Measurement-Device-Independent Quantum Random-Number Generator With Source Flaws

Tao Wu, Chun-Hui Zhang, Xing-Yu Zhou, Jian Li, and Qin Wang

***Abstract*—The measurement-device-independent quantum random number generator (MDI-QRNG) can resist all security loopholes on measurement devices, and it thus seems very promising in practical implementations. In the MDI-QRNG, sources are often assumed to be perfectly prepared, however, there inevitably exist errors in the quantum state preparation process due to imperfections in realistic equipments and devices. In this paper, we do investigations on the MDI-QRNG with source flaws, showing its performance at different state errors. Besides, we also consider the influence of the finite-size effect, and compare the performance of different sources in MDI-QRNGs. This work provides valuable references for practical implementation of MDI-QRNGs.**

***Index Terms*—Quantum random-number generation, measurement-device-independent, source flaws, finite-size effects.**

I. Introduction

RANDOM numbers have wide applications in many fields of scientific research, such as cryptography, secure communication, and quantitative finance [1]. How to generate plenty of true random numbers with high speed is an essential scientific problem. Although some computer-generated random numbers, called pseudo-random numbers [2], can pass various number verification procedures, they are determined by given algorithm and seed, which in principle can be predicted and may introduce security loopholes to applications. Recently, with the development of quantum information technology, it is discovered that the inherent randomness of quantum mechanics can be used to generate true random numbers, called the quantum random number generator (QRNG), which posseses the inherent characteristic of unpredictability [3], [4], [5], [6], [7], [8], [9], [10]. It is based on some quantum processes such as measurement collapse and vacuum fluctuations. The most typical QRNG scheme [11], [12]is consisting of one 50-50 beam-splitter and two single-photon detectors. Besides, methods on high-speed random bit generation based on other mechanism such as chaotic lasers had also been reported [13], [14].

According to whether the device is trusted or not, we can divide QRNGs into three categories, device-trusted QRNGs [12], device-independent QRNGs (DI-QRNGs) [15] and semi-device-independent QRNGs (SDI-QRNGs) [16], [17], [18], [19], [20], [21], [24]. Among them, the device-trusted QRNG assumes that the devices are entirely credible, in which quantum random numbers can be generated at high speed by designing a suitable circuit. The technology of this type QRNG is relatively mature and has gradually moved towards commercialization. However, this perfect assumption on devices may not be satisfied in practical applications, leading to security risks in the generated random numbers. The DI-QRNG assumes that the devices are completely untrustworthy, and mainly based on the violation of Bell's inequality in quantum mechanics [25], [26]. From the perspective of security, the random numbers generated by the DI-QRNG protocol possess the highest security, however, its random number generation rate is relatively lower due to the limitations on entangled source generations with current technologies. As a result, some researchers proposed the SDI-QRNG protocol by referring the idea in MDI-QKD protocols [27], [28], [29]. As a compromised solution, the SDI-QRNG only makes some simple assumptions on devices, but it can significantly increase the generation rate of quantum random numbers, and possess higher security than the device-trusted one.

Usually, there are three types of SDI-QRNGs, the source-independent QRNG (SI-QRNG) [18], [19], [20], the measurement-device-independent QRNG (MDI-QRNG) [21], [24], and the SDI-QRNG based on dimension witness [16], [17]. The main differences among the protocols are that they make different assumptions about the source or the measurement. In the SI-QRNG, the source is assumed to be untrusted while the measurement is trusted. On the contrast, in the MDI-QRNG, the source is assumed to be trusted while the measurement is untrusted. Furthermore, the SDI-QRNG based on dimension witness only assumes that the source and measurement are independent and a fixed dimension. However, there always exist errors in the state-preparation process due to imperfect devices. Therefore, we should take the state-preparation error into account in practical applications of MDI-QRNGs. Otherwise, it may cause loopholes and make the random numbers insecure. In the following, we investigate the MDI-QRNG with source flaws

Manuscript received 31 July 2023; revised 3 October 2023; accepted 5 November 2023. Date of publication 9 November 2023; date of current version 24 November 2023. This work was supported in part by the National Natural Science Foundation of China under Grants 12074194, 12104240, 62101285, and U19A2075, in part by the Industrial Prospect and Key Core Technology Projects of Jiangsu provincial key R&D Program under Grant BE2022071, in part by the Natural Science Foundation of Jiangsu Province under Grants BK20192001 and BK20210582, and in part by the NUPTSF under Grants NY220122 and NY220123. *(Tao Wu and Chun-Hui Zhang contributed equally to this work.) (Corresponding author: Qin Wang.)*

