ARTICLE OPEN

Security analysis and improvement of source independent quantum random number generators with imperfect devices

Xing Lin^{1,2,3}, Shuang Wang^{1,2,3}✉, Zhen-Qiang Yin^{1,2,3}, Guan-Jie Fan-Yuan^{1,2,3}, Rong Wang^{1,2,3}, Wei Chen^{1,2,3}, De-Yong He^{1,2,3}, Zheng Zhou^{1,2,3}, Guang-Can Guo^{1,2,3} and Zheng-Fu Han^{1,2,3}

A quantum random number generator (QRNG) as a genuine source of randomness is essential in many applications, such as number simulation and cryptography. Recently, a source-independent quantum random number generator (SI-QRNG), which can generate secure random numbers with untrusted sources, has been realized. However, the measurement loopholes of the trusted but imperfect devices used in SI-QRNGs have not yet been fully explored, which will cause security problems, especially in high-speed systems. Here, we point out and evaluate the security loopholes of practical imperfect measurement devices in SI-QRNGs. We also provide corresponding countermeasures to prevent these information leakages by recalculating the conditional minimum entropy and adding a monitor. Furthermore, by taking into account the finite-size effect, we show that the influence of the afterpulse can exceed that of the finite-size effect with the large number of sampled rounds. Our protocol is simple and effective, and it promotes the security of SI-QRNG in practice as well as the compatibility with high-speed measurement devices, thus paving the way for constructing ultrafast and security-certified commercial SI-QRNG systems.

npj Quantum Information (2020)6:100; <https://doi.org/10.1038/s41534-020-00331-9>

INTRODUCTION

Random numbers have become a core element in many fields, ranging from daily applications, such as lotteries, to scientific simulation and cryptography. Pseudo or classical random number generators, relying on deterministic algorithms or physical processes, have been widely used. However, their predictability and strong long-range correlation mean that they are not suitable for applications that need high security, such as cryptography.

In contrast, quantum random number generators (QRNGs) are considered the best solution for generating unpredictable random numbers by exploiting the intrinsic uncertainty of quantum mechanics¹. Many QRNG protocols have been presented recently; they are based on different sources, such as the spatial^{2–6} and temporal^{7–10} modes of photons, vacuum-state fluctuations^{11–15}, laser phase noise^{16–19}, stimulated scattering^{20,21}, and other quantum phenomena^{22–26}. Most of them rely on fully trusted devices, however, realistic devices are usually imperfect or even untrusted, and they might provide side information to eavesdroppers and cause overestimation of the conditional min-entropy.

Device-independent QRNGs (DI-QRNGs), which are based on the violation of the Bell inequality, have been proposed to solve this problem, but their extremely low bit rates and low loss tolerance limit their development^{27–29}. To date, the rate of the fastest DI-QRNG has been reported to be 181 bps³⁰, which is very low for practical applications. To increase both the bit rate and security, source independent QRNGs (SI-QRNGs), as a compromise solution, have been proposed^{31–36}. By a proper conditional min-entropy estimation, SI-QRNGs can generate high-speed secure random numbers with the untrusted source.

In general, measurement devices in SI-QRNGs are trusted and cannot be controlled by attackers. However, practical measurement

devices are not perfect. It is reasonable to suppose that there is no classical or quantum relevance between measurement devices and attackers, but we do not prevent attackers from obtaining the essential parameters of detectors that can reveal the detector imperfections. These imperfections, such as the afterpulse, provide side information to attackers and thus impact the security of SI-QRNGs.

In this work, we build a model of practical imperfect measurement devices and evaluate the influences of these imperfections on the discrete-variable SI-QRNG. We also propose a protocol to eliminate these influences and then estimate the conditional min-entropy and the rate of this SI-QRNG. In the framework of the discrete variable SI-QRNGs, single photon avalanche detectors (SPDs) are the core detection components and the imperfect factors of practical SPDs, such as the afterpulse, detector efficiency, and sensitivity to photon number distribution, will cause the conditional min-entropy to be estimated incorrectly. Here, we present an effective method to estimate the conditional min-entropy focusing on the afterpulse. Additionally, we analyse the influences of detector efficiency mismatch and photon number distribution in entropy estimation and then consider a scheme to remove them. Finally, by using the random sampling method³¹ as the previous protocol³¹ and entropy inequality method³⁷, we analyze the secure randomness rates with the finite key effect and compare the influences of different factors.

This paper is organized as follows. First, we describe how random numbers can be generated by a typical SI-QRNG. Then, we show the effects of different parameters and present a model to account for these effects. In addition, we analyse a numerical simulation of the finite size effect. Finally, we conclude with a discussion.

¹CAS Key Laboratory of Quantum Information, University of Science and Technology of China, 230026 Hefei, Anhui, China. ²CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, 230026 Hefei, Anhui, China. ³State Key Laboratory of Cryptology, P. O. Box 5159, 100878 Beijing, P. R. China. ✉email: wshuang@ustc.edu.cn

RESULTS

A typical SI-QRNG

In a discrete-variable SI-QRNG scenario, as shown in Fig. 1, the source is an untrusted party that might be controlled by an attacker, Eve, and Alice has trusted measurement devices such as threshold detectors (SPDs), a polarizing beam splitter (PBS) and a filter as well as the trusted randomness encoding device. By estimating the conditional min-entropy based on the error rate of the X-basis measurement, randomness extraction can then extract uniform random numbers from the original data³¹. The detailed process is as follows.

First, the untrusted source which might be controlled by Eve emits N pulses with quantum state ρ . From the perspective of Alice, the emitted photons should be in the qubit state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$.

After proper filtering and attenuation, Alice randomly chooses n_x pulses and measures them in the X basis to estimate error. The remaining $n_z = N - n_x$ pulses will be used to generate raw random numbers in the Z basis measurement.

Note that it is a key assumption that the measurement devices are compatible with the squashing model³⁸. In an ideal scheme, a pulse with multiphotons will be *squashed* into a qubit; therefore, the unknown arbitrary-dimensional signal state emitted from the source will become the qubit or vacuum state. Then, n'_x qubits in the X basis and n'_z qubits in the Z basis will be detected with post-selection of the vacua. In practice, the threshold detectors are considered equivalents of the squashing operation in this protocol; therefore we can use the squashing model directly in the analysis. However, the threshold detectors are usually placed at the end of the system, and a double click might not be avoided. Therefore, in the postprocess, it is necessary to randomly assign the outcome to 0 or 1 for double-click events to satisfy the needs of the squashing model³⁹.

