scientific reports

Check for updates

OPEN

Quantum random number generator using a cloud superconducting quantum computer based on source-independent protocol

Yuanhao Li[1,2], Yangyang Fei[1,2]✉, Weilong Wang[1,2]✉, Xiangdong Meng[1,2], Hong Wang[1,2], Qianheng Duan[1,2] & Zhi Ma[1,2]

Quantum random number generator (QRNG) relies on the intrinsic randomness of quantum mechanics to produce true random numbers which are important in information processing tasks. Due to the presence of the superposition state, a quantum computer can be used as a true random number generator. However, in practice, the implementation of the quantum computer is subject to various noise sources, which affects the randomness of the generated random numbers. To solve this problem, we propose a scheme based on the quantum computer which is motivated by the source-independent QRNG scheme in optics. By using a method to estimate the upper bound of the superposition state preparation error, the scheme can provide certified randomness in the presence of readout errors. To increase the generation rate of random bits, we also provide a parameter optimization method with a finite data size. In addition, we experimentally demonstrate our scheme on the cloud superconducting quantum computers of IBM.

Random number generators play an important role in many fields, such as cryptography[1] and scientific simulations[2]. Different applications require different levels of randomness. For the applications which require the random numbers to be statistically unbiased, pseudo random number generators (PRNGs) or classical random number generators relying on deterministic algorithms or physical processes have been widely used[3,4]. Although their output sequences may appear random and usually have a perfect balance between 0 and 1, the predictability and strong long-range correlation may result in security loopholes when employed in some applications, particularly in cryptography and quantum key distribution[5,6].

To solve this problem, based on the intrinsic uncertainty of quantum mechanics, quantum random number generators (QRNGs) can produce unpredictable random numbers and have attracted great attention in the past few years. Nowadays, many QRNG protocols implemented in optics have been proposed by using different randomness sources, including single photon detection[7–9], vacuum state fluctuation[10–12], laser phase fluctuation[13,14] and amplified spontaneous emission noise[15,16]. There are already some commercial QRNG products implementing these protocols. In general, a QRNG system consists of two parts, a randomness source and a measurement unit. The randomness source emits the superposition state in the measurement basis whose measurement outcome is unpredictable to produce random numbers. For example, for the superposition state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, the results of projection measurements onto the $\{|0\rangle, |1\rangle\}$ basis of the state are purely random and ideally form the random numbers.

On the other hand, quantum computers based on different physical implementations have been rapidly developed[17], including superconducting quantum circuits[18,19], nuclear magnetic resonance[20,21] and optical systems[22]. Some companies have launched cloud quantum computers which enable users to send quantum programs to use quantum computer[23,24]. Furthermore, due to the presence of superposition state, a quantum computer can be considered as an unbiased QRNG to generate random numbers[25]. Generally, a quantum bit (qubit) can be prepared in the superposition state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ by applying the Hadamard gate on

[1]State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, Henan, China. [2]Henan Key Laboratory of Network Cryptography Technology, Zhengzhou 450001, Henan, China. ✉email: fei_yy@foxmail.com; wlwang19888@163.com

the initial state $|0\rangle$. Thus, repeating measurements on the qubit in the $\{|0\rangle, |1\rangle\}$ basis, the numbers 0 and 1 can be obtained with equal probabilities. Compared with the PRNG based on conventional digital computers, the QRNG based on quantum computers does not require random seeds, in which the risk of the predictability of output sequence can be avoided.

However, the imperfections of realistic devices and the presence of hardware noise may leave security loopholes that influence the randomness of generated random numbers in practice. To enhance the security of QRNG, self-testing or device-independent (DI) QRNGs are proposed which do not need to trust the generated quantum state and the measurement devices[26–28]. By observing the violation of the Bell inequality, the randomness of source can be guaranteed and true random numbers can be obtained. Unfortunately, realizing the practical implementation is difficult due to the requirement of a loophole-free Bell test, and the random number generation rate is very low, which cannot satisfy the demands of practical applications. To increase the generation rate and make the protocols more practical, a semi-self-testing or semi-device-independent (SDI) QRNG scheme with trusted part of the physical devices is proposed which presents a trade-off between the generation rate and the security of certified randomness[29–31].

Among SDI-QRNG schemes, source-independent (SI) QRNG has gathered lots of attention[32–34]. With reasonable assumptions that measurement devices are well-calibrated and the source is untrusted, the SI-QRNG can generate secure random numbers and achieve considerable random number generation rates. Most of the SI-QRNG protocols are realized by the quantum optics devices. Utilizing a laser as a randomness source, Zhu *et al.* proposed a SI-QRNG scheme and realized a randomness generation rate of over 5000 bps[34], and Marco *et al.* proposed a continuous-variable version of SI-QRNG protocol and realized a generation rate of 17 Gbps[35].

In addition to the optics based SI-QRNG, the method of SI-QRNG protocol can also be performed on the quantum computer. The existing quantum computers are noisy and vulnerable to various types of errors, which causes errors in the preparation of superposition state $|+\rangle$ and affects the randomness of random numbers. For the conventional QRNG implementations, which output random numbers by directly measuring the quantum superposition state $|+\rangle$, the randomness of the output data cannot be well estimated due to the difficulty to model devices precisely. Although the random numbers generated by quantum computers can pass statistical testing after the combination of the von Neumann[36] and Samuelson extractors[37], the final random number extraction rate cannot be given and the randomness of the random numbers cannot be certified[38].