The authors are with the Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China, also with the Broadband Wireless Communication and Sensor Network Technology, Key Lab of Ministry of Education, NUPT, Nanjing 210003, China, also with the Telecommunication and Networks, National Engineering Research Center, NUPT, Nanjing 210003, China, and also with the Key Laboratory of Quantum Information, University of Science and Technology of China, Chinese Academy of Sciences, Hefei 230026, China (e-mail: qinw@njupt.edu.cn).

Digital Object Identifier 10.1109/JPHOT.2023.3331547

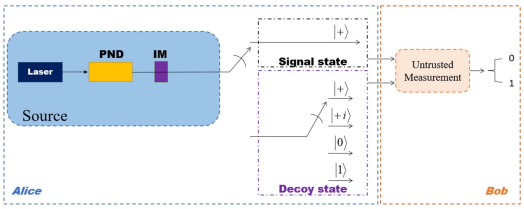

Fig. 1. (Color online) A schematic diagram of the MDI-QRNG protocol. PND, photon-number distribution; IM, intensity modulator.

and different light sources. Moreover, the finite-size effects are also taken into account.

II. MDI-QRNG With Sources Flaws

The schematic of MDI-QRNG protocol is illustrated in Fig. 1. It includes the state preparation and the measurement parts, where Alice plays the role of state preparations, and Bob carries out positive operator-valued measurements (POVM).Moreover, a three-intensity decoy-state method is applied. Next, we introduce the decoy-state MDI-QRNG.

Step 1: The light source with certain photon-number distribution (PND) is modulated into three different light intensities through an intensity modulator (IM) with random number seeds: $S_\emptyset$, S_d and S_s, and $S_\emptyset + S_d + S_s = \{1, 2, 3, \ldots, N\}$. Accordingly, the photon possesses three different average photon numbers, denoted as the vacuum $u_\emptyset$, the decoy u_d and the signal u_s, individually.

Step 2: The light pulses with intensity u_d are randomly prepared into one of states $\{|0\rangle, |1\rangle, |+\rangle, |+i\rangle\}$, where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|+i\rangle = (|0\rangle + i|1\rangle)/\sqrt{2}$, while the pulses with intensity of u_s are always encoded as $|+\rangle$.

Step 3: All the pulses are transmitted to Bob and are performed with positive operator-valued measures (POVMs) by Bob. All the outputs are recorded as a sequence with bit $b \in \{0, 1\}$. The value of b is decided by which detector clicking in two detectors. Other click events are discarded.

Step 4: With the measurement results of the decoy pulses and the vacuum pulses, we can tightly estimate the POVM parameters in randomness extraction rate R. After performing randomness extraction on the signal outputs, the random numbers can be generated with a length NR.

Here, we should specify that there are some differences between the QKD and the QRNG. First, the goal of QKD and QRNG are different. The former is to share identical secret keys between two remote users, Alice and Bob, while for the latter, the goal is to generate random bits at the measurement part. Second, there are differences in the post-processing process. In a QKD, Alice and Bob need to carry out error corrections and privacy amplifications to obtain identical keys, while in a QRNG, Bob only needs to perform privacy amplifications to achieve random bits, and does not need to proceed the error correction process. Besides, the decoy method in QRNG is introduced not only to detect attacks of eavesdroppers when generating random numbers in different locations, but also to help us tightly estimate the POVM parameters in calculating the randomness extraction rate. According to the analysis model in [21], we can derive the POVM operation on a k-photon pulse with output b as $F_{b|k}$,

$$F_{b|k} = a_{b|k}(I + \overrightarrow{n}_{b|k} \cdot \overrightarrow{\sigma}),\ \overrightarrow{n}_{b|k} = (n_{b_x|k}, n_{b_y|k}, n_{b_z|k}), \quad (1)$$

where $b \in \{0, 1\}, k \geq 1$. If a pulse is vacuum, the virtual POVM operation is $F_{b|0} = a_{b|0} I$. All the parameters satisfy

$$\begin{aligned} &a_{b|k} \geq 0, a_{0|k} + a_{1|k} = 1, k \geq 0, \\ &\overrightarrow{n}_{b|k} \leq 1, a_{0|k}\overrightarrow{n}_{0|k} + a_{1|k}\overrightarrow{n}_{1|k} = \overrightarrow{0}, \end{aligned} \quad (2)$$

