned} \tag{9}$$

where φ is the phase shifted by PS. Then, the output electric field of the BS can be expressed as

$$\begin{bmatrix} E_5 \\ E_6 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} E_3 \\ E_4 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} E_3 + E_4 \\ E_3 - E_4 \end{bmatrix}. \tag{10}$$

Hence, the output light intensity of Michelson interferometer is given by

$$P_{\mathrm{out}} = E_5^* E_5 = \frac{1}{2} E_0^2 + \frac{1}{2} E_0^2 \Big(\sqrt{c^2 + d^2} \cos\big(\varphi + \omega\tau + \varepsilon(t) - \varepsilon(t+\tau) + \beta\big)\Big), \tag{11}$$

where $c = \sin(2\theta_1)\sin(2\theta_2)\cos(\delta_1 - \delta_2) + \cos(2\theta_1)\cos(2\theta_2)$, $d = \sin(2\theta_1)\sin(2\theta_2)\sin(\delta_1 - \delta_2)$ and $\beta = \arctan(c/d)$. The Michelson interference visibility ν can be deduced as follows $\nu = \sqrt{c^2 + d^2}$, which is related to the rotation angle deviation of FRM. Consequently, the imperfect FRM under external magnetic fields would change the visibility of the Michelson interferometer, which cannot satisfy the assumption that the visibility is always equal to 1 in other analyses.

Defining $\Delta\phi(t) = \phi(t) - \phi(t+\tau)$ represents the quantum random phase fluctuation which can be treated as Gaussian white noise [61]. The variance of $\Delta\phi(t)$ can be described by

$$\big\langle \Delta\phi^2(t) \big\rangle = \frac{2\tau}{\tau_c}, \tag{12}$$

where $\tau_c = (\pi \Delta\nu_{\mathrm{laser}})^{-1}$ is the coherence time of the laser, and $\Delta\nu_{\mathrm{laser}}$ is the linewidth of laser. In the QRNG scheme, the phase difference of the Michelson interferometer is stabilized at a constant value by adjusting the PS, i.e., $\varphi + \omega\tau + \beta = 2m\pi + \pi/2$ (m is an integer). After removing the direct current signal, the measured signal of the PD can be obtained,

$$I(t) \propto P\sqrt{c^2 + d^2} \sin\big(\Delta\phi(t)\big) \approx P\sqrt{c^2 + d^2}\,\Delta\phi(t), \tag{13}$$

where P is the laser power and $\Delta\phi(t)$ is sufficiently small. Hence, the phase fluctuation of the laser source can be measured directly by the intensity of the interferometer output. The output voltage of the PD fits with Gaussian distribution, whose variance contains the contributions of quantum noise and classical noise. Thus, we have

$$\sigma_t^2 = \sigma_q^2 + \sigma_c^2 = AP^2\big(c^2 + d^2\big)\big\langle \Delta\phi^2 \big\rangle + \sigma_c^2 = AP^2\big(c^2 + d^2\big)\frac{2\tau}{\tau_c} + \sigma_c^2, \tag{14}$$

and the mean value of output voltage $\mu = 0$, where A is the linear response constant between the optical power and voltage variance determined by the responsivity and gain of the PD. In general, the classical noise introduced by the background noise or the imperfect devices obeys a Gaussian distribution, and its variance σ_c^2 is invariable. Based on Eq. (14), it can be known that the total variance of output voltage and the variance of quantum noise are affected by the visibility of interferometer, while the imperfect FRM would influence the visibility of interferometer. To extract secure random bits from the raw data, an appropriate post-processing scheme should be performed, such as Toeplitz-hashing matrix function [18, 27, 29, 56, 63, 64], exclusive-OR operation [33–38] and m-least significant bits operation [36–38].

Meanwhile, entropy estimation is the key part to determine how many random bits can be extracted. The accuracy of entropy estimation will directly affect the randomness of generated random numbers and the security of practical QRNGs. Generally, min-entropy is used to quantify the amount of quantum randomness in a practical QRNG scheme. The min-entropy associated with the maximum guessing probability for an eavesdropper about variable X is defined as

$$H_{\min}(X) = -\log_2\Big[\max_{x_i \in X} P_X(x_i)\Big], \tag{15}$$

where $P_X(x_i)$ represents the probability distribution with variable X and $\max_{x_i\in X} P_X(x_i)$ is the highest probability of a single bin in a random variable X.