According to the error rate e_{bx} , which represents the ratio of detecting $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ in the X basis, and the complementary uncertainty relation, as well as that in the quantum key distribution (QKD)⁴⁰, we can obtain the extractable random numbers from the raw data: $K = n'_z[1 - h(e_{bx} + \theta)] - t_e$, where θ is the deviation due to statistical fluctuations, 2^{-t_e} is the failure probability of the randomness extraction and $h(x)$ represents the binary Shannon entropy function of x .

Finally, uniform random numbers can be obtained from the raw data by a randomness extractor. A random seed with a length of n_{seed} and n_{post} will be consumed in the basis choice and the postprocess, respectively.

Fig. 1 A schematic diagram of a SI-QRNG. Eve controls the laser diode (LD) and sends pulses with states that are changed to mixed states through a filter and a phase randomizer (PR). Through a photon distribution monitor (PDM) which consists of a beam splitter (BS), an attenuator (ATT), a photodiode (PD) and a variable optical attenuator (VOA), the pulses are sent to an optical switch (OS) to choose the measurement basis—the X basis measurement (XBM) or Z basis measurement (ZBM)—both of which consist of a polarization beam splitter (PBS) and two single photon detectors (SPD). The PDM block is used for the distribution monitor and does not exist in general SI-QRNGs in the ref.³¹.

Model

In the previous SI-QRNG scheme, the untrusted source was the focus of the QRNG, and previous work has tried to eliminate Eve's influence on the source. However, in real implementation, the ignored imperfections of measurement devices, such as the afterpulse, detection efficiency mismatch, and sensitivity to the photon number distribution, also have a strong impact on security. In what follows, we first build the underlying response probability model with these factors and recalculate the entropy to reveal these factors' influence mechanism on SI-QRNGs. Then we propose a scheme to solve these problems.

For threshold detectors, SPDs, the usual model of the response probabilities without the afterpulse effect p_a^d can be written as⁴¹

$$p_a^d = 1 - \tau_a(1 - e_{da}) \quad a \in \{0, 1, +, -\}, \quad (1)$$

where τ_a is the zero photon distribution probability after the influence of the loss and detector efficiency and e_{da} is the background counting rate. The subscript a indicates the different detectors which include D_0 and D_1 in the Z basis and D_+ and D_- in the X basis.

One of the most important factors of SPDs is the afterpulse, which has considerable effects on high-speed systems and will be blinding existing analytical models from reality. Therefore, it is necessary to build an afterpulse-compatible model. To adapt the model with the afterpulse, we should change the response probabilities p_a^d to

$$p_a = 1 - \tau_a(1 - e_{da})(1 - P_{\text{apa}}), \quad (2)$$

where P_{apa} is the practical current afterpulse probability of each detector which is given by⁴²

$$P_{\text{apa}} = \frac{\hat{p}_a}{1 - \hat{p}_a} p_{ba}^d, \quad (3)$$

where $\hat{p}_a = \sum_{j=1}^n \hat{p}_{ja}$ is the overall first-order afterpulse rate, and $\hat{p}_{ja}$ is the first-order afterpulse coefficient contributed by the former j th detection window avalanche. p_{ba}^d represents the former response ratio without the afterpulse. It should be noted that we only consider infinite former responses here and the finite responses influence will be discussed later.

Furthermore, to achieve compatibility between our model and the squashing model, it is necessary to precisely depict the probabilities of single-click and double-click events. Moreover, we define the error counts as the events in which only D_- responds, and according to the squashing model, a double click event should be assigned a random bit, which will add a half error count in the X basis. Therefore, according to Eq. (2), the probabilities of single-click and double-click events Q_{single} , Q_{double} in the Z basis and the error rate EQ in the X basis are given by

$$Q_{\text{single}} = p_0(1 - p_1) + p_1(1 - p_0), \quad (4)$$

$$Q_{\text{double}} = p_0 p_1, \quad (5)$$

$$EQ = p_-(1 - p_+) + \frac{1}{2} p_- p_+. \quad (6)$$

Afterpulse

The afterpulse is a key factor in SPD, especially in high-speed systems. In a discrete variable QRNG system, as the afterpulse probability becomes very high with the increase in the system speed, it has a significant impact on not only the random number generation rate but also on the security, which has been ignored in previous works.

Here, we first consider the afterpulse influence mechanism on raw random numbers generated on the Z basis. Intuitively, for a dual detector system, we can infer that the afterpulse will increase the response probability of the detector and increase the

production probability of “00” or “11”. This means that the raw sequence will come to have more positive correlations, which will lead to the overestimation of the entropy and thus an information leak to Eve in the previous models. In what follows, we quantitatively analyse the influence of afterpulse on random number sequences.

In statistical analysis, we always use the autocorrelation coefficient a_i to describe the i th autocorrelation of a n -bit sequence $\{x_i\}$ ⁴³:

$$a_i = \frac{\sum_{j=1}^{n-i} (x_j - \bar{x})(x_{j+i} - \bar{x})}{\sum_{j=1}^n (x_j - \bar{x})^2}, \quad (7)$$

where $\bar{x}$ is the expectation value of $\{x_i\}$. In general, if the sequence is a series of random numbers with good statistical characteristics, the theoretical expectation of a_i should be 0.

With the model presented in the previous sections, we can derive the *prior* autocorrelation coefficient with afterpulse a_i^p :

$$a_i^p = [p_1^{i1}(1 - p_0^{i0}) - p_1^{i0}(1 - p_0^{i1})](1 - k) + [p_0^{i0}(1 - p_1^{i1}) - p_0^{i1}(1 - p_1^{i0})](-k), \quad (8)$$

where p_a^{i1} is the response probability of D_a with the former i th detection response and p_a^{i0} is that without the former i th detection response. k is the expectation of this raw sequence, which is given by

$$k = \frac{p_1(1 - p_0)}{p_1(1 - p_0) + p_0(1 - p_1)}. \quad (9)$$

Note that we assign double-click events to random bits, so these events should not affect the autocorrelation coefficient in the statistical analysis. Therefore, here we only consider the random numbers generated by single-click events.