Based on the POVM results, the rate of random bits extracted from the output signal is given by

$$R = 2p_{1|s}a_{0|1}H_{\min}\left(\frac{1 + \sqrt{1 - (n_{0_y|1})^2 - (n_{0_z|1})^2}}{2}\right), \quad (3)$$

where $p_{k|\gamma}$ is the photon-number distribution, denoting the probability of a k-photon state in source γ, $n_{0_y|1}$ and $n_{0_z|1}$ are the second and third elements in $\overrightarrow{n}_{0|1}$, and $H_{\min}(x) = -\log_2 max(x, 1-x)$ is the min-entropy function. The random bits are extracted from the single-photon components of signal pulses, and the extraction rate is related to the randomness in the signal outputs and evaluated by the min-entropy function $H_{\min}(x)$.

Due to the imperfection of the device, we take the state-preparation error [22], [23] into account.

$$\begin{aligned} |\phi_0\rangle &= \cos\left(\frac{\delta_1}{2}\right)|0\rangle + \sin\left(\frac{\delta_1}{2}\right)|1\rangle \\ |\phi_1\rangle &= \sin\left(\frac{\delta_2}{2}\right)|0\rangle + \cos\left(\frac{\delta_2}{2}\right)|1\rangle \\ |\phi_+\rangle &= \sin\left(\frac{\pi}{4} + \frac{\delta_3}{2}\right)|0\rangle + \cos\left(\frac{\pi}{4} + \frac{\delta_3}{2}\right)e^{i(\theta_1+\beta)}|1\rangle \\ |\phi_{+i}\rangle &= \sin\left(\frac{\pi}{4} + \frac{\delta_4}{2}\right)|0\rangle + \cos\left(\frac{\pi}{4} + \frac{\delta_4}{2}\right)e^{i\left(\frac{\pi}{2}+\theta_2+\beta\right)}|1\rangle \end{aligned} \quad (4)$$

$\{\delta_1, \delta_2, \delta_3, \delta_4\}$ represent the error caused by the preparation time bit of the intensity modulator, $\{\theta_1, \theta_2\}$ show the error generated by the phase modulator's modulation relative to the phase, β means the deflection angle of the reference frame. After transmitted to Bob, the m-photon state is performed with POVMs. The gain of source $\gamma \in \{s, d\}$ is calculated as

$$\begin{aligned} Q_{b|(\gamma,m)} &= tr(|m\rangle\langle m|F_{b|\gamma}) \\ &= p_{0|\gamma}a_{b|0} + \sum_{k=1}^{\infty} p_{k|\gamma}a_{b|k}[1 + tr(|m\rangle\langle m|\overrightarrow{n}_{b|k} \cdot \overrightarrow{\sigma})], \end{aligned} \quad (5)$$

where $m \in \{\phi_0, \phi_1, \phi_+, \phi_{+i}\}$, $F_{b|\gamma}$ is the combination of all POVMs on pulses from the source γ: $F_{b|\gamma} = \sum_{k=0}^{+\infty} p_{k|\gamma}F_{b|k}$. For example, if the source is weak coherent state (WCS), it given by $p_{k|\gamma} = \frac{(u_\gamma\eta)^k}{k!}e^{-u_\gamma\eta}$, where η is the overall transmission efficiency and $u_\gamma\eta$ is the mean photon number, with $\eta = t\eta_B$, where t is the channel transmittance and η_B is the detection efficiency of Bob's detector.

In realistic implementations, the number of pulses is always finite, denoted as N. We define $N_\emptyset$, N_d and N_s as the number of elements corresponding to the subset $S_\emptyset$, S_d and S_s individually, then $N = N_\emptyset + N_d + N_s$. The values of $Q_{b|\emptyset}$ and $Q_{b|(\gamma,m)}$ are recorded directly from the experiment, where $Q_{b|\emptyset}$ is the clicking rate with output $b \in \{0,1\}$ for vacuum pulses, and $Q_{b|(\gamma,m)}$ is the clicking rate with output $b \in \{0,1\}$ for state $|m\rangle$ from source γ. However, some parameters in (3) cannot be measured by experiment directly such as $a_{0|1}$, $n^2_{0_y|1}$, $n^2_{0_z|1}$, we need to estimate them with statistical fluctuations.