In the practical QRNG scheme, the quantum noise and classical noise E are time-independent and follow Gaussian distributions centred at zero with variances σ_q^2 and σ_c^2, respectively. Assuming that the eavesdropper has infinite computational power to fully master the classical noise E. Under this worst condition, to guarantee that the eavesdropper does not obtain any side information about the extracted random numbers through classical noise, we need to obtain a lower bound on the min-entropy in the presence of classical noise. The conditional min-entropy is

$$H_{\min}(X|E) = -\log_2\Big[\max_{x_i \in X|E} P_{X|E}(x_i)\Big]. \tag{16}$$

Hence, the quantum part of the measured signal needs to be accurately estimated. To maximize the extractable quantum randomness, the ratio of the quantum signals to classical noises is maximized. Considering the measured signal is sampled by an n-bit ADC, where the sampling range of ADC is $[-R+\Delta/2, R+3\Delta/2]$ and the bin width of ADC is $\Delta = R/2^{n-1}$, the probability distribution of discrete measurement results satisfies

$$P_{X|E}(x_i) = \begin{cases} \frac{1}{2}\mathrm{erfc}(\frac{R-0.5\Delta}{\sqrt{2}\sigma_q}), & i = i_{\min}, \\ \mathrm{erf}(\frac{\Delta}{2\sqrt{2}\sigma_q}), & i_{\min} < i < i_{\max}, \\ \frac{1}{2}\mathrm{erfc}(\frac{R-1.5\Delta}{\sqrt{2}\sigma_q}), & i = i_{\max}, \end{cases} \tag{17}$$

where $i_{\min} = -2^{n-1}$, $i_{\max} = 2^{n-1}$, and n is the sampling resolution. According to Eq. (16) and Eq. (17), there is a positive correlation between $H_{\min}(X)$ and σ_q^2, while the value of σ_q^2 is affected by the rotation angle deviation of Faraday rotator in the FRM. Therefore, the imperfect FRM influences the estimation of extractable randomness in a practical QRNG system.

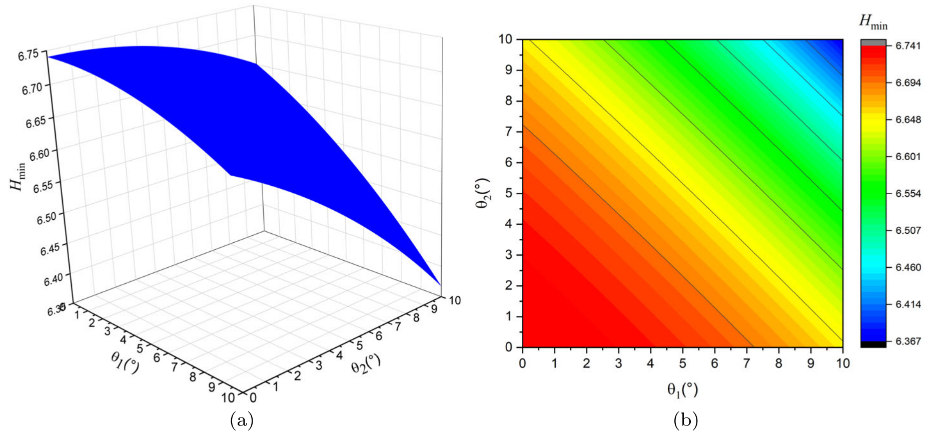

Figure 4 (a) The relationship between the conditional min-entropy $H_{\min}$ and the rotation angle deviations of FRMs. (b) Contour map of conditional min-entropy $H_{\min}$ in the X-Y axis plane in Fig. 4(a)

Table 1 A summary of the influences of imperfect FRMs on the extractable randomness

The rotation angle deviations of two FRMs	Conditional min-entropy	Security of the QRNG	Solution
Both unchanged	Not overestimated	Not affected	None
Only one changed	Overestimated	Affected	Details in Sect. 3.2.
Both unchanged	Overestimated	Affected	
Greater the changed	Greater the amount of overestimation	More affected	

According to Eq. (14), we suppose in an ideal scenario, that $A = 400$, $P = 1$ mW, $\delta_1 - \delta_2 = 0.9\pi$, $\tau = 540$ ps and $\tau_c = 2.5$ ns, $\sigma_c^2 = 0$, so the total variance σ_t^2 is equal to the quantum noise variance σ_q^2. The sampling range is set to $R = \pm 3\sigma_{q-\text{ideal}}$, where $\sigma_{q-\text{ideal}}$ is the standard deviation of quantum signal with two ideal FRMs, and the sampling resolution n is set to 8. By numerical simulation, the relationship between the conditional min-entropy $H_{\min}$ and the rotation angle deviations of FRMs is shown in Fig. 4, where we only consider the case in which $0 \leq \theta_1(\theta_2) \leq 10°$. When the two FMRs are ideal, i.e., the rotation angle deviation $\theta_1 = \theta_2 = 0$, the conditional min-entropy reaches the maximum value. As shown in Fig. 4, the conditional min-entropy gradually decreases with increasing rotation angle deviations of the FRMs. The rotation angle deviation of FRM leads to a decrease in the interferometer visibility, and thus reduces the variance in quantum noise and the calculated conditional min-entropy. Moreover, θ_1 and θ_2 show symmetry with $H_{\min}$, which means the two FRMs in the interferometer have the same effect on the extractable randomness. In other words, as long as one of the two FRMs is imperfect, the variance of quantum noise and conditional min-entropy will be affected. A summary of the influences of imperfect FRMs on the extractable randomness is shown in Table 1. Therefore, imperfect FRMs lead to lower conditional min-entropy in the case of $0° \leq \theta_1(\theta_2) \leq 10°$. If legitimate users fail to notice the imperfect FRMs introduced by external magnetic fields, the extractable randomness will be overestimated, which influences the randomness of the final random numbers. Therefore, the security of practical QRNG systems under external magnetic fields would be threatened.