In the “Methods” section, we will show the detail of the a_i^p calculation and it is proven that the relation between a_i^p and $\hat{p}_{ia}$ is quadratic and degenerates to linear when all the parameters of the two detectors are the same. As shown in Fig. 2, with the increase of $\hat{p}_{ia}$, a_i^p increases rapidly and has an obviously positive correlation.

To solve this security issue, it is necessary to analyse the entropy adapted to the afterpulse model. Here, we define $H_{\min}(A|E)$ as the total conditional minimum entropy of the raw random numbers. It needs to be emphasized that the use of minimum entropy is necessary because Eve is allowed to obtain the probability distribution $\{P_i\}$ of the raw sequence, and there is an optimum strategy for Eve that she can use to guess the maximum probability event and obtain more information than under the

Fig. 2 The relation function between a_i^p and $\hat{p}_{ia}$. The same values are given to the parameters of the detectors. We assume that pulses with coherent states that contain the mean photon number $\nu = 1$ insert SPDs with detection efficiency $\eta_\alpha = 0.1$, $e_{da} = 6 \times 10^{-7}$ and $p_a = 0.05$. For ideal devices, the prior autocorrelation coefficient should be 0.

limitation of conditional entropy. Therefore, we should estimate this worst-case and calculate the minimum randomness event with the afterpulse.

We first consider only the model of raw randomness generation in the Z basis and calculate the conditional minimum entropy $H_{\min}(Z|E)$ with the afterpulse under this condition. According to the response probability model with the afterpulse in Eqs. (2) and (3), the afterpulse probability $P_{\text{ap}\alpha}$ is dependent on the former response ratio p_{ba}^d . Let us consider the maximum leakage information condition, in which the contribution of $P_{\text{ap}\alpha}$ to the two detectors reaches its maximum difference. If D_0 always responds before, which is opposite to the behavior of D_1 , the afterpulse contributions to the two detectors will become the most unbalanced. Understandably, the final distribution $P(i)$ will deviate far from Alice's estimation and Eve will obtain the maximum amount of leaked information. Under this condition, the response probabilities p_0 and p_1 will become:

$$\begin{aligned} p_0^{(1)} &= 1 - \tau_0(1 - e_{d0})(1 - \frac{p_0}{1 - p_0}), \\ p_1^{(0)} &= 1 - \tau_1(1 - e_{d1}). \end{aligned} \quad (10)$$

Assuming that the input state is $|+\rangle$, we can obtain the conditional minimum entropy $H_{\min}(Z|E)$ (without the consideration of double clicks)

$$\begin{aligned} H_{\min}(Z|E) &= -\log_2(\max_i P_i), \\ &= -\log_2 \left\{ \max \left[\frac{p_0^{(1)}(1 - p_1^{(0)})}{Q_{01}}, \frac{p_1^{(0)}(1 - p_0^{(1)})}{Q_{01}} \right] \right\}, \\ Q_{01} &= p_0^{(1)}(1 - p_1^{(0)}) + p_1^{(0)}(1 - p_0^{(1)}). \end{aligned} \quad (11)$$

Without loss of generality, we consider the parameter difference of the two detectors, and $H_{\min}(Z|E)$ will become:

$$\begin{aligned} H_{\min}(Z|E) &= -\log_2 \left\{ \max_{\{a,b\}, \{m,n\}=\{1,0\}} \left[\frac{p_a^{(m)}(1 - p_b^{(n)})}{Q_{ab}^{mn}} \right] \right\}, \\ Q_{ab}^{mn} &= p_a^{(m)}(1 - p_b^{(n)}) + p_b^{(n)}(1 - p_a^{(m)}), \\ p_a^{(1)} &= 1 - \tau_a(1 - e_{da})(1 - \frac{p_a}{1 - p_a}), \\ p_a^{(0)} &= 1 - \tau_a(1 - e_{da}). \end{aligned} \quad (12)$$

In what follows, we discuss the total conditional minimum entropy $H_{\min}(A|E)$ in SI-QRNGs. In a typical SI-QRNG, a key idea is that the protocol with randomness generation and randomness extraction can be seen as similar to that with error correction and randomness generation³¹, which borrows a similar technique from the security analysis of the QKD⁴⁰. Corresponding to the original protocol discussed in the previous section, the equivalent virtual protocol can be described as follows: the input states ρ will be corrected to perfect diagonal states $|+\rangle$ by a phase error correction with losses of the $h(e_{bx})$ states and the remaining $1 - h(e_{bx})$ corrected states $|+\rangle$ can be used to generate perfect random numbers in the Z basis. In this sense, when we estimate $H_{\min}(A|E)$, it is reasonable that we first estimate the influence of the error rate e_{bx} in the X basis and correct all the states to $|+\rangle$, and then the problem can be changed to the estimation of the conditional minimum entropy $H_{\min}(Z|E)$ with these input states $|+\rangle$. In the previous section, we obtained the error rate EQ in the X basis with our afterpulse model in Eq. (6). Therefore, the number of corrected states $|+\rangle$ is:

$$n_{\text{corrected}} = n_z(1 - h(EQ)), \quad (13)$$

where n_z is the number of pulses detected in the Z basis.

Note that the double clicks in the Z basis should also be considered. A series of true random numbers will be input to fill in these double-click events, and, of course, these true random numbers will be subtracted from the final bit rate. According to the probabilities of single click and double-click events Q_{single} , and

Q_{double} in the Z basis in Eqs. (4), and (5) and the conditional minimum entropy in the Z basis $H_{\min}(Z|E)$ in Eq. (12), we can obtain $H_{\min}(A|E)$ by:

$$H_{\min}(A|E) = [H_{\min}(Z|E)Q_{\text{single}} + 1 \times Q_{\text{double}}] \times [1 - h(EQ)] - Q_{\text{double}}. \quad (14)$$

In the previous discussion, we considered the afterpulse probability P_{apa} with Eq. (3) under the condition that there are infinite former responses⁴². However, in real implementations, there are finite pulses in front and hence only these corresponding responses' afterpulse contributions should be calculated. Here we consider this condition and recalculate the afterpulse probability P'_{apa} with finite former responses.