In the following, we denote the upper bound and the lower bound of the estimated probability quantity χ as

$$\begin{aligned} \chi^U &= \min\{p_{k|\gamma} + \Delta(N_\gamma, 2), 1\}, \\ \chi^L &= \max\{p_{k|\gamma} - \Delta(N_\gamma, 2), 0\}, \end{aligned} \tag{6}$$

except with a failure probability ε. N_γ is the number of pulses with the intensity γ ($\gamma \in \{s, d\}$), $\Delta(p, q)$ is the error function, given by *Lemma 1* [30] as follows.

Lemma 1: If the statistics λ^p are obtained by measuring p samples of observation ς according to a POVM with q outcomes, then for any $\varepsilon > 0$, ς is contained in the set

$$\begin{aligned} \Gamma_\Delta &= \left\{ \varsigma : |\lambda^p(\varsigma) - \lambda^\infty(\varsigma)| \le \Delta(p,q) \right. \\ &\quad \left. = \sqrt{\frac{\ln(1/\varepsilon) + q\ln(p+1)}{2p}} \right\}, \end{aligned} \tag{7}$$

except with a failure probability ε at most, where $\lambda^\infty(\varsigma)$ denotes the probability distribution defined by the POVM applied to ς. The deviation $\Delta(p, q)$ is introduced to evaluate the fluctuation between the frequency λ^p and the probability λ^∞. And λ^p is contained on the interval $[\lambda^\infty - \Delta(p,q), \lambda^\infty + \Delta(p,q)]$ with a successful probability $1 - \varepsilon$ at least.

If the pulse is sent from the vacuum source, no matter what the encoded information and the measurement operation are, the rate of output b is the background counting rate d_B, thus $Q_{b|\emptyset} = a_{b|0} = d_B$. Based on the parameters with known statistical fluctuations, we obtain the lower bound for $a_{0|1}$, as

$$a^L_{0|1} = \frac{1}{2c_1}\left(p^U_{2|d}Q_{0|(s,\phi_+)} - p^L_{2|s}Q_{0|(d,\phi_+)} - c_0 a^U_{0|0} - 2c_2\right) \tag{8}$$

where $a^U_{0|0} = \min\{Q_{0|\emptyset} + \Delta(N_\emptyset, 2), 1\}$, $c_0 = p^U_{2|d}p^U_{0|s} - p^L_{2|s}p^L_{0|d}$, $c_1 = p^U_{2|d}p^U_{1|s} - p^L_{2|s}p^L_{1|d}$, $c_2 = \sum_{k=2}^{l}(p^U_{2|d}p^U_{k|s} - p^L_{2|s}p^L_{k|d}) + p^U_{2|d}(1 - \sum_{k=0}^{l} p^L_{k|s})$, and l is the largest number of k satisfying $\chi^L_{k|d} > 0$. And then $(n^2_{0_z|1})^L$ and $(n^2_{0_y|1})^L$ are obtained as

$$\begin{aligned} (n^2_{0_z|1})^L = \min\Bigg\{ & \left[\frac{Q^L_{0|(d,\phi_0)} - \left(1 - p^L_{0|d} - p^L_{1|d}\right) - p^U_{0|d}a^U_{0|0}}{p^U_{1|d}a^U_{0|1}} - 1\right]^2, \\ & \left[\frac{1 - p^L_{0|d} - p^L_{1|d} + p^U_{0|d}a^U_{0|0} - Q^L_{0|(d,\phi_1)}}{p^U_{1|d}a^U_{0|1}} + 1\right]^2, \\ & \left[\frac{p^L_{0|d}a^L_{0|0} - Q^U_{0|(d,\phi_1)}}{p^L_{1|d}a^L_{0|1}} + 1\right]^2, \left[\frac{Q^U_{0|(d,\phi_0)} - p^L_{0|d}a^L_{0|0}}{p^L_{1|d}a^L_{0|1}} - 1\right]^2, 1\Bigg\}, \end{aligned}$$