3.1.2 Impact of sampling device under the QRNG with imperfect FRM

The electrical signal is discretized into a digital signal by an ADC to obtain the raw data. To achieve a high generation rate, the parameters of ADC need to be optimized in practical QRNGs, which are important for the estimation of extractable randomness. We have demonstrated that the performance of FRM can be affected by external magnetic fields. Meanwhile, the different parameters of ADC may have different effects on the estimation of the extractable randomness under external magnetic fields. Hence, the impacts of ADC parameters should be discussed in detail.

The sampling range R and sampling resolution n are two important parameters of the ADC. By defining a parameter called normalized conditional min-entropy in our analysis, the influences of the sampling range and sampling resolution on the extractable randomness are discussed. The normalized conditional min-entropy is defined as $H_{\text{min-norm}} = H_{\text{min}}/n$, which represents the number of extractable secure randomness per bit. To simplify, we analyze the cases in which the rotation angle deviations of two FRMs are the same and $\theta_1 = \theta_2 = 0°, 5°, 10°$ for the subsequent analysis. The sampling range R can be defined as $R = \pm k\sigma_{q\text{-ideal}}$, where k is the ratio between sampling range R and the standard deviation of ideal quantum signal $\sigma_{q\text{-ideal}}$. The finite sampling range will lead to the measured signal outside the range $\pm k\sigma_{q\text{-ideal}}$ falling into the first or last bins of an ADC. The simulation results shown in Fig. 5 are obtained with a sampling resolution of $n = 8$, where the sampling range R is increased from $\sigma_{q\text{-ideal}}$ to $6\sigma_{q\text{-ideal}}$ with a step of $0.1\sigma_{q\text{-ideal}}$. When the QRNG is not attacked by external magnetic field, that is, the FRMs are perfect, the optimal sampling range R is approximately $2.5\sigma_{q\text{-ideal}}$, corresponding to 0.87548 extractable secure random bits per bit. And the optimal sampling range decreases with the increase of rotation angle deviation. Moreover, the difference in the normalized conditional min-entropy between the QRNG with imperfect FRMs and that with ideal FRMs slightly increases with the sampling range when the sampling range is greater than $2.5\sigma_{q\text{-ideal}}$. Therefore, the influence of external magnetic fields on extractable randomness can be reduced by optimizing the sampling range, such as the optimal sampling range for an ideal FRM. As shown in Fig. 5, when R is smaller than a threshold value, the values of $H_{\text{min-norm}}$ at 5° and 10° are greater than that at 0° in the same sampling range. The sampling range is too small resulting in the peak value of the probability distribution in the first and last bins of ADC. As a consequence, if the sampling range for the QRNG with ideal FRMs is lower than the threshold value, the randomness of the final generated random numbers may not be affected by the imperfect FRM, because the extractable randomness is underestimated in the practi-

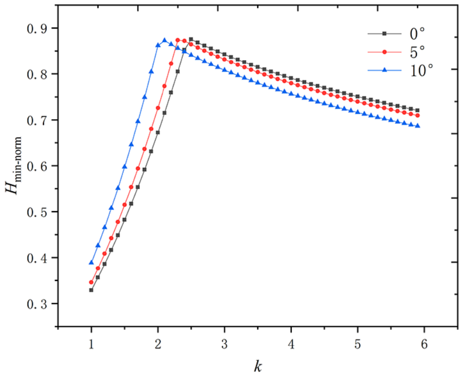

Figure 5 Simulation results for the normalized conditional min-entropy $H_{\text{min-norm}}$ as a function of k related to the sampling range at different rotation angle deviations. The grey squared line, red dotted line and blue triangular line represent the rotation angle deviations at 0°, 5°, 10°, respectively

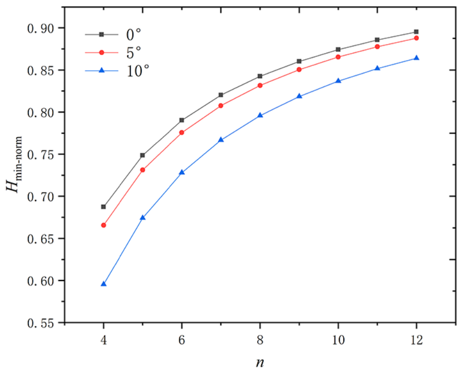

Figure 6 Simulation results for the normalized conditional min-entropy $H_{\mathrm{min-norm}}$ as a function of the sampling resolution n for different rotation angle deviations. The grey squared line, red dotted line and blue triangular line represent the rotation angle deviation at 0°, 5°, 10°, respectively

Table 2 A summary of the impacts of sampling device under the QRNG with imperfect FRM

Sampling range	Sampling resolution	Normalized conditional min-entropy	Security of the QRNG	Solution
Below threshold value	Normal	Not overestimated	Not affected	None
Exceed threshold value	Normal	Not overestimated	Affected	Setting a suitable sampling rangeand increasing the sampling resolution, as well as the other solutions in Sect. 3.2.
Exceed threshold value	Larger	Smaller the amount of overestimation	Less affected	

cal QRNG system. Overall, the influence of external magnetic fields on the security of the QRNG can be reduced by adjusting the sampling range of ADC, where it is recommended that the sampling range does not exceed the optimal sampling range.