SI-QRNG protocol does not require accurate characterization of the equipment to estimate the randomness of generated random numbers under the situation that the measurement error is known. Although the measurement error is timely varied, one's own quantum computer can monitor the measurement error on time. The final extraction rate of random numbers can be given by estimating the error in the preparation of superposition state $|+\rangle$. Motivated by the original SI-QRNG protocol[34], we propose a scheme that can guarantee the randomness of random numbers generated by noisy quantum computers. Rather than focusing on the influence of the source controlled by the adversary on the random numbers, we explore how many random bits can be extracted from raw data in the case of imperfect quantum gates. Using the cloud superconducting quantum computer of IBM, we experimentally examine the effectiveness of the proposed protocol based on the SI-QRNG protocol.

The rest of this article is organized as follows. In second section, the protocol based on SI-QRNG using cloud superconducting quantum computer is briefly introduced. In third section, we analyze the protocol, where the final extracted number of random bits is further given in the presence of readout errors, and the estimation method and optimization of the parameter are provided. In fourth section, an experimental demonstration of the scheme is performed with the cloud superconducting quantum computer of IBM. Finally, we conclude this paper in fifth section.

QRNG based on source-independent protocol

In the quantum computer, the initial state of a qubit is generally prepared in $|0\rangle$ and can be represented with state vector as $\begin{bmatrix}1 & 0\end{bmatrix}^T$ (T = Transpose). By applying $RY(\pi/2)$ gate, the superposition state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ can be acquired, in which $RY(\pi/2)$ gate performs $\pi/2$ rotation around Y-axis in the Bloch sphere and can be expressed with $\frac{1}{\sqrt{2}}\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix}$. If the quantum computer is noiseless and the quantum operations are perfect, the measurement results in the computational basis $|0\rangle$ and $|1\rangle$ should be uniformly random based on the mathematical axiom of quantum mechanics. However, the initial state, quantum gate and readout of each qubit may be impacted by hardware noise, which causes the temporal correlation between the output bits[39]. Thus, in the QRNG based on quantum computer, it is important to calculate how many random bits can be extracted from the raw data.

Motivated by the optics based SI-QRNG protocol proposed in Ref.[34], we implement the protocol based on SI-QRNG using the quantum computer, as shown in Fig. 1. The detailed steps of the protocol are as follows:

(1) Source: By applying $RY(\pi/2)$ gate on the initial state $|0\rangle$, a qubit is prepared in superposition state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$.
(2) Random sampling: By utilizing a short random seed, we randomly choose the X basis quantum circuit or Z-basis quantum circuit to measure the quantum superposition state $|+\rangle$. By adding a $RY(\pi/2)$ gate to the circuits, the Z-basis measurement can be converted into X-basis measurement, where $X = \{|0\rangle \pm |1\rangle/\sqrt{2}\}$ and $Z = \{|0\rangle, |1\rangle\}$. In this process, the quantum circuit is executed n times, including n_x times in the X-basis quantum circuit and n_z times in the Z-basis quantum circuit, where $n = n_x + n_z$.
(3) Parameter estimation: The quantum state emitted by the source should be $|+\rangle$ state when the quantum computer system is noiseless. The measurement result of $|+\rangle$ is $|1\rangle$ and the result of $|-\rangle$ is $|0\rangle$ in the X-basis,

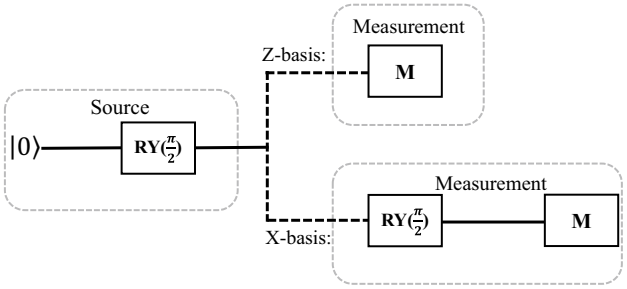


Figure 1. Quantum circuits for the QRNG based on SI protocol. The qubit state is randomly measured in the X-basis or Z-basis.

respectively. Therefore, a result of $|0\rangle$ means an error. We estimate the bit error rate e_{bx} in the X-basis measurement and the statistical deviation is denoted by o, the preparation error of $|+\rangle$ state in the Z-basis e_z can be estimated by

$$e_z \leq e_{bx} + o. \tag{1}$$

o is the deviation due to statistical fluctuations which is bounded by[34]

$$\varepsilon_e = Prob(e_z > e_{bx} + o) \leq \frac{1}{\sqrt{q_x(1-q_x)e_{bx}(1-e_{bx})n}} 2^{-n\zeta(o)}, \tag{2}$$

where $\zeta(o) = H(e_{bx} + o + q_x o) - q_x H(e_{bx}) - (1-q_x)H(e_{bx} + o)$, $q_x = n_x/n$ is the rate of X-basis choice and $H(x) = -xlog_2(x) - (1-x)log_2(1-x)$ represents the Shannon entropy function. If the value of $e_{bx} + o$ exceeds 0.5, we abort the protocol.

(4) Randomness generation: The measurement results of the Z-basis are used to generate random numbers. We perform Z-basis quantum circuit n_z times to generate n_z random bits.

(5) Randomness extraction: To extract true random numbers, the Topelitz-matrix hashing method is used. The number of final random bits is[34]

$$K \geq n_z - n_z H(e_z) - t_e, \tag{3}$$

where 2^{-t_e} is the failure probability of the randomness extraction[40]. In practice, to construct a Toeplitz matrix of size $n_z \times [n_z - n_z H(e_z) - t_e]$ for randomness extraction, the length of $n_z + n_z - n_z H(e_z) - t_e$ random bits is required. According to the leftover hash lemma[41], the final output random bits are not affected by the random bits used in the construction of the Topelitz matrix.