$$\begin{aligned} (n^2_{0_y|1})^L = \min\Bigg\{ & \left[\frac{Q^U_{0|(d,\phi_{+i})} - \left(1 - p^L_{0|d} - p^L_{1|d}\right) - p^U_{0|d}a^U_{0|0}}{p^L_{1|d}a^U_{0|1}} - 1\right]^2, \\ & \left(\frac{Q^U_{0|(d,\phi_{+i})} - p^L_{0|d}a^L_{0|0}}{p^L_{1|d}a^L_{0|1}} - 1\right)^2, 1 - \left(n^2_{0_z|1}\right)^L \Bigg\} \end{aligned} \tag{9}$$

Considering the statistical fluctuation of the parameters and the concavity of the min-entropy $H_{\min}$ in (3), the lower bound of the randomness extraction rate is

$$R^L = 2p^L_{1|s}a^L_{0|1}\frac{N_s}{N}H_{\min}\left(\frac{1 + \sqrt{1 - (n^2_{0_y|1})^L - (n^2_{0_z|1})^L}}{2}\right), \tag{10}$$

where $L(U)$ denotes the lower (upper) bound. When $a_{0|1}$, $n^2_{0_y|1}$, $n^2_{0_z|1}$ are estimated, R^L is obtained, and the tightness of $a_{0|1}$, $n^2_{0_y|1}$, $n^2_{0_z|1}$ determines the generation rate of random bits.

III. Numerical Simulations and Analysis

We display the performance of our MDI-QRNG scheme under the condition of using inefficient and noisy threshold detectors. In the simulations, we choose reasonable values of system parameters [21], [24], [30], [31]: detection efficiency and background counting rate of Bob's detector are $\eta_B = 14.5\%$ and $d_B = 10^{-6}$, and the failure probability of statistical fluctuation is set as $\varepsilon = 10^{-5}$. Besides, to simplify the calculation, we assume the same value of state preparation error for four states, i.e. $\delta_1 = \delta_2 = \delta_3 = \delta_4 = \delta$, and fix the intensity of the decoy source as $u_d = 0.2$, then optimize all parameters to maximize the ultimate randomness extraction rate for a given number N and transmission loss. Simulation results are shown in Figs. 2–5.

To show the influence of state preparation error on performance of MDI-QRNG, we plot the randomness extraction rate with different preparation errors ($\delta = 0, \pi/16, \pi/8, \pi/4$) in the asymptotic case and finite-size case ($N = 10^{12}$). It shows consistency between the asymptotic case and the finite-size cases that the randomness extraction rate will get worse when the preparation error gets larger. As is shown in Fig. 2, where different state-preparation errors are considered, the asymptotic case is characterized by a higher randomness extraction rate and a greater loss-tolerant ability than the finite-size case. This feature becomes particularly evident when the state preparation error reaches $\pi/4$. Besides we investigate the influence of the finite-size effect under different preparation errors in Fig. 3, showing the randomness extraction rate of MDI-QRNG versus the number of total pulses at 10 dB loss. First, with the increase of the error, the rate is decreasing faster under the same number of pulses; Second, the rate is more sensitive to the finite size effect