The sampling resolution n of ADC is related to the loss of information induced by the discretized sampled probability distribution of the measured signal, which significantly impacts the estimation of randomness for practical QRNGs. Figure 6 shows the simulation results for the normalized conditional min-entropy $H_{\mathrm{min-norm}}$ as a function of n by setting the sampling range $R = \pm 3\sigma_{q\mathrm{-ideal}}$ and the rotation angle deviations of 0°, 5°, 10°, respectively. Intuitively, $H_{\mathrm{min-norm}}$ increases with the sampling resolution n at different rotation angle deviations. When the quantum phase fluctuation based QRNG is disturbed by external magnetic fields, $H_{\mathrm{min-norm}}$ is significantly reduced. Besides, the difference between the $H_{\mathrm{min-norm}}$ of the QRNG with perfect FRMs and that with imperfect FRMs decreases with the increase of n. From the legitimate user's point of view, a greater n allows eavesdropper to steal less information from each bit. As shown in Fig. 5 and Fig. 6, the difference of $H_{\mathrm{min-norm}}$ at 0° and 5° is significantly lower than that of 5° and 10°. In other words, in the presence of the same rotation angle deviation increase, the greater the rotation angle deviation of FRM initially, the greater the reduction in extractable randomness. In conclusion, the sampling range and resolution both have impacts on the extractable randomness of the QRNG with imperfect FRMs. Methods such as properly setting the sampling range N and increasing the sampling resolution n will help to resist the influence of an external magnetic field and thus improve the security of final generated random numbers. As shown in Table 2, we give a summary of the impacts of sampling device under QRNG with imperfect FRM.

3.2 Countermeasures against the influences of imperfect FRM induced by external magnetic fields

In the previous sections, we found that the rotation angle deviations of FRMs are influenced by the strength of the external magnetic field, thus compromising the final extractable randomness and security of quantum phase fluctuation based QRNG with unbalanced Michelson interferometer system. To protect the QRNG from external magnetic fields, we propose countermeasures from two different perspectives: the magnetic field and FRM.

Adding devices to shield and monitor the magnetic fields around the practical QRNG system is a straightforward countermeasure. The low impedance and high permeability of the ferromagnetic material allow the magnetic field inside the shield to be significantly reduced. In the QRNG based on quantum phase fluctuation, the magnetic shielding of sensitive devices can be achieved by using a hollow shell made of high permeability ferromagnetic materials to enclose the materials sensitive of sensitivity to magnetic field strength. Nevertheless, limited by the shielding ability of the magnetic field, the security of the QRNG system can still be compromised by an eavesdropper that increases the strength of external magnetic field. Thus, it is necessary to deploy devices to monitor magnetic fields, such as Hall elements and semiconductor magnetoresistance elements. Hall elements based on the Hall effect reflect the magnitude of the external magnetic field by the Hall voltage, and semiconductor magnetoresistance elements based on the magnetoresistive effect can determine whether the magnetic field is changed by its resistance value. By integrating the Hall elements or semiconductor magnetoresistance elements in the QRNG system, the external magnetic field strength can be monitored. Once the Hall voltage or resistance changes above a certain threshold, it indicates that the security of the QRNG is at risk. Hence, the security of the QRNG system can be guaranteed by the necessary magnetic field shielding and monitoring.

On the other hand, external magnetic fields lead to imperfections in FRMs, so countermeasures can be taken to solve the impact of imperfect FRM on quantum phase fluctuation based QRNG with unbalanced Michelson interferometer. The imperfect FRMs in the Michelson interferometer causes the polarization state of the reflected signal to be unable to rotate 90° accurately, which reduces the visibility of the interferometer and affects the extractable randomness. Thus, by adding a polarization state measurement device and