Note that there is also another method to estimate the number of final random bits. Vallone *et al.*[42] performed a complete finite key analysis of the protocol where the conditional min-entropy of the measurement results of Z-basis can be bounded by using the Rényi entropy of order 1/2 of the measurement results of X-basis $H_{1/2}(\{n_x\})$. Thus, by estimating the max-entropy $H_{1/2}(\{n_x\})$, the number of final random bits can be determined. In principle, both the methods in Ref.[34] and[42] can be used to estimate the number of final random bits. We choose the method in Ref.[34] in our protocol.

Analysis

In this section, we analyze the randomness of QRNG based on the quantum computer. Due to the presence of noise in the quantum computer, the readout, initial state and quantum gate are imperfect and thus impact the number of extracted random bits. The number of final random bits K, which is given by Eq. (3), does not consider the effect of readout errors. We first calculate the number of final random bits with different readout errors in "The number of extracted random bits in the presence of readout error" section. Then, to calculate the number of final random bits, a method for estimating the upper bound of e_z, i.e., the error in the preparation of quantum superposition state, is given out in "The estimation of upper bound of e_z" section. Finally, considering the influence of the finite data size on the parameter estimation, the ratio of X-basis measurements is optimized in "Optimization of parameter q_x" section.

The number of extracted random bits in the presence of readout error. In practice, the readout operation of a quantum state is imperfect. Generally, the readout errors of $|0\rangle$ and $|1\rangle$ are different, which leads to the asymmetry in the 1/0 ratio of measurement outcomes. Thus, the influence of readout error on the number of extracted random numbers cannot be ignored. In the SI-QRNG based on optics, the influence of detector imperfection on the generated random numbers is analyzed in detail[43]. Motivated by this method, we analyze the scenario that the readout errors of $|0\rangle$ and $|1\rangle$ are different in the quantum computer and recalculate the number of final extracted random bits.

The readout error of $|0\rangle$, r_0, means the probability to output $|1\rangle$ while the actual state should be $|0\rangle$. Similarly, the readout error of $|1\rangle$, r_1, means the probability to output $|0\rangle$ while the actual state should be $|1\rangle$. When r_0 and r_1 are equal, the numbers of 1 and 0 in the measurement outcomes of superposition state $|+\rangle$ are equal and the randomness of the output bits cannot be affected by the readout error. Thus, the readout process of a qubit can be

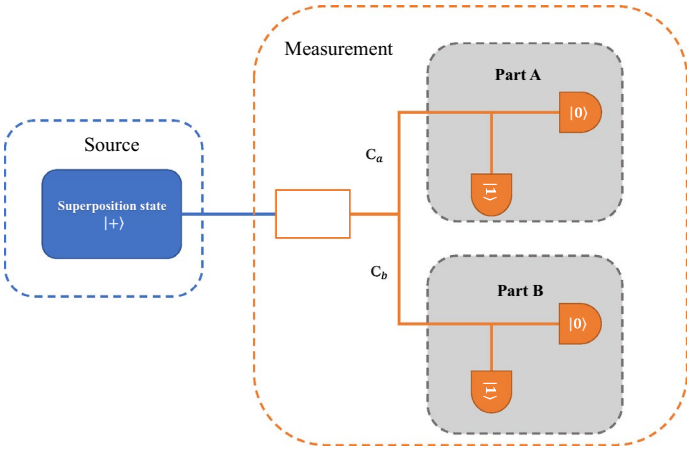


Figure 2. Equivalence of SI-QRNG under the different readout errors of a quantum state. The readout of a quantum state is equivalent to the superposition of two extreme parts: Part A and Part B. The readout errors of $|0\rangle$ and $|1\rangle$ are equal in Part A and are completely different in Part B, where the probabilities of occurrence of Part A and Part B are c_a and c_b, respectively.

equivalent to the superposition of two parts, as shown in Fig. 2. One is the case that the readout errors of $|0\rangle$ and $|1\rangle$ are equal, and the probability of occurrence of Part A is c_a. The other one is the case that the readout errors of $|0\rangle$ and $|1\rangle$ are completely different and the probability of occurrence of Part B is c_b, in which the readout error of one quantum state is 1 and the readout error of another quantum state is 0. Therefore, no genuine randomness can be extracted from Part B. The relationship between c_a and c_b is $c_a + c_b = 1$. Moreover, the readout error should fulfill

$$\begin{cases} r_0 = c_a r_{0,A} + c_b r_{0,B} \\ r_1 = c_a r_{1,A} + c_b r_{1,B}, \end{cases} \tag{4}$$

where $r_{i,j}$ denotes the readout error of quantum state $|i\rangle$ for Part j with $i \in \{0, 1\}$ and $j \in \{A, B\}$. Without loss of generality, we assume that the readout error r_0 is no larger than r_1. Due to the relationships $r_{0,A} = r_{1,A}$, $r_{0,B} = 0$ and $r_{1,B} = 1$, Eq. (4) can be simplified as

$$\begin{cases} r_0 = c_a r_{0,A} \\ r_1 = c_a r_{1,A} + c_b. \end{cases} \tag{5}$$

Furthermore, we can obtain that $c_b = r_1 - r_0$ and $c_a = 1 - c_b = 1 - (r_1 - r_0)$. Because random numbers cannot be extracted from the output bits in Part B, the mutual information between legitimate user (Q) and any third party user (E) is

$$I(Q : E) = c_a H(e_z) + 1 - c_a = (1 - r_1 + r_0)H(e_z) + r_1 - r_0. \tag{6}$$

Therefore, we can rewrite the number of extracted random bits as

$$K_{final} = n_z[1 - I(Q : E)] - t_e = (1 - r_1 + r_0)[n_z - n_z H(e_z)] - t_e. \tag{7}$$

By observing Eqs. (3) and (7), we can find that the two formulas are the same when $r_1 = r_0$ (i.e., the readout error is the same for $|0\rangle$ and $|1\rangle$).