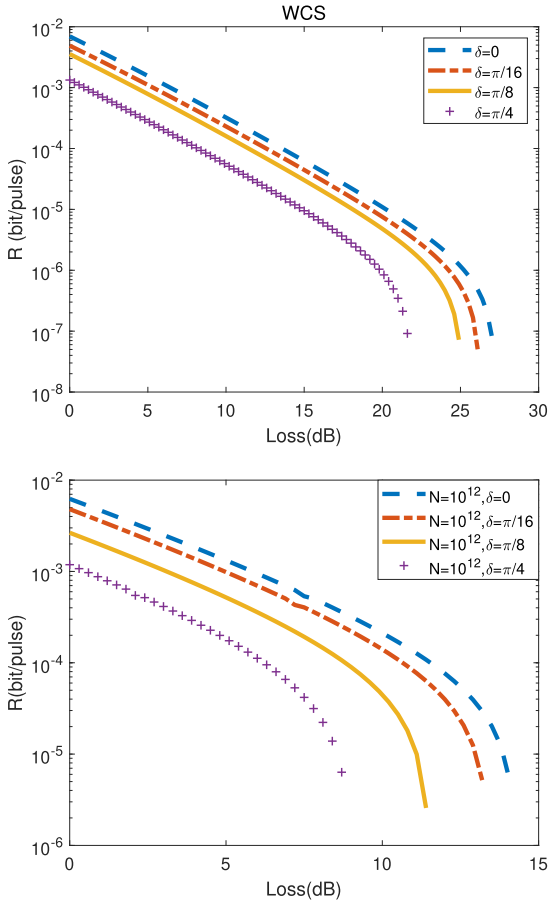

Fig. 2. Comparisons of randomness extraction rates versus loss of MDI-QRNG with different preparation errors in asymptotic case and finite-size case ($N = 10^{12}$).

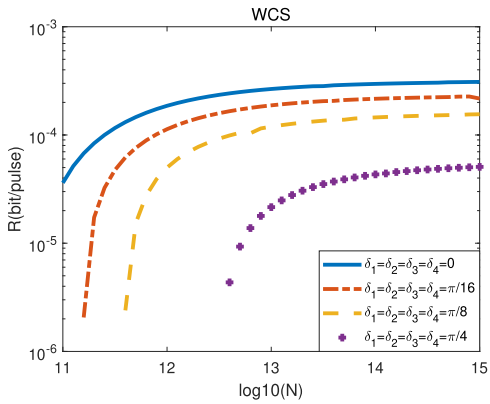

Fig. 3. Influence of finite size on randomness extraction rate with different state preparation errors when the loss is 10 dB.

when with less number of pulses. Fig. 3 shows how finite-size effects affect the randomness extraction rate. In particular it shows that, given a certain state-preparation error, we should choose the appropriate number of pulses to meet the demand of random extraction rate experiment. For example, we must generate the number of pulses over $N = 10^{12}$ in order to achieve a high extraction rate.

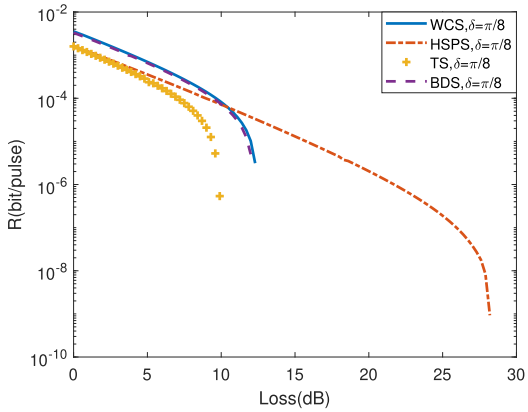

Fig. 4. Randomness extraction rates of MDI-QRNG with HSPS, WCS [30], TS and BDS [33] when the state preparation error $\delta = \pi/8$ and the number of pulses is $N = 10^{12}$.

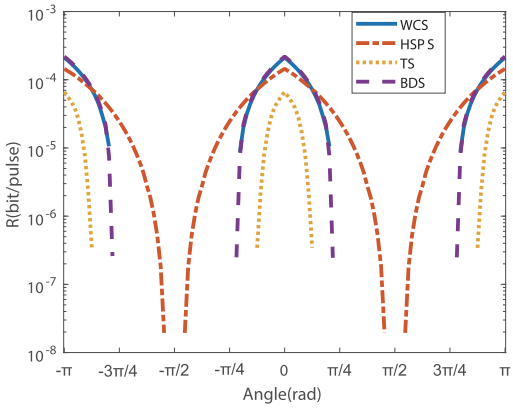

Fig. 5. Randomness extraction rates of MDI-QRNG with HSPS, WCS [30], TS and BDS [33] versus different state preparation errors when the loss is 10 dB and the number of pulses is $N = 10^{12}$.