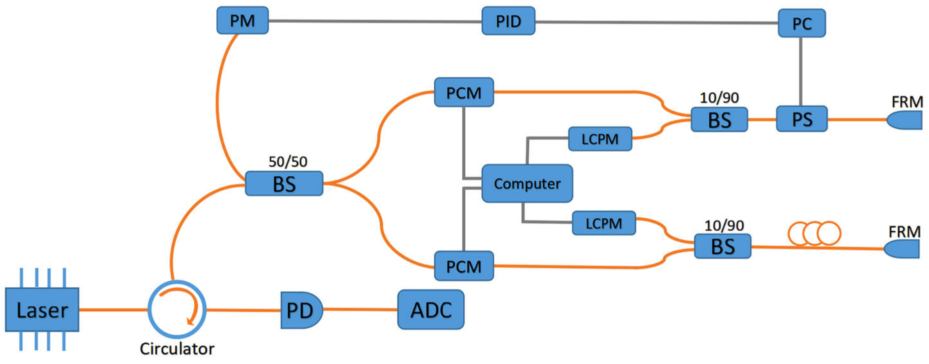

Figure 7 Specific experimental device for polarization control countermeasure. LCPM: liquid crystal polarization meter

polarization control module (PCM) in the QRNG, the polarization state of the signal reflected by the FRM can be guaranteed to be rotated by 90°. The detailed polarization control countermeasure experimental device is shown in Fig. 7. The signal reflected by the FRM passes through a 10:90 BS and is split into two parts: one part (10%) is connected to a liquid crystal polarization meter (LCPM) to measure the polarization state of the signal, which has the merit of high stability and accuracy; the other part (90%) is transmitted and connected to a PCM used to modulate the polarization state of the signal. The measurement results of LCPM are uploaded to a computer that sends a feedback signal to precisely tune the PCM in real time. In this way, the polarization state of the signal reflected by the FRM can be stably maintained. For the signal reflected by another FRM, the same method is used to maintain the stability of the polarization state of the signal, as shown in Fig. 7. Thereby, the polarization control countermeasures could resist the impact of imperfect FRM and improve the security of the practical QRNG.

4 Conclusion

In this work, we have analyzed the impacts of external magnetic fields on the practical security of a quantum phase fluctuation based QRNG with unbalanced Michelson interferometer. We experimentally investigated the variation in the rotation angle of the FRM under different external magnetic fields. The experimental results show that the effect of external magnetic field on the rotation angle is significant when the directions of external and internal magnetic fields are opposite as well as the strength of external magnetic field exceeds a certain threshold. Therefore, by controlling the strength of the magnetic field around the FRM, an adversary may cause imperfect performance of FRM, which opens a vulnerability in for the security of the QRNG. Based on this vulnerability, we investigate the influences of imperfect FRM. Through numerical simulation, we find that the variance of measured signal and extractable randomness can be influenced by external magnetic fields. The conditional min-entropy decreases with the rotation angle deviation of FRM in the case of $0 \leq \theta_1(\theta_2) \leq 10°$. Without noticing the rotation angle deviation of FRM introduced by external magnetic fields, the extractable randomness will be overestimated. Furthermore, we also consider the impacts of the sampling device on the estimation of extractable randomness in the presence of imperfect FRM. The simulation results reveal that the methods of appropriately setting sampling range and increasing sampling resolution could help to resist the influence of external magnetic fields and improve the security of practical QRNG systems. Finally, we proposed some countermeasures against the impacts of external magnetic fields, which include adding magnetic field shielding (monitoring) devices and utilizing a PCM to control the polarization state of the signal.

Our results have demonstrated that the security of practical QRNGs is affected by external magnetic fields. For QRNGs operating in complex magnetic fields with inadequate shielding, the extractable randomness may be reduced due to the imperfect equipment disturbed by external magnetic fields. Moreover, an eavesdropper can exploit vulnerabilities related to magnetic field strength to eavesdrop on the final generated random numbers. In summary, our work reveals the importance of considering the influence of external magnetic fields and deploying corresponding countermeasures to guarantee the security of practical QRNGs.

Acknowledgements

The authors thank Henan Key Laboratory of Network Cryptography Technology for equipment supply.

Funding
This work was supported by the National Natural Science Foundation of China (No. 61901525, 61972413, 62002385) and National Key R&D Program of China (No. 2021YFB3100100).

Abbreviations
QRNG, Quantum random number generator; FRM, Faraday rotation mirror; QKD, quantum key distribution; PD, photodetector; DI-QRNG, device-independent QRNG; SDI-QRNG, semi-device-independent QRNG; BS, beam splitter; PS, phase shifter; PM, power meter; PID, proportional-integral-derivative; PC, piezo con-troller; ADC, analog-to-digital converter; PCM, polarization control module; PBS, polarization BS; SMF, single mode fiber; LCPM, liquid crystal polarization meter.

Availability of data and materials
The data that support the findings of this study can be obtained from the corresponding author upon a reasonable request.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
All authors have approved the publication. The research in this work did not involve any human, animal or other participants.

Competing interests
The authors declare no competing interests.

Author contributions
Yuan-Hao Li performed security analysis and wrote the first version of the manuscript. Yang-Yang Fei and Wei-Long Wang conceived the idea for this work and analyzed partial results. Xiang-Dong Meng and Yu Han performed the experimental work. Hong Wang and Qian-Heng Duan conducted partial security analysis. Zhi Ma conceived and supervised the work. All authors reviewed and approved the final manuscript.