The estimation of upper bound of e_z. In practice, the preparation of superposition state $|+\rangle$ is affected by various noises, which results in errors and affects the random number generation rate. To determine how many random bits can be extracted from the raw data, we need to estimate the upper bound of parameter e_z, i.e., the errors in the preparation of $|+\rangle$ state. As shown in Fig. 1, e_z can be mainly divided into two parts, one is the errors in the preparation of initial state $|0\rangle$, and the other is the errors in the operation of single-qubit $RY(\pi/2)$ gate. Through experimental measurements, the errors in the preparation of the initial state can be determined. And one's own quantum computer can obtain the initialization error on time. According to Eq. (1), the upper bound of e_z can be determined with the estimation of e_{bx}. Thus, to estimate the upper bound of e_z, the value of e_{bx} should be firstly estimated. In this subsection, we consider two cases, one is to consider the errors in quantum gate and readout, and the other is to consider the errors in the initial state, quantum gate and readout.

In our protocol, only the single-qubit gate $RY(\pi/2)$ is used. Due to the presence of various noise and the imperfection of control mechanism, $RY(\pi/2)$ gate exits deviations of the rotation angle around the Y-axis and the axis of rotation. In this case, the actual $RY(\pi/2)$ gate can be equivalent to the superposition of $RY(\theta)$ gate and $RZ(\theta)$ gate. Denoting that the deviation of the rotation angle around the Y-axis is δ and the rotation angle around the Z-axis is ϕ. Therefore, the actual rotation angle around the Y-axis is $\frac{\pi}{2} + \delta$ and the $RY(\frac{\pi}{2} + \delta)$ gate

can be represented by square matrices, i.e., $RY(\frac{\pi}{2}+\delta)=\begin{bmatrix} cos(\frac{\pi}{4}+\frac{\delta}{2}) & -sin(\frac{\pi}{4}+\frac{\delta}{2}) \\ sin(\frac{\pi}{4}+\frac{\delta}{2}) & cos(\frac{\pi}{4}+\frac{\delta}{2}) \end{bmatrix}$. The $RZ(\phi)$ gate is expressed with $\begin{bmatrix} e^{-i\frac{\phi}{2}} & 0 \\ 0 & e^{i\frac{\phi}{2}} \end{bmatrix}$.

Case 1: The errors in quantum gate and readout are considered.

To prepare the superposition state $|+\rangle$, the first $RY(\pi/2)$ gate is performed on the initial state $|0\rangle$, which is equivalent to the superposition of $RY(\frac{\pi}{2}+\delta)$ gate and $RZ(\phi)$ gate, resulting in the quantum state

$$\begin{aligned} |\varphi_1\rangle &= \frac{cos\left(\frac{\pi}{4}+\frac{\delta}{2}\right)e^{-i\frac{\phi}{2}}+sin\left(\frac{\pi}{4}+\frac{\delta}{2}\right)e^{i\frac{\phi}{2}}}{\sqrt{2}}|+\rangle+\frac{cos\left(\frac{\pi}{4}+\frac{\delta}{2}\right)e^{-i\frac{\phi}{2}}-sin\left(\frac{\pi}{4}+\frac{\delta}{2}\right)e^{i\frac{\phi}{2}}}{\sqrt{2}}|-\rangle \\ &= \left[cos\left(\frac{\pi}{4}+\frac{\delta}{2}\right)e^{-i\frac{\phi}{2}}\ \ sin\left(\frac{\pi}{4}+\frac{\delta}{2}\right)e^{i\frac{\phi}{2}}\right]^T. \end{aligned} \tag{8}$$

Therefore, the prepared quantum state is in the superposition of $|+\rangle$ state and $|-\rangle$ state, where the probability of $|+\rangle$ state is $\frac{1+cos\delta cos\phi}{2}$ and the probability of $|-\rangle$ state is $\frac{1-cos\delta cos\phi}{2}$, respectively. Applying the same $RY(\frac{\pi}{2}+\delta)$ gate and $RZ(\phi)$ gate on the quantum state $|\varphi_1\rangle$, the resulting quantum state is

$$|\varphi_2\rangle=\left(\left(\frac{1-sin(\delta)}{2}\right)(cos\phi-isin\phi)-\left(\frac{1+sin(\delta)}{2}\right)\right)|0\rangle+\left(\left(\frac{cos(\delta)}{2}\right)(cos\phi-isin\phi+1)\right)|1\rangle. \tag{9}$$

Finally, we can obtain $|0\rangle$ or $|1\rangle$ to measure the quantum state $|\varphi_2\rangle$, where the probability of $|0\rangle$ is $(\frac{sin^2\delta+1-cos\phi+sin^2\delta cos\phi}{2})$ and the probability of $|1\rangle$ is $\frac{cos^2\delta}{2}(1+cos\phi)$ in theory.