Here, we assume that there are m previous detection windows. As in our earlier definition, $\hat{p}_{ja}$ is the first-order afterpulse probability coefficient contributed by the former j th detection. A high-order afterpulse is the superposition of the contributions of each first-order afterpulse. All of these high-order afterpulse probabilities contributed by the former k th detection window p_{apa}^k are given by:

$$p_{\text{apa}}^k = \sum_{i=k}^m \prod_i \hat{p}_{ia}. \quad (15)$$

According to the previous analysis, always letting one of the detectors respond before is the best case for Eve. The total afterpulse probability $P'_{\text{apa}}(m)$ in this case changes to

$$P'_{\text{apa}}(m) = \sum_{k=1}^m p_{\text{apa}}^k = \sum_{k=1}^m \sum_{i=k}^m \prod_i \hat{p}_{ia}. \quad (16)$$

Previous works^{44,45} show that the afterpulse probability $\hat{p}_{ja}$ at time t conforms to an "exponential model", where the characteristic decay of the afterpulse probability depends on the depth of the levels in which the charges are trapped. A simplified model for the gating detector can be given by:

$$\hat{p}_{ja} = A_a e^{-m\omega_a}, \quad (17)$$

where ω_a is the ratio between the gating time and the de-trapping lifetime, and A_a is the amplitude factor for the depth level. Therefore, the total afterpulse probability contributed by m previous detection windows can be derived as:

$$P'_{\text{apa}}(m) = A_a e^{-\omega_a} \frac{[(1 + A_a)e^{-\omega_a}]^m - 1}{(1 + A_a)e^{-\omega_a} - 1}, \quad (18)$$

and $\omega_a > \ln(1 + A_a)$ is the convergence condition for $m \rightarrow \infty$. In the "Methods" section, we will show the details of the derivation and the relation to infinite previous pulses.

In Fig. 3, we have shown the relation between the conditional minimum entropy $H_{\min}(A|E)$ and the overall afterpulse rate $\hat{p}_a$ with and without the afterpulse. The two lines of $H_{\min}(A|E)$ with the afterpulse have a significant inverse relationship with $\hat{p}_a$ and decrease nearly 20% when $\hat{p}_a$ increases to 0.1. We can also see that the conditional minimum entropy with previous infinite pulses will decrease more rapidly than that with previous finite pulses. This means that limiting the number of responses in a detection period is an effective way to enhance the conditional minimum entropy, especially under the condition with the high afterpulse probability.

Detection efficiency and the photon distribution

In addition to the afterpulse, the other non-negligible parameter that might affect the conditional minimum entropy is the zero photon distribution probability τ_a in Eq. (2). In the SI-QRNG protocol, τ_a is determined by the detection efficiency, loss, and photon distribution input to the detector. The difference in detection efficiency and loss will cause an imbalance in the final random numbers and have a severe impact on the security of the

Fig. 3 The relation between $H_{\min}(A|E)$ and $\hat{p}_a$ with no afterpulse (Np), previous infinite afterpulse (Ip) and previous finite afterpulse (Fp), which consists of 1000 pulses. The factors $\omega_a = 0.001$ and A_a are related to $\hat{p}_a$. The pulses with coherent states that contain $\nu = 10$ photons insert SPDs with $\eta_a = 0.1$ and $e_d = 6 \times 10^{-7}$. The shadow gap is the side information leaked to Eve due to the afterpulse.

Fig. 4 The relation between $H_{\min}(A|E)$ and $\frac{\eta_1}{\eta_0}$ with different $\hat{p}_a$ (0, 0.05). The pulses with a Poisson distribution that contains $\nu = 10$ photons insert SPDs with $\eta_a = 0.1$ and $e_d = 6 \times 10^{-7}$.

scheme. In Fig. 4, we show that with detection efficiency mismatch, $H_{\min}(A|E)$ falls sharply. Moreover, the photon distribution input to the detector also influences the conditional minimum entropy. In previous works, the photon distribution is usually seen as a Poisson distribution, which is not universal for sources and might result in information leakage as the afterpulse. Here, we analyse how the detection efficiency, loss, and photon distribution affect τ_a and design a scheme to monitor these influences.

In theory, the photon distributions before and after loss satisfy a Bernoulli transformation. The untrusted photon source through a filter, which is used to guarantee the source in single mode, will become a photon number mixed state by a phase randomizer⁴⁶.

$$\rho = \sum_{n=0}^{\infty} P_{\text{untrusted}}(n) |n\rangle \langle n|, \quad (19)$$

and then through the loss transmittance in the system, t_{alla} and the detector's efficiency, η_a , the photon distributions input to the detectors will become⁴⁷

$$D(m) = B[P_{\text{untrusted}}(n), \xi_a] = \sum_{n=m}^{\infty} P_{\text{untrusted}}(n) \binom{n}{m} \xi_a^m (1 - \xi_a)^{n-m}, \quad (20)$$

where $\xi_a = t_{\text{all}}\eta_a$. As a consequence, we can obtain the zero photon distribution probability τ_a by

$$\tau_a = D(0) = \sum_{n=0}^{\infty} P_{\text{untrusted}}(n)(1 - \xi_a)^n. \quad (21)$$

Now, the key question for Alice becomes how to monitor the distribution of the untrusted source $P_{\text{untrusted}}(n)$. With the existence of the afterpulse, it is difficult to obtain the distribution precisely only through the SPDs. Fortunately, this can be done by borrowing a similar technique from the source monitor of the QKD⁴⁸. As shown in Fig. 1, in the photon distribution monitor block, a beam splitter (BS) is used to take out a beam of photons to a photodetector (PD) which is used to monitor the photon distribution of the source. Then the others will go through the BS, and an attenuation with the attenuation coefficient t_0 is placed to guarantee that the distribution after it is the same as that detected in the PD, which satisfies:

$$t_0 = \frac{(1 - \eta_{\text{BS}})}{\eta_{\text{BS}}} \eta_{\text{DET}}, \quad (22)$$

where η_{BS} is the transmittance of the BS and η_{DET} is the detection efficiency of the PD. Through random sampling of the pulses, we can estimate the photon distribution $P_{\text{untrusted}}(n)$, and with Eq. (21), the zero photon distribution probability τ_a after the attenuation rate t_{all} and the detection efficiency η_a can be obtained, which can help us to precisely estimate $H_{\text{min}}(A|E)$ with Eq. (14). And a series of biased random seeds will be consumed in the random sampling of the pulses, which guarantees that the distribution measurements are independent.