Received: 8 May 2023 Accepted: 13 November 2023 Published online: 20 November 2023

References

1. Stinson DR. Cryptography theory and practice. Boca Raton: CRC Press; 1995.
2. Ferrenberg AM, Landau DP, Wong YJ. Monte Carlo simulations: hidden errors from "good" random number generators. Phys Rev Lett. 1992;69:3382–4.
3. Hall C, Schneier B. Remote electronic gambling. In: Computer security applications conference. 2002.
4. Calude CS, Dinneen MJ, Dumitrescu M, Svozil K. Experimental evidence of quantum randomness incomputability. Phys Rev A. 2010;82:022102.
5. Bera MN, Acín A, Kuś M, Mitchell MW, Lewenstein M. Randomness in quantum mechanics: philosophy, physics and technology. Rep Prog Phys. 2017;80(12):124001.
6. Stefanov A, Gisin N, Guinnard O, Guinnard L, Zbinden H. Optical quantum random number generator. J Mod Opt. 2000;47(4):595–8.
7. Ma H-Q, Xie Y, Wu L-A. Random number generation based on the time of arrival of single photons. Appl Opt. 2005;44(36):7760–3.
8. Dynes JF, Yuan ZL, Sharpe AW, Shields AJ. A high speed, postprocessing free, quantum random number generator. Appl Phys Lett. 2008;93(3):031109.
9. Nie Y-Q, Zhang H-F, Zhang Z, Wang J, Ma X, Zhang J, Pan J-W. Practical and fast quantum random number generation based on photon arrival time relative to external reference. Appl Phys Lett. 2014;104(5):051110.
10. Fürst H, Weier H, Nauerth S, Marangon DG, Kurtsiefer C, Weinfurter H. High speed optical quantum random number generation. Opt Express. 2010;18(12):13029–37.
11. Ren M, Wu E, Liang Y, Jian Y, Wu G, Zeng H. Quantum random-number generator based on a photon-number-resolving detector. Phys Rev A. 2011;83(2):023820.
12. Sharma V, Bhardwaj A. Analysis of differential phase shift quantum key distribution using single-photon detectors. In: 2022 international conference on numerical simulation of optoelectronic devices (NUSOD). 2022. p. 17–8. https://doi.org/10.1109/NUSOD54938.2022.9894772.
13. Sharma V, Banerjee S. Quantum communication using code division multiple access network. Opt Quantum Electron. 2020;52:381.
14. Sharma V, Banerjee S. Analysis of atmospheric effects on satellite-based quantum communication: a comparative study. Quantum Inf Process. 2019;18:67.
15. Yin J, Cao Y, Li Y-H, Ren J-G, Liao S-K, Zhang L, Cai W-Q, Liu W-Y, Li B, Dai H et al. Satellite-to-ground entanglement-based quantum key distribution. Phys Rev Lett. 2017;119(20):200501.
16. Er-Long M, Zheng-Fu H, Shun-Sheng G, Tao Z, Da-Sheng D, Guang-Can G. Background noise of satellite-to-ground quantum key distribution. New J Phys. 2005;7(1):215.
17. Gabriel C, Wittmann C, Sych D, Dong R, Mauerer W, Andersen UL, Marquardt C, Leuchs G. A generator for unique quantum random numbers based on vacuum states. Nat Photonics. 2010;4(10):711–5.
18. Haw JY, Assad SM, Lance AM, Ng NHY, Sharma V, Lam PK, Symul T. Maximization of extractable randomness in a quantum random-number generator. Phys Rev Appl. 2015;3:054004. https://doi.org/10.1103/PhysRevApplied.3.054004.