Furthermore, considering the readout error in the quantum computer, we can obtain

$$\begin{cases} N_0 = n_0(1-r_0)+n_1r_1 \\ N_1 = n_1(1-r_1)+n_0r_0, \end{cases} \tag{10}$$

where N_0 and N_1 are the numbers of 0 and 1 in the results of X-basis measurement with readout error which satisfies $N_0+N_1=n_x$, n_0 and n_1 represent the numbers of 0 and 1 in the results of X-basis measurement without readout error, respectively. n_0 and n_1 can be expressed as

$$\begin{cases} n_0 = \left(\frac{sin^2\delta+1-cos\phi+sin^2\delta cos\phi}{2}\right)n_x \\ n_1 = \frac{cos^2\delta}{2}(1+cos\phi)n_x. \end{cases} \tag{11}$$

In our protocol, the result of $|-\rangle$ state in the randomness source is defined as the preparation error of superposition state, so the error e_{bx} is equal to the probability of $|-\rangle$ state, i.e., $e_{bx}=\frac{1-cos\delta cos\phi}{2}$.

By solving Eq. (10), the value of n_0 and n_1 can be obtained. In a real quantum computer, the deviation of rotation angle around the Y-axis δ and around the Z-axis ϕ are both in $(-\frac{\pi}{2},\frac{\pi}{2})$, so $0<cos\phi<1$. According to Eq. (11), we can obtain $cos^2\delta=\frac{2n_1}{n_x(1+cos\phi)}$. Based on the expression for $cos^2\delta$ and the range value of $cos\phi$, the range of δ can be determined which satisfies $\frac{n_1}{n_x}<cos^2\delta<\frac{2n_1}{n_x}$. Given a value of δ, the value of ϕ can also be determined with Eq. (11). Therefore, the preparation error of $|+\rangle$ in the X-basis measurement can be calculated with $e_{bx}=\frac{1-cos\delta cos\phi}{2}$.

Case 2: The errors in the initial state, quantum gate and readout are considered.

Due to the presence of errors in preparation of initial state, the initial state can be represented with $|\varphi_0\rangle=\alpha|0\rangle+\beta|1\rangle$, where $|\alpha|^2+|\beta|^2=1$, and the value of α and β can be obtained by measuring the initial state directly. In the computational basis, the state can be written as vector $\left[\alpha\ \ \beta\right]^T$. The first $RY(\pi/2)$ gate is applied on the initial state $|\varphi_0\rangle$ to prepare the state $|+\rangle$, resulting in quantum state

$$\begin{aligned} |\varphi_1\rangle &= \frac{e^{-i\frac{\phi}{2}}\left(\alpha cos\left(\frac{\pi}{4}+\frac{\delta}{2}\right)-\beta sin\left(\frac{\pi}{4}+\frac{\delta}{2}\right)\right)+e^{i\frac{\phi}{2}}\left(\alpha sin\left(\frac{\pi}{4}+\frac{\delta}{2}\right)+\beta cos\left(\frac{\pi}{4}+\frac{\delta}{2}\right)\right)}{\sqrt{2}}|+\rangle \\ &+\frac{e^{-i\frac{\phi}{2}}\left(\alpha cos\left(\frac{\pi}{4}+\frac{\delta}{2}\right)-\beta sin\left(\frac{\pi}{4}+\frac{\delta}{2}\right)\right)-e^{i\frac{\phi}{2}}\left(\alpha sin\left(\frac{\pi}{4}+\frac{\delta}{2}\right)+\beta cos\left(\frac{\pi}{4}+\frac{\delta}{2}\right)\right)}{\sqrt{2}}|-\rangle \\ &= \left[e^{-i\frac{\phi}{2}}\left(\alpha cos\left(\frac{\pi}{4}+\frac{\delta}{2}\right)-\beta sin\left(\frac{\pi}{4}+\frac{\delta}{2}\right)\right)\ e^{i\frac{\phi}{2}}\left(\alpha sin\left(\frac{\pi}{4}+\frac{\delta}{2}\right)+\beta cos\left(\frac{\pi}{4}+\frac{\delta}{2}\right)\right)\right]^T. \end{aligned} \tag{12}$$

Thus, the probability of $|+\rangle$ state and $|-\rangle$ state are $cos\phi(\alpha^2cos\delta-\beta^2cos\delta-\alpha\beta sin\delta)$ and $1-cos\phi(\alpha^2cos\delta-\beta^2cos\delta-\alpha\beta sin\delta)$, respectively. To measure the quantum state on the X-basis, the same $RY(\frac{\pi}{2}+\delta)$ gate and $RZ(\phi)$ gate are performed on the quantum state $|\varphi_1\rangle$, and the quantum state $|\varphi_2\rangle$ is obtained with

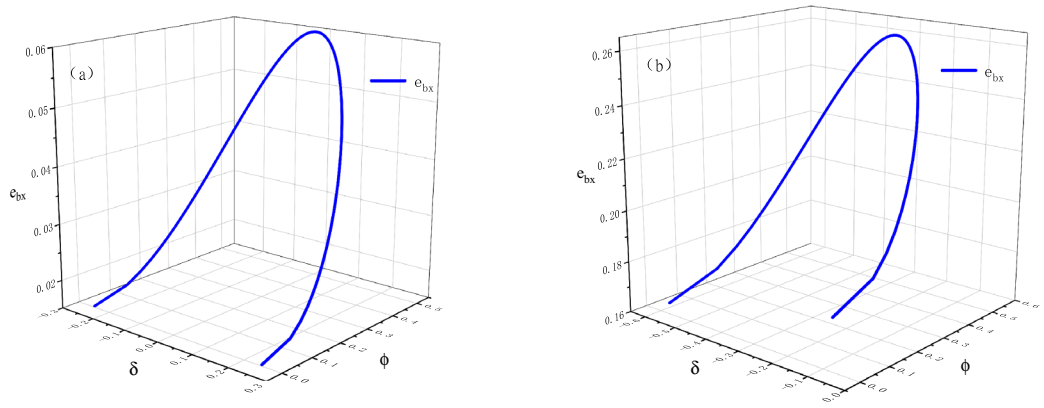


Figure 3. Relationships between e_{bx}, δ and ϕ. Simulated results with varying δ and ϕ. (**a**) Case 1; (**b**) Case 2.