Simulation in finite-size regime

In practice, the resources of Alice are limited and the system can run for only finite time. Limited samplings will suffer from statistical fluctuations, which might enable attacks by Eve. Therefore, it is of great importance to estimate the parameters in the finite-size regime for the final random number security. Here, we consider the influence of the finite data size on the error estimation in the X basis as well as the process of photon distribution monitoring. We also consider the composable security and obtain the final random number rate R_f with the total security parameter ζ .

In the error parameter estimation step, Alice can obtain EQ in the X basis according to Eq. (6) and can approximate the phase error rate e_{pz} in the Z basis by EQ . However, due to statistical fluctuations, e_{pz} cannot be estimated accurately and the method of approximating it is crucial. In this section, we use two approaches to bound it: one of the methods is random sampling theory used in the ref.³¹ and the other is entropy inequality.

The upper bound of e_{pz} can be defined by

$$e_{\text{pz}} \leq EQ + \theta, \quad (23)$$

and on the basis of the random sampling analysis in the ref.⁴⁹, θ is the deviation due to statistical fluctuations which is bounded by

$$\epsilon_e = \text{Prob}(e_{\text{pz}} > EQ + \theta) \leq \frac{1}{\sqrt{q_x(1-q_x)EQ(1-EQ)N}} 2^{-n\zeta(\theta)}, \quad (24)$$

where $\zeta(\theta) = h(EQ + \theta - q_x h(EQ)) - (1 - q_x)h(EQ + \theta)$, q_x is the rate of X basis measurement and N is the total number of pulses. With the model presented in the previous sections, the number of final random bits is given by

$$R = n_z [(H_{\text{min}}(Z|E)Q_{\text{single}} + 1 \times Q_{\text{double}}) \times (1 - h(EQ + \theta)) - Q_{\text{double}}] - t_e, \quad (25)$$

where n_z is the number of pulses measurement in Z basis and $\epsilon = 2^{-t_e}$ is the failure probability of the randomness extraction

Table 1. List of the experiment parameters used in numerical simulations.

N	ϵ_{all}	ϵ_d	e_d	η_a	η_{BS}	e_q	v	t_e	q_x
10^{10}	2×2^{-50}	2^{-50}	6×10^{-7}	10%	0.5	0.02	10^6	100	0.02

N is the total number of pulses. e_q is the misalignment-error probability. v is the rate of pulses measured in Z basis.

which satisfies the relation with security parameter $\epsilon_{\text{all}} = \sqrt{(\epsilon_e + 2^{-t_e})(2 - \epsilon_e - 2^{-t_e})}$.

Furthermore, the entropy inequality is an alternative method to bound the final random bit rate through bounding e_{pz} ³⁷ by:

$$\theta = \sqrt{\frac{n_z + n_x}{n_z n_x} \frac{n_x + 1}{n_x} \ln \frac{2}{\epsilon_e}}. \quad (26)$$

Here we set ϵ_e as the total security parameter ϵ_{all} because there is no error correction, which is different from the QKD. The final random bit rate can be bounded by

$$R = n_z [(H_{\text{min}}(Z|E)Q_{\text{single}} + 1 \times Q_{\text{double}}) \times (1 - h(EQ + \theta)) - Q_{\text{double}}] - 2 \log_2 \frac{1}{\epsilon_{\text{all}}}. \quad (27)$$

In what follows, we present and discuss the results of the numerical simulation. We use the experimental parameters listed in Table 1. The relations between the loss of VOA and the randomness generation rates, with different values of $\hat{p}_a$ and different methods, are shown in Fig. 5. Compared with the rate without the afterpulse, the rate with the afterpulse is lower and decreases more obviously; from the loss not exceeding 5 dB, the influence of the afterpulse has become more memorable than that of statistical fluctuation gradually and the afterpulse will result in the lower tolerance for fewer photons as well as more information leakage to Eve. Moreover, the bound of the entropy inequality results in a higher randomness generation rate than random sampling. The rate peak is approximately 1–2 dB, and there is a slight difference with different analysis methods.

Furthermore, there is also statistical fluctuation in the photon distribution monitor. Even if we use an ideal photodetector, the distribution estimation will also fluctuate with limited sampling pulses. Assume that Alice randomly chooses N pulses in the photon distribution monitor, and the vacuum probability value input to SPDs τ'_a can be estimated by Eq. (21). According to Hoeffding's inequality⁵⁰, the confidence interval of the vacuum probability is $\tau_a \in [\tau'_a - \delta_d, \tau'_a + \delta_d]$ with confidence level $\kappa = 1 - \epsilon_d$, where ϵ_d is the distribution estimation failing probability, which is given by $\epsilon_d = 2\exp(-2N\delta_d^2)$. To show the effect of statistical fluctuations in the numerical simulation, we assume that the untrusted source distribution estimation result is a Poissonian distribution. As shown in Fig. 6, the limited random sampling pulses will cause the large gap between the ideal $H_{\text{min}}(A|E)$ and practical $H_{\text{min}}(A|E)$ with finite size effect and it will be shrunken when the length of the random sampling pulses is at least 10^5 .

For a larger system, giving one monolithic security proof is error prone. Therefore, in the past few years, composable security, as a solution to this problem, has been developed in the research of QRNGs^{34,35} as well as QKDs^{37,49,51,52}. Here we also establish composable security and obtain the final random number rate R_f .

In general, the raw random sequence of Alice can be quantum correlated with a quantum state that is held by Eve. Mathematically, this situation is described by the classical quantum state

$$\rho_{\text{AE}} = \sum_i p_i |i\rangle\langle i| \otimes \rho_E^i, \quad (28)$$

where $\{|i\rangle\}$ denotes an orthonormal basis for Alice's system, and the subscript E indicates the system of Eve. It is easy to see that, for any attack, the state resulting from the run of a perfectly secure

Fig. 5 Optimal randomness generation rates as a function of the loss of VOA with different values of $\hat{p}_a$ and error estimation methods including random sampling (RS), entropy inequality (EI) and infinite length (IL). RS, EI, and IL represent the models without the afterpulse and RSp, EIp, and ILp represent the models with the afterpulse $\hat{p}_a = 5\%$. The experimental parameters are listed in Table 1, and we assume that the pulse distribution is the coherent state that contains $\nu = 50$ photons initially. **a** The condition with low loss. **b** The condition with the loss of up to 50 dB.