We further extend MDI-QRNG with WCS to other light sources, i.e. heralded single-photon sources (HSPS), thermal sources (TS), binomial distribution sources (BDS), and make comparisons among them on tolerant ability of the channel loss and the preparation error. Next, we introduce their photon-number distribution (PND). The HSPS is characterized as [32]

$$p_{k|\gamma}^{(H)} = [1-(1-d_A)(1-\eta_A)^k]\frac{(u_\gamma\eta)^k}{k!}e^{-u_\gamma\eta}, \tag{11}$$

where d_A and η_A represent the background counting rate and the detection efficiency of Alice's detectors respectively and are reasonably set with the value as $\eta_A = 60\%$ and $d_A = 10^{-6}$. The PND of TS [33] is characterized as

$$p_{k|\gamma}^{(T)} = \frac{(u_\gamma\eta)^k}{(u_\gamma\eta+1)^{k+1}}. \tag{12}$$

And the PND of BDS is given by [33]

$$p_{k|\gamma,n}^{(B)} = C_n^k \cdot \left(\frac{u_\gamma\eta}{n}\right)^k \cdot \left(1-\frac{u_\gamma\eta}{n}\right)^{n-k}, \tag{13}$$

where C_n^k corresponds to the binomial (n,k), and n is the maximum photon number in BDS. Here we set n = 25 for simulation.

In Fig. 4, we plot the extraction rate versus the channel loss of MDI-QRNGs with four different light sources when $\delta = \pi/8$ and $N = 10^{12}$. From Fig. 4, we can see that the channel loss-tolerant ability of HSPS is superior to the other three sources, which can reach up to 28 dB, much higher than the others. It may be attributed to the low ratio of the vacuum pulse in HSPS, making the parameter estimation more tight. In BDS, the maximum photon number n could be an arbitrary value larger than 1, and an interesting fact is that when $n = 25$, BDS is already close to the poisson distribution.

Fig. 5 shows the extraction rate versus the preparation error of MDI-QRNG with four light sources at 10 dB loss when $N = 10^{12}$. Here, it reveals periodic changes of the randomness extraction rate of MDI-QRNGs, caused by the periodic change of states due to preparation errors. Besides, the HSPS can tolerate the highest state-preparation error, showing its robustness on source flaws. Such a periodic change of the randomness extraction rate is very interesting. When we investige the reason of this phenomenon, we find that as the state preparation error equals to $\pi/2$, the different states mentioned in (4) become the same state, a situation which corresponds to the worst scenario for randomness extraction rates.

IV. Conclusion

In summary, we present a three-intensity decoy-state MDI-QRNG scheme by taken both the source flaw and the finite-size effect into account, and carry out corresponding numerical simulations. Simulation results show that both source preparation errors and statistical fluctuations give significant influences on the performances of MDI-QRNGs. Besides, we make comparisons among MDI-QRNG with different practical light sources, which shows HSPS can tolerate the highest loss and preparation errors. Therefore, the present work can pave the way towards practical implementations of MDI-QRNGs.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable suggestions. The authors declare no conflicts of interest.