$$|\varphi_2\rangle = \left[e^{-i\phi}cos\left(\frac{\pi}{4}+\frac{\delta}{2}\right)\left(\alpha cos\left(\frac{\pi}{4}+\frac{\delta}{2}\right)-\beta sin\left(\frac{\pi}{4}+\frac{\delta}{2}\right)\right)-sin\left(\frac{\pi}{4}+\frac{\delta}{2}\right)\left(\alpha sin\left(\frac{\pi}{4}+\frac{\delta}{2}\right)+\beta cos\left(\frac{\pi}{4}+\frac{\delta}{2}\right)\right)\right]|0\rangle + \left[e^{i\phi}cos\left(\frac{\pi}{4}+\frac{\delta}{2}\right)\left(\alpha sin\left(\frac{\pi}{4}+\frac{\delta}{2}\right)+\beta cos\left(\frac{\pi}{4}+\frac{\delta}{2}\right)\right)+sin(\frac{\pi}{4}+\frac{\delta}{2})\left(\alpha cos\left(\frac{\pi}{4}+\frac{\delta}{2}\right)+\beta sin\left(\frac{\pi}{4}+\frac{\delta}{2}\right)\right)\right]|1\rangle \tag{13}$$

By measuring the quantum state $|\varphi_2\rangle$, we can obtain that the probability of $|0\rangle$ state is $\alpha^2+\frac{1}{2}(\beta^2-\alpha^2)(cos^2\delta+cos\phi cos^2\delta)+\frac{1}{2}\alpha\beta sin2\delta(cos\phi+1)$ and the probability of $|1\rangle$ state is $\beta^2+\frac{1}{2}(\alpha^2-\beta^2)(cos^2\delta+cos\phi cos^2\delta)-\frac{1}{2}\alpha\beta sin2\delta(cos\phi+1)$ in theory. The error e_{bx} is equal to the probability of $|-\rangle$ state, i.e., $e_{bx}=1-cos\phi(\alpha^2cos\delta-\beta^2cos\delta-\alpha\beta sin\delta)$.

Based on Eq. (10), the numbers of 0 and 1 in the results of X-basis measurement without readout errors, i.e., n_0 and n_1, can be determined. According to the probabilities of 0 and 1 by measuring the quantum state $|\varphi_2\rangle$, n_0 and n_1 can be expressed as

$$\begin{cases} n_0=(\alpha^2+\frac{1}{2}(\beta^2-\alpha^2)(cos^2\delta+cos\phi cos^2\delta)+\frac{1}{2}\alpha\beta sin2\delta(cos\phi+1))n_x \\ n_1=(\beta^2+\frac{1}{2}(\alpha^2-\beta^2)(cos^2\delta+cos\phi cos^2\delta)-\frac{1}{2}\alpha\beta sin2\delta(cos\phi+1))n_x \end{cases}. \tag{14}$$

Similar with the analysis of Case 1, the deviations of rotation angle around the Y-axis δ and around the Z-axis ϕ are both in $(-\frac{\pi}{2},\frac{\pi}{2})$ and $0<cos\phi<1$. With Eq. (14) and the range value of $cos\phi$, the range of δ can be determined which satisfies $\frac{\alpha^2-\frac{n_0}{n_x}}{2}<\frac{1}{2}(\alpha^2-\beta^2)cos^2\delta-\frac{1}{2}\alpha\beta sin2\delta<\alpha^2-\frac{n_0}{n_x}$. Given a value of δ, the value of ϕ can also be determined with Eq. (14). Therefore, the preparation error of $|+\rangle$ in the X-basis measurement can be calculated with $e_{bx}=1-cos\phi(\alpha^2cos\delta-\beta^2cos\delta-\alpha\beta sin\delta)$.

For example, suppose $\frac{N_0}{n_x}=0.151$, $\frac{N_1}{n_x}=0.849$, $r_0=0.05$, $r_1=0.1$, $\alpha^2=0.9$ and $\beta^2=0.1$, we can obtain $\frac{n_0}{n_x}=0.06$ and $\frac{n_1}{n_x}=0.94$ with Eq. (10). Based on the expression of δ, the range value of δ can be calculated and the corresponding results are $(-0.24747, 0.2474)$ and $(-0.56921, -0.07428)$ in Case 1 and Case 2, respectively. With (11) and Eq. (14), the deviation of rotation angle around the Z-axis ϕ is determined in the two Cases. Moreover, the relationship between δ and ϕ is shown in Fig. 4b and d. Utilizing the determined value of δ and ϕ, the error e_{bx} can be calculated in Case 1 and Case 2, and the relationship between δ, ϕ and e_{bx} is shown in Fig. 3. Figure 4a and c shows the relationship between δ and e_{bx} in Case 1 and Case 2, respectively. In Case 1, we can discover that the parameter e_{bx} has a maximum value when $\delta=0$, i.e., $e_{bx}\leq 0.05998$. In Case 2, the parameter e_{bx} also has a maximum value, i.e., $e_{bx}\leq 0.26016$. The value of e_{bx} calculated in Case 2 is larger than that in Case 1, which means that the errors in preparation of initial state have effects on e_{bx}. Then, according to Eq. (1), the bound of error e_z can be determined.