19. 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. https://doi.org/10.1103/PhysRevA.81.063814.
20. Zheng Z, Zhang Y, Huang W, Yu S, Guo H. 6 Gbps real-time optical quantum random number generator based on vacuum fluctuation. Rev Sci Instrum. 2019;90(4):043105.
21. Qi B, Chi Y-M, Lo H-K, Qian L. High-speed quantum random number generation by measuring phase noise of a single-mode laser. Opt Lett. 2010;35(3):312–4.
22. Guo H, Tang W, Liu Y, Wei W. Truly random number generation based on measurement of phase noise of a laser. Phys Rev E. 2010;81(5):051137.
23. Abellán C, Amaya W, Jofre M, Curty M, Acín A, Capmany J, Pruneri V, Mitchell M. Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode. Opt Express. 2014;22(2):1645–54.
24. Lei W, Xie Z, Li Y, Fang J, Shen W. An 8.4 Gbps real-time quantum random number generator based on quantum phase fluctuation. Quantum Inf Process. 2020;19(11):405.
25. Zhang X-G, Nie Y-Q, Zhou H, Liang H, Ma X, Zhang J, Pan J-W. Note: fully integrated 3.2 Gbps quantum random number generator with real-time extraction. Rev Sci Instrum. 2016;87(7):076102.
26. Zhu Y, Lu Y, Zhu J, Zeng G. High speed quantum-random-number generation via measurement on phase noise of laser. Int J Quantum Inf. 2011;9(04):1113–22.
27. Nie Y-Q, Huang L, Liu Y, Payne F, Zhang J, Pan J-W. The generation of 68 Gbps quantum random number by measuring laser phase fluctuations. Rev Sci Instrum. 2015;86(6):063105.
28. Xu F, Qi B, Ma X, Xu H, Zheng H, Lo H-K. Ultrafast quantum random number generation based on quantum phase fluctuations. Opt Express. 2012;20(11):12366–77.
29. Liu J, Yang J, Li Z, Su Q, Huang W, Xu B, Guo H. 117 Gbits/s quantum random number generation with simple structure. IEEE Photonics Technol Lett. 2017;29(3):283–6. https://doi.org/10.1109/LPT.2016.2639562.
30. Raffaelli F, Sibson P, Kennard JE, Mahler DH, Thompson MG, Matthews JCF. Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip. Opt Express. 2018;26(16):19730–41. https://doi.org/10.1364/OE.26.019730.
31. Shakhovoy R, Sharoglazova V, Udaltsov A, Duplinskiy A, Kurochkin V, Kurochkin Y. Influence of chirp, jitter, and relaxation oscillations on probabilistic properties of laser pulse interference. IEEE J Quantum Electron. 2021;57(2):1–7.
32. Shakhovoy R, Sych D, Sharoglazova V, Udaltsov A, Fedorov A, Kurochkin Y. Quantum noise extraction from the interference of laser pulses in an optical quantum random number generator. Opt Express. 2020;28(5):6209–24.
33. Williams CR, Salevan JC, Li X, Roy R, Murphy TE. Fast physical random number generator using amplified spontaneous emission. Opt Express. 2010;18(23):23584–97.
34. Li X, Cohen AB, Murphy TE, Roy R. Scalable parallel physical random number generator based on a superluminescent LED. Opt Lett. 2011;36(6):1020–2.
35. Wei W, Xie G, Dang A, Guo H. High-speed and bias-free optical random number generator. IEEE Photonics Technol Lett. 2011;24(6):437–9.
36. Li Y, Fei Y, Wang W, Meng X, Wang H, Duan Q, Ma Z. Analysis of the effects of temperature increase on quantum random number generator. Eur Phys J D. 2021;75(2):1–9.
37. Li Y, Fei Y, Wang W, Meng X, Wang H, Duan Q, Ma Z. Experimental study on the security of superluminescent led-based quantum random generator. Opt Eng. 2021;60(11):116106.
38. Guo Y, Cai Q, Li P, Jia Z, Xu B, Zhang Q, Zhang Y, Zhang R, Gao Z, Shore KA et al. 40 Gb/s quantum random number generation based on optically sampled amplified spontaneous emission. APL Photon. 2021;6(6):066105.
39. Pironio S, Acín A, Massar S, de La Giroday AB, Matsukevich DN, Maunz P, Olmschenk S, Hayes D, Luo L, Manning TA et al. Random numbers certified by bell's theorem. Nature. 2010;464(7291):1021–4.
40. Liu Y, Yuan X, Li M-H, Zhang W, Zhao Q, Zhong J, Cao Y, Li Y-H, Chen L-K, Li H, Peng T, Chen Y-A, Peng C-Z, Shi S-C, Wang Z, You L, Ma X, Fan J, Zhang Q, Pan J-W. High-speed device-independent quantum random number generation without a detection loophole. Phys Rev Lett. 2018;120:010503. https://doi.org/10.1103/PhysRevLett.120.010503.
41. Liu W-Z, Li M-H, Ragy S, Zhao S-R, Bai B, Liu Y, Brown PJ, Zhang J, Colbeck R, Fan J et al. Device-independent randomness expansion against quantum side information. Nat Phys. 2021;17(4):448–51.
42. Cao Z, Zhou H, Yuan X, Ma X. Source-independent quantum random number generation. Phys Rev X. 2016;6:011020. https://doi.org/10.1103/PhysRevX.6.011020.
43. Marangon DG, Vallone G, Villoresi P. Source-device-independent ultrafast quantum random number generation. Phys Rev Lett. 2017;118:060503. https://doi.org/10.1103/PhysRevLett.118.060503.
44. Xu B, Chen Z, Li Z, Yang J, Su Q, Huang W, Zhang Y, Guo H. High speed continuous variable source-independent quantum random number generation. Quantum Sci Technol. 2019;4(2):025013. https://doi.org/10.1088/2058-9565/ab0fd9.
45. Nie Y-Q, Guan J-Y, Zhou H, Zhang Q, Ma X, Zhang J, Pan J-W. Experimental measurement-device-independent quantum random-number generation. Phys Rev A. 2016;94:060301. https://doi.org/10.1103/PhysRevA.94.060301.
46. Cao Z, Zhou H, Ma X. Loss-tolerant measurement-device-independent quantum random number generation. New J Phys. 2015;17(12):125011. https://doi.org/10.1088/1367-2630/17/12/125011.
47. Lunghi T, Brask JB, Lim CCW, Lavigne Q, Bowles J, Martin A, Zbinden H, Brunner N. Self-testing quantum random number generator. Phys Rev Lett. 2015;114(15):150501.
48. Li H-W, Yin Z-Q, Wu Y-C, Zou X-B, Wang S, Chen W, Guo G-C, Han Z-F. Semi-device-independent random-number expansion without entanglement. Phys Rev A. 2011;84(3):034301.
49. Bowles J, Quintino MT, Brunner N. Certifying the dimension of classical and quantum systems in a prepare-and-measure scenario with independent devices. Phys Rev Lett. 2014;112(14):140407.
50. Chen Z, Li Z, Xu B, Zhang Y, Guo H. The m-least significant bits operation for quantum random number generation. J Phys B, At Mol Opt Phys. 2019;52(19):195501. https://doi.org/10.1088/1361-6455/ab3c01.
51. Huang W, Zhang Y, Zheng Z, Li Y, Xu B, Yu S. Practical security analysis of a continuous-variable quantum random-number generator with a noisy local oscillator. Phys Rev A. 2020;102:012422. https://doi.org/10.1103/PhysRevA.102.012422.
52. Shakhovoy R, Puplauskis M, Sharoglazova V, Duplinskiy A, Sych D, Maksimova E, Hydyrova S, Tumachek A, Mironov Y, Kovalyuk V, Prokhodtsov A, Goltsman G, Kurochkin Y. Phase randomness in a semiconductor laser: issue of quantum random-number generation. Phys Rev A. 2023;107:012616. https://doi.org/10.1103/PhysRevA.107.012616.