References

[1] B. Schneier. *Applied Cryptography*, 2nd ed. New York, NY, USA: Wiley, 1996.
[2] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Rev. Mod. Phys.*, vol. 89, 2017, Art. no. 015004.
[3] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultrahigh-speed random number generation based on a chaotic semiconductor laser," *Phys. Rev. Lett.*, vol. 103, 2009, Art. no. 024102.
[4] B. Qi, Y. M. Chi, H. K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," *Opt. Lett.*, vol. 35, pp. 312–314, 2010.
[5] H. Guo, W. Tang, Y. Liu, and W. Wei, "Truly random number generation based on measurement of phase noise of a laser," *Phys. Rev. E.*, vol. 81, 2010, Art. no. 051137.
[6] M. Furst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, "High speed optical quantum random number generation," *Opt. Exp.*, vol. 18, 2010, Art. no. 13029.
[7] Y. Shen, L. A. Tian, and H. X. Zou, "Practical quantum random number generator based on measuring the shot noise of vacuum states," *Phys. Rev. A*, vol. 18, 2010, Art. no. 063814.
[8] C. Gabriel et al., "A generator for unique quantum random numbers based on vacuum states," *Nat. Photon.*, vol. 4, pp. 711–715, 2010.
[9] M. Ren, E. Wu, Y. Liang, Y. Jian, G. A. Wu, and H. P. Zeng, "Quantum random-number generator based on a photon-number-resolving detector," *Phys. Rev. A*, vol. 83, 2011, Art. no. 023820.
[10] M. Wahl, M. Leifgen, M. Berlin, T. Rohlicke, H. J. Rahn, and O. Benson, "An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements," *Appl. Phys. Lett.*, vol. 98, 2011, Art. no. 171105.
[11] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," *Rev. Sci. Instrum.*, vol. 71, no. 4, pp. 1675–1680, 2000.
[12] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, "Optical quantum random number generator," *J. Mod. Opt.*, vol. 47, pp. 595–598, 2000.
[13] K. Yoshimura et al., "Secure key distribution using correlated randomness in lasers driven by common random light," *Phys. Rev. Lett.*, vol. 108, 2012, Art. no. 070602.
[14] H. Gao et al., "0.75 Gbit/s high-speed classical key distribution with mode-shift keying chaos synchronization of Fabry–Perot lasers," *Light. Sci. Appl.*, vol. 10, 2021, Art. no. 172.
[15] S. Wehner, "Tsirelson bounds for generalized clauser-horne-shimony-holt inequalities," *Phys. Rev. A*, vol. 73, 2006, Art. no. 022110.
[16] H. W. Li et al., "Semi-device-independent random-number expansion without entanglement," *Phys. Rev. A*, vol. 84, 2011, Art. no. 034301.
[17] J. Bowles, M. T. Quintino, and N. Brunner, "Certifying the dimension of classical and quantum systems in a prepare-and-measure scenario with independent devices," *Phys. Rev. Lett.*, vol. 112, 2014, Art. no. 140407.
[18] Z. Cao, H. Zhou, X. Yuan, and X. Ma, "Source-independent quantum random number generation," *Phys. Rev. X.*, vol. 6, 2016, Art. no. 011020.
[19] X. Lin et al., "Certified randomness from untrusted sources and uncharacterized measurements," *Phys. Rev. Lett.*, vol. 129, 2022, Art. no. 050506.
[20] W. B. Liu et al., "Source-independent quantum random number generator against detector blinding attacks," 2022, *arXiv:2204.12156*.
[21] Z. Cao, H. Y. Zhou, and X. F. Ma, "Loss-tolerant measurement-device-independent quantum random number generation," *New J. Phys.*, vol. 17, 2015, Art. no. 125011.
[22] J. Wang et al., "Experimental study of four-state reference-frame-independent quantum key distribution with source flaws," *Phys. Rev. A*, vol. 99, no. 3, 2019, Art. no. 032309.
[23] H.-J. Ding, X. Ma, J.-Y. Liu, C.-H. Zhang, X.-Y. Zhou, and Q. Wang, "Boosting the performance of loss-tolerant measurement-device-independent quantum key distribution," *Opt. Lett.*, vol. 48, pp. 2797–2800, 2023.
[24] Y. Q. Nie et al., "Experimental measurement-device-independent quantum random-number generation," *Phys. Rev. A*, vol. 94, 2016, Art. no. 060301.
[25] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-machanical description of physical reality be considered complete?," *Phys. Rev.*, vol. 47, 1935, Art. no. 777.
[26] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, "Bell nonlocality," *Rev. Mod. Phys.*, vol. 86, 2014, Art. no. 419.
[27] C. Jiang et al., "Measurement-device-independent quantum key distribution protocol with phase post-selection," *Photon. Res.*, vol. 10, 2022, Art. no. 1703.
[28] G. J. Fan-Yuan et al., "Measurement-device-independent quantum key distribution for nonstandalone networks," *Photon. Res.*, vol. 9, pp. 1881–1891, 2021.
[29] H. K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, 2012, Art. no. 130503.
[30] T. Song, X. Tan, and J. Weng, "Statistical fluctuation analysis of measurement-device-independent quantum random-number generation," *Phys. Rev. A*, vol. 99, 2019, Art. no. 022333.
[31] C. H. Zhang, C. M. Zhang, and Q. Wang, "Efficient passive measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 99, 2019, Art. no. 052325.
[32] X. Y. Zhou, C. H. Zhang, C. M. Zhang, and Q. Wang, "Obtaining better performance in the measurement-device-independent quantum key distribution with heralded single-photon sources," *Phys. Rev. A*, vol. 96, 2017, Art. no. 052337.
[33] G. Foletto, F. Picciariello, C. Agnesi, P. Villoresi, and G. Vallone, "Security bounds for decoy-state quantum key distribution with arbitrary photon-number statistics," *Phys. Rev. A*, vol. 105, no. 1, 2022, Art. no. 012603.