Optimization of parameter q_x. In the cloud superconducting quantum computer of IBM, the quantum circuit is repeatedly sent to the real devices. The running time directly affects the final data and parameter estimation. To increase the final generation rate of the QRNG and improve the security of the QRNG protocol, parameters should be optimized. Based on the parameter optimization method in Ref.[34], we consider the influence of the finite data size on the parameter estimation and optimize the ratio of X-basis measurements q_x.

In our protocol, the measurements results of superposition state $|+\rangle$ in the Z basis are used to generate random numbers, and the errors in the preparation of superposition state $|+\rangle$ can be estimated by the measurement results of X-basis. Based on the method introduced in "Optimization of parameter q_x" section, e_z can be well approximated by e_{bx} with an infinite data size. However, due to the statistical fluctuations, the parameter e_z cannot be estimated accurately and the method of approximating is crucial. The parameter e_z is estimated by Eq. (1) and the statistical fluctuation o is bounded by Eq. (2). According to Eq. (2), there is a trade-off between q_x and o for the ratio of the final random bit length over the raw data size given that ε_e is fixed. Generally, the

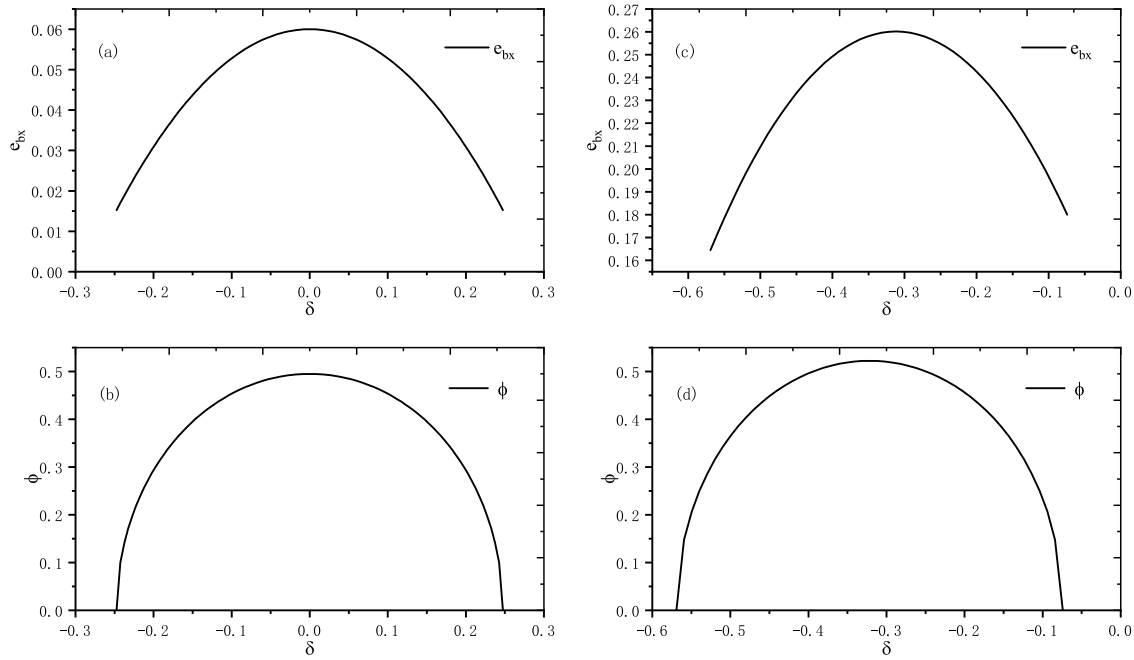


Figure 4. (**a**, **c**) Projection of the *xz* plane of Fig. 3a and b. Relationship between rotation angle error δ and preparation error of $|+\rangle$ state e_{bx}. (**b**, **d**) Projection of the *xy* plane of Fig. 3a and b. Relationship between errors in the rotation angle around Y-axis δ and Z-axis ϕ.

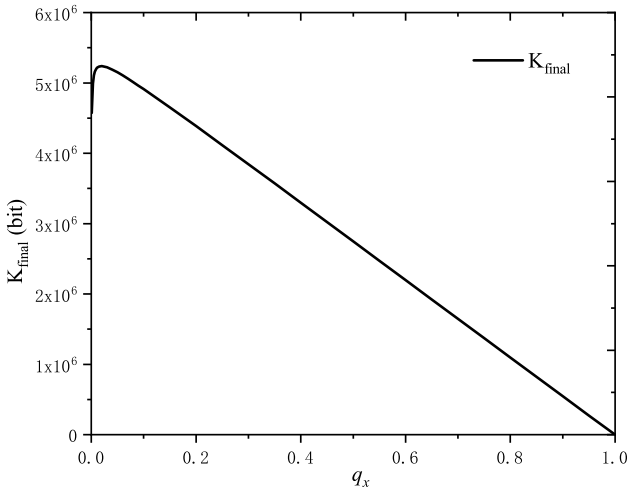
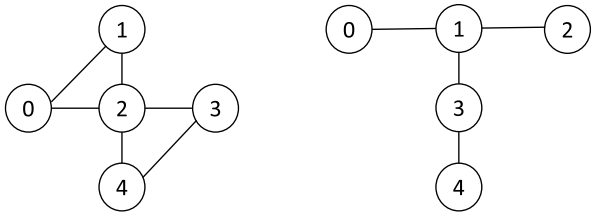