Fig. 6 Conditional minimum entropy $H_{\min}(A|E)$ as a function of the sampling length with the finite size (FS) and infinite length (IL). FZ and IL represent the rates without the afterpulse, and FZp and ILp represent the rates with the afterpulse $\hat{p}_a = 5\%$. Assume that pulses with coherent states contain $\nu = 10$ photons.

scheme has the form $\rho'_{AE} = \rho_A \otimes \rho_E$ where $\rho_A = \sum_i \frac{1}{|J|} |i\rangle\langle i|$ is the uniform mixture of all possible values of the bit string. As is common in quantum cryptography, a QRNG protocol is ζ -secret if and only if, for any attack, the classical quantum state ρ_{AE} satisfies

$$\frac{1}{2} \|\rho_{AE} - \rho'_{AE}\|_1 \leq \zeta, \quad (29)$$

where $\|\cdot\|_1$ denotes the trace norm. In our protocol, the total failing probability is a combination of two processes, error estimation and photon distribution estimation. As the composable security analysis in the QKD⁴⁹, ζ can be given by

$$\zeta \leq \sqrt{(\epsilon_d + \epsilon_e + 2^{-t_e})(2 - \epsilon_d - \epsilon_e - 2^{-t_e})}, \quad (30)$$

where ϵ_e and ϵ_d are the failure probabilities of the error estimation and photon distribution estimation, respectively. 2^{-t_e} is the failure probability of the randomness extraction. Combining the analysis in Eq. (30), the final random number rate is

$$R_f = \min_{\tau_a \in [\tau_a - \delta_d, \tau_a + \delta_d]} \{n_z [(H_{\min}(Z|E)Q_{\text{single}} + 1 \times Q_{\text{double}}) \times (1 - h(EQ + \theta)) - Q_{\text{double}}]\} - t_e, \quad (31)$$

where θ is the deviation due to statistical fluctuations, which is bounded by Eq. (24).

DISCUSSION

In conclusion, we have pointed out and evaluated the security loopholes of practical imperfect devices in discrete-variable SI-QRNGs. By our analysis, Eve might obtain the imperfection parameters of the measurement and obtain side information to enhance the guessing probability of outcomes. The entropy estimation error can reach 20% without consideration of the large afterpulse, and even higher under the conditions of the large mismatch of the detector efficiency and the misestimation of the photon number distribution. To solve these problems, we provide a new protocol with distribution monitoring and entropy estimation methods to extract the secure randomness bits with these existing factors. By analysing the finite-size effect, we show the final randomness rates and find that under some conditions, the influence of the afterpulse will exceed that of the finite size effect. Finally, we establish a composable security model to guarantee the security of the total protocol. Compared with the general SI-QRNG in³¹, our model is more practical and more compatible with imperfect devices.

Our model also provides a way to achieve high-speed SI-QRNGs. The common discrete variable SI-QRNGs are usually limited by the frequency of SPDs which is approximately 100 Mbps. A faster counting rate is not allowed due to the leaked information of the afterpulse. With our model, however, the afterpulse is also a factor in the randomness rate, which means that we can use SPDs with higher afterpulse rates. In recent research, a SPD, with a rate of up to 500 MHz has been presented, which has an afterpulse rate of nearly 10%⁵³. This is not tolerated in most protocols but with our analysis, a high-speed SI-QRNG can be obtained without any security problem of the afterpulse. Therefore, with the promotion rates of SPDs, the imperfect-device-compatible model will be more suitable for high-speed scenarios, and this may make it potentially easier for a discrete-variable GHz-SI-QRNG to be realized.

METHODS

Calculation of the autocorrelation coefficient

In this section, we will show the details of calculating a_i^p . According to Eq. (7), we have given out the general expression of the autocorrelation coefficient. To obtain the final result, it is important to derive each statistical value of the numerator and denominator.

Here we assume that the n -bits raw random number sequence contains nk bits with the value “0” and $n(1 - k)$ bits with the value “1”. The

expectation and variance can be given by

$$\bar{x} = k, \quad \sum_{j=1}^n (x_j - \bar{x})^2 = nk(1-k)^2 + n(1-k)k^2. \quad (32)$$

Now we consider the value of the numerator $\sum_{j=1}^{n-i} (x_j - \bar{x})(x_{j+i} - \bar{x})$. For the j th resultful detection event, considering that $x_j = 1$ or 0, the afterpulse probability of detector D_a ($a \in \{0, 1\}$) in the $(j+i)$ th resultful detection event will become (where the high-order afterpulse generated by the j th response is disregarded):

$$p_{apa}^{i1} = \frac{\hat{p}_a}{1 - \hat{p}_a} p_{ba}^d + \hat{p}_{ia}(1 - p_{ba}^d), \quad (33)$$

or $p_{apa}^{i0} = \frac{\hat{p}_a}{1 - \hat{p}_a} p_{ba}^d + \hat{p}_{ia}(-p_{ba}^d),$

and the corresponding response probability is

$$p_a^{i1} = 1 - \tau_a(1 - e_{da})(1 - p_{apa}^{i1}), \quad (34)$$

or $p_a^{i0} = 1 - \tau_a(1 - e_{da})(1 - p_{apa}^{i0}).$

Therefore, the prior statistical autocorrelation coefficient can be derived by ($n \gg i$):

$$\begin{aligned} a_i^p &= \frac{\sum_{j=1}^{n-i} (x_j - \bar{x})(x_{j+i} - \bar{x})}{\sum_{j=1}^n (x_j - \bar{x})^2} \\ &= \frac{\sum_{j=1}^i (1 - \bar{x})(x_{j+i} - \bar{x}) + \sum_{j=i+1}^n (0 - \bar{x})(x_{j+i} - \bar{x})}{\sum_{j=1}^n (x_j - \bar{x})^2} \\ &= \frac{1}{nk(1-k)^2 + n(1-k)k^2} \\ &\quad \times \{ (n-i)k(1-k) \\ &\quad \times [(1-k)p_1^{i1}(1-p_0^{i0}) + (0-k)p_0^{i0}(1-p_1^{i1})] \\ &\quad + (n-i)(1-k)(-k) \\ &\quad \times [(1-k)p_1^{i0}(1-p_0^{i1}) + (0-k)p_0^{i1}(1-p_1^{i0})] \} \\ &= [p_1^{i1}(1-p_0^{i0}) - p_1^{i0}(1-p_0^{i1})](1-k) \\ &\quad + [p_0^{i0}(1-p_1^{i1}) - p_0^{i1}(1-p_1^{i0})](-k). \end{aligned} \quad (35)$$