53. Schranz Á, Marosits Á, Udvary E. Effects of sampling rate on amplified spontaneous emission based single-bit quantum random number generation. In: 2019 21st international conference on transparent optical networks (ICTON). Los Alamitos: IEEE; 2019. p. 1–4.
54. Zanforlin U, Donaldson RJ, Collins RJ, Buller GS. Analysis of the effects of imperfections in an optical heterodyne quantum random-number generator. Phys Rev A. 2019;99:052305. https://doi.org/10.1103/PhysRevA.99.052305.
55. Li F-Y, Wang D, Wang S, Li M, Yin Z-Q, Li H-W, Chen W, Han Z-F. Effect of electromagnetic disturbance on the practical QKD system in the smart grid. Chin Phys B. 2014;23(12):124201.
56. Sharma V, Banerjee S. Analysis of quantum key distribution based satellite communication. In: 2018 9th international conference on computing, communication and networking technologies (ICCCNT). 2018. p. 1–5. https://doi.org/10.1109/ICCCNT.2018.8494189.
57. Reezwana A, Islam T, Bai X, Wildfeuer CF, Ling A, Grieve JA. A quantum random number generator on a nanosatellite in low Earth orbit. Commun Phys. 2022;5(1):314.
58. Smith PR, Marangon DG, Lucamarini M, Yuan ZL, Shields AJ. Out-of-band electromagnetic injection attack on a quantum random number generator. Phys Rev Appl. 2021;15:044044.
59. Tan H, Zhang W-Y, Zhang L, Li W, Liao S-K, Xu F. External magnetic effect for the security of practical quantum key distribution. Quantum Sci Technol. 2022;7(4):045008. https://doi.org/10.1088/2058-9565/ac7d07.
60. Petermann K. Laser diode modulation and noise. vol. 3. Berlin: Springer; 1991.
61. Henry C. Theory of the linewidth of semiconductor lasers. IEEE J Quantum Electron. 1982;18(2):259–64.
62. Sharma V. Effect of noise on practical quantum communication systems. Def Sci J. 2016;66:186–92. https://doi.org/10.14429/dsj.66.9771.
63. Ma X, Xu F, Xu H, Tan X, Qi B, Lo H-K. Postprocessing for quantum random-number generators: entropy evaluation and randomness extraction. Phys Rev A. 2013;87:062327. https://doi.org/10.1103/PhysRevA.87.062327.
64. Ma X, Yuan X, Cao Z, Qi B, Zhang Z. Quantum random number generation. npj Quantum Inf. 2016;2:016021.
65. Gehring T, Lupo C, Kordts A, Solar Nikolic D, Jain N, Rydberg T, Pedersen TB, Pirandola S, Andersen UL. Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information. Nat Commun. 2021;12:605.
66. Bruynsteen C, Gehring T, Lupo C, Bauwelinck J, Yin X. 100-Gbit/s integrated quantum random number generator based on vacuum fluctuations. PRX Quantum. 2023;4:010330. https://doi.org/10.1103/PRXQuantum.4.010330.
67. Dani RK, Wang H, Bossmann SH, Wysin G, Chikan V. Faraday rotation enhancement of gold coated Fe_2o_3 nanoparticles: comparison of experiment and theory. J Chem Phys. 2011;135(22):224502.
68. Royer F, Jamon D, Rousseau JJ, Cabuil V, Zins D, Roux H, Bovier C. Experimental investigation on γ-Fe_2o_3 nanoparticles Faraday rotation: particles size dependence. Eur Phys J Appl Phys. 2003;22(2):83–7.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.