According to Eqs. (33) and (34), the response probabilities p_a^{i1} and p_a^{i0} are both linear about $\hat{p}_{ia}$. Therefore, it is obvious that a_i^p is a quadratic function about $\hat{p}_{ia}$ and when we choose the same parameters for the two detectors, a_i^p will become:

$$\begin{aligned} a_i^p &= [p_0^{i1}(1-p_0^{i0}) - p_0^{i0}(1-p_0^{i1})](1-k) \\ &\quad + [p_0^{i0}(1-p_0^{i1}) - p_0^{i1}(1-p_0^{i0})](-k) \\ &= p_0^{i1} - p_0^{i0} \\ &= \tau_0(1 - e_{d0})p_{b0}^d \hat{p}_{i0}. \end{aligned} \quad (36)$$

and it will degenerate to a linear function about $\hat{p}_{ia}$.

Calculation of the total afterpulse probability for previous finite responses

In this section, we will derive the total afterpulse probability. According to Eqs. (16) and (17), we can obtain the $P'_{apa}(m)$ by:

$$\begin{aligned} P'_{apa}(m) &= \sum_{k=1}^m \sum_{i=k} \prod_i \hat{p}_{ia} \\ &= \sum_{k=1}^m \sum_{i=k} \prod_i A_a e^{-i\omega_a} \\ &= \sum_{k=1}^m \sum_{j=1}^k \binom{k}{j} A_a^j e^{-k\omega_a} \\ &= \sum_{k=1}^m A_a (1 + A_a)^{k-1} e^{-k\omega_a} \\ &= A_a e^{-\omega_a} \frac{[(1 + A_a)e^{-\omega_a}]^m - 1}{(1 + A_a)e^{-\omega_a} - 1}. \end{aligned} \quad (37)$$

To compare the afterpulse probability for previous infinite responses $P_{apa}(\text{all})$, it is necessary to obtain $\hat{p}_a$ by:

$$\begin{aligned} \hat{p}_a &= \sum_{j=1}^m \hat{p}_{ja} = \sum_{j=1}^m A_a e^{-j\omega_a} = A_a e^{\omega_a} \frac{e^{-m\omega_a} - 1}{e^{-\omega_a} - 1} \\ &= \frac{A_a e^{-\omega_a}}{1 - e^{-\omega_a}} \quad (m \rightarrow \infty), \end{aligned} \quad (38)$$

and then according to Eq. (3), we can get $P_{apa}(\text{all})$ by:

$$P_{apa}(\text{all}) = \frac{\hat{p}_a}{1 - \hat{p}_a} = \frac{A_a e^{-\omega_a}}{1 - (1 + A_a)e^{-\omega_a}}. \quad (39)$$

It is obvious that $P'_{apa}(m)$ is a monotonic decreasing function and will degenerate to $P_{apa}(\text{all})$ when $m \rightarrow \infty$, and the condition of convergence for Eq. (37) is $(1 + A_a)e^{-\omega_a} < 1$, that $\omega_a > \ln(1 + A_a)$.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Received: 13 March 2020; Accepted: 31 October 2020;

Published online: 10 December 2020

REFERENCES

- Born, M. Quantenmechanik der stoßvorgänge. *Z. f.ür. Phys.* **38**, 803–827 (1926).
- Stefanov, A., Gisin, N., Guinnard, O., Guinnard, L. & Zbinden, H. Optical quantum random number generator. *J. Mod. Opt.* **47**, 595–598 (2000).
- Jennnewein, T., Achleitner, U., Weihs, G., Weinfurter, H. & Zeilinger, A. A fast and compact quantum random number generator. *Rev. Sci. Instrum.* **71**, 1675–1680 (2000).
- Gräfe, M. et al. On-chip generation of high-order single-photon w-states. *Nat. Photonics* **8**, 791 (2014).
- Oberreiter, L. & Gerhardt, I. Light on a beam splitter: more randomness with single photons. *Laser Photonics Rev.* **10**, 108–115 (2016).
- Wang, P., Long, G. & Li, Y. Scheme for a quantum random number generator. *J. Appl. Phys.* **100**, 056107–056107 (2006).
- Dynes, J. F., Yuan, Z. L., Sharpe, A. W. & Shields, A. J. A high speed, postprocessing free, quantum random number generator. *Appl. Phys. Lett.* **93**, 031109 (2008).
- Wayne, M. A., Jeffrey, E. R., Akselrod, G. M. & Kwiat, I. P. G. Photon arrival time quantum random number generation. *J. Mod. Opt.* **56**, 516–522 (2009).
- Wahl, M. et al. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements. *Appl. Phys. Lett.* **98**, 171105 (2011).
- Nie, Y.-Q. et al. Practical and fast quantum random number generation based on photon arrival time relative to external reference. *Appl. Phys. Lett.* **104**, 051110 (2014).
- Gabriel, C. et al. A generator for unique quantum random numbers based on vacuum states. *Nat. Photonics* **4**, 711 (2010).
- Shen, Y., Tian, L. & Zou, H. Practical quantum random number generator based on measuring the shot noise of vacuum states. *Phys. Rev. A* **81**, 063814 (2010).
- Symul, T., Assad, S. & Lam, P. K. Real time demonstration of high bitrate quantum random number generation with coherent laser light. *Appl. Phys. Lett.* **98**, 231103 (2011).
- Zhu, Y., He, G. & Zeng, G. Unbiased quantum random number generation based on squeezed vacuum state. *Int. J. Quantum Inf.* **10**, 1250012 (2012).
- Zhou, Q., Valivarthi, R., John, C. & Tittel, W. Practical quantum random-number generation based on sampling vacuum fluctuations. *Quantum Eng.* **1**, e8 (2019).
- 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.* **35**, 312–314 (2010).
- Guo, H., Tang, W., Liu, Y. & Wei, W. Truly random number generation based on measurement of phase noise of a laser. *Phys. Rev. E* **81**, 051137 (2010).
- Jofre, M. et al. True random numbers from amplified quantum vacuum. *Opt. Express* **19**, 20665–20672 (2011).
- Zhou, H., Yuan, X. & Ma, X. Randomness generation based on spontaneous emissions of lasers. *Phys. Rev. A* **91**, 062316 (2015).
- Bustard, P. J. et al. Quantum random bit generation using stimulated raman scattering. *Opt. Express* **19**, 25173–25180 (2011).
- England, D. et al. Efficient raman generation in a waveguide: a route to ultrafast quantum random number generation. *Appl. Phys. Lett.* **104**, 051117 (2014).
- Zhou, H., Li, J., Zhang, W. & Long, G.-L. Quantum random-number generator based on tunneling effects in a si diode. *Phys. Rev. Appl.* **11**, 034060 (2019).
- Demir, K. & Ergün, S. Security analysis of a random number generator based on a chaotic hyperjerk system. *EPL* **129**, 30001 (2020).
- Yao, X.-J., Tang, X., Wu, Z.-M. & Xia, G.-Q. Multi-channel physical random number generation based on two orthogonally mutually coupled 1550 nm vertical-cavity surface-emitting lasers. *Acta Phys. Sin.* **67**, 024204 (2018).
- Vallone, G., Marangon, D. G., Tomasin, M. & Villoresi, P. Quantum randomness certified by the uncertainty principle. *Phys. Rev. A* **90**, 052327 (2014).

26. Ma, X., Yuan, X., Cao, Z., Qi, B. & Zhang, Z. Quantum random number generation. *npj Quantum Inf.* **2**, 1–9 (2016).
27. Pironio, S. et al. Random numbers certified by bell's theorem. *Nature* **464**, 1021 (2010).
28. Christensen, B. et al. Detection-loophole-free test of quantum nonlocality, and applications. *Phys. Rev. Lett.* **111**, 130406 (2013).
29. Bierhorst, P. et al. Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature* **556**, 223 (2018).
30. Liu, Y. et al. Device-independent quantum random-number generation. *Nature* **562**, 548 (2018).
31. Cao, Z., Zhou, H., Yuan, X. & Ma, X. Source-independent quantum random number generation. *Phys. Rev. X* **6**, 011020 (2016).
32. Xu, F., Shapiro, J. H. & Wong, F. N. Experimental fast quantum random number generation using high-dimensional entanglement with entropy monitoring. *Optica* **3**, 1266–1269 (2016).
33. Marangon, D. G., Vallone, G. & Villoresi, P. Source-device-independent ultrafast quantum random number generation. *Phys. Rev. Lett.* **118**, 060503 (2017).
34. Avesani, M., Marangon, D. G., Vallone, G. & Villoresi, P. Source-device-independent heterodyne-based quantum random number generator at 17 gbps. *Nat. Commun.* **9**, 5365 (2018).
35. Drahi, D. et al. Certified quantum randomness from untrusted light. <https://arxiv.org/abs/1905.09665> (2019).
36. Zheng, Z. et al. Bias-free source-independent quantum random number generator. *Opt. Express* **28**, 22388–22398 (2020).
37. Tomamichel, M., Lim, C. C. W., Gisin, N. & Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **3**, 634 (2012).
38. Beaudry, N. J., Moroder, T. & Lütkenhaus, N. Squashing models for optical measurements in quantum communication. *Phys. Rev. Lett.* **101**, 093601 (2008).
39. Gittsovich, O. et al. Squashing model for detectors and applications to quantum-key-distribution protocols. *Phys. Rev. A* **89**, 012325 (2014).
40. Shor, P. W. & Preskill, J. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441 (2000).
41. Yu, Z.-W., Zhou, Y.-H. & Wang, X.-B. Reexamination of decoy-state quantum key distribution with biased bases. *Phys. Rev. A* **93**, 032307 (2016).
42. Fan-Yuan, G.-J. et al. Afterpulse analysis for quantum key distribution. *Phys. Rev. Appl.* **10**, 064032 (2018).
43. Knuth, D. E. *The Art of Computer Programming*, vol. 3 (Pearson Education, London, 1997).
44. Cova, S., Lacaite, A. & Ripamonti, G. Trapping phenomena in avalanche photodiodes on nanosecond scale. *IEEE Electron Device Lett.* **12**, 685–687 (1991).
45. Korzh, B., Lunghi, T., Kuzmenko, K., Boso, G. & Zbinden, H. Afterpulsing studies of low-noise ingaas/inp single-photon negative-feedback avalanche diodes. *J. Mod. Opt.* **62**, 1151–1157 (2015).
46. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
47. Lee, C. T. External photodetection of cavity radiation. *Phys. Rev. A* **48**, 2285 (1993).
48. Xu, B., Peng, X. & Guo, H. Passive scheme with a photon-number-resolving detector for monitoring the untrusted source in a plug-and-play quantum-key-distribution system. *Phys. Rev. A* **82**, 042301 (2010).
49. Fung, C.-H. F., Ma, X. & Chau, H. Practical issues in quantum-key-distribution postprocessing. *Phys. Rev. A* **81**, 012318 (2010).
50. Hoeffding, W. Probability inequalities for sums of bounded random variables. *J. Am. Stat. Assoc.* **58**, 13 (1963).
51. Müller-Quade, J. & Renner, R. Composability in quantum cryptography. *N. J. Phys.* **11**, 085006 (2009).
52. Lim, C. C. W., Curty, M., Walenta, N., Xu, F. & Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **89**, 022307 (2014).
53. Comandar, L. C. et al. Gigahertz-gated ingaas/inp single-photon detector with detection efficiency exceeding 55% at 1550 nm. *J. Appl. Phys.* **117**, 083109 (2015).

ACKNOWLEDGEMENTS

We thank Xiongfeng Ma and Xingjian Zhang for helpful discussions. This work was supported by the National Key Research And Development Program of China (Grant No. 2018YFA0306400), the National Natural Science Foundation of China (Grants No. 61622506, No. 61575183, 61627820, No. 61475148, and No. 61675189), and the Anhui Initiative in Quantum Information Technologies.

AUTHOR CONTRIBUTIONS

S.W., Z.-Q.Y., G.-J.F.-Y., R.W., and X.L. conceived the basic idea of the protocol. X.L. finished the details of the protocol and the simulations. S.W. and X.L. wrote the paper. S.W., W.C., D.-Y.H., Z.Z., G.-C.G., and Z.-F.H. supervised the project and all authors participated in discussions.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Correspondence and requests for materials should be addressed to S.W.

Reprints and permission information is available at <http://www.nature.com/reprints>

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

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2020