Figure 5. Relationship between basis choice rate q_x and final extracted random bits K_{final}. Here, we set $e_{bx} = 0.05, r_0 = 0.05, r_1 = 0.1$ and $n = 8.192 \times 10^6$.

failure probability ε_e is picked to be a small value. Hence, the value of q_x should be optimized for the randomness extraction rate and follows the condition:

$$\begin{aligned} &\textbf{Max} : K_{final}, \\ &\textbf{s}.t. : \varepsilon_e = Prob(e_z > e_{bx} + o) \leq \frac{1}{\sqrt{q_x(1-q_x)e_{bx}(1-e_{bx}n)}} 2^{-n\zeta(o)} \end{aligned} \tag{15}$$

With the method of the numerical solution, the optimized q_x can be obtained. In the cloud superconducting quantum computer of IBM, the maximum executing number of a quantum circuit is 8192 times. Repeating the quantum circuit, the final number of executions n can be up to 8.192×10^6 times. The value of ε_e is 2^{-100} in our later data processing. Supposing that the preparation error of superposition sate in the X-basis e_{bx} is 0.05, the readout error of $|0\rangle$ is $r_0 = 0.05$ and the readout error of $|1\rangle$ is $r_0 = 0.1$, we can compute the optimal q_x for the



(a) *IBMQ_5_yorktown* (b) *IBMQ_lima*

Figure 6. Device topology of *IBMQ_5_yorktown* and *IBMQ_lima*.

Device	Readout error	
	r_0	r_1
IBMQ_5_yorktown	0.072	0.0394
IBMQ_lima	0.0964	0.0122

Table 1. The readout errors of Q_0 for *IBMQ_5_yorktown* and *IBMQ_lima*.

final extracted random bits K_{final}, as shown in Fig. 5. The value of K_{final} has a maximum value which means that the generation rate of random numbers can achieve a maximum value for a given condition.

Experiment on the cloud superconducting quantum computer of IBM

In this section, we perform our proposed protocol on the cloud superconducting quantum computers of IBM to show its practicality. Since the error in the preparation of the initial sates is almost zero in the quantum computers of IBM, the error e_{bx} can be estimated with the method in Case 1. In the quantum computer system, 8192 is the maximum number of uninterrupted shots available. For demonstration purposes, the basis choice is achieved by running the Z-basis measurement of the quantum circuit with 8192 times and the X-basis measurement of the quantum circuit with 251 times.

IBMQ_5_yorktown and *IBMQ_lima* are used in the experiment where the device topologies are shown in Fig. 6[44]. *IBMQ_5_yorktown* and *IBMQ_lima* both have five qubits and the readout error for each qubit is provided by Qiskit[45]. Without loss of generality, we select the qubit 0 (Q_0) of the two devices to execute the quantum circuit and the readout errors of Q_0 for these two devices are shown in Table 1.

By running the quantum circuits of SI-QRNG repeatedly, we obtain two sequences under each quantum computer device which are the results of the Z-basis measurement and X-basis measurement. The sequence L_z of Z-basis measurement is used to extract random bits and its length n_z is 819200. The other sequence L_x is used to estimate the preparation error of superposition state $|+\rangle$ in the Z-basis e_{bx} and its length n_x is 25100.

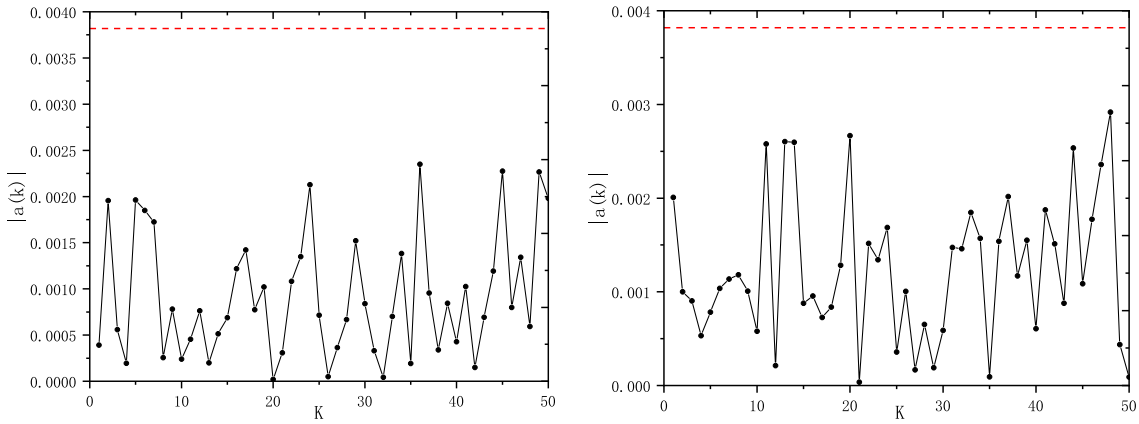
In the sequence L_x of *IBMQ_5_yorktown*, the number of 0 is $N_0 = 2669$ and the number of 1 is $N_1 = 22431$. According to Eq. (10) and the readout error of Q_0, we can obtain $n_0 = 299.8557$ and $n_1 = 24800.1443$. With Eq. (11), the value of δ is calculated which is between -0.1095186 and 0.1095186. Exploiting the expression for e_{bx}, we can obtain the maximum value of e_{bx} is 0.011943. Based on Eqs. (1) and (2), the bound of e_z is determined and equals to 0.0122442. Thus, the number of random bits $K_{yorktown}$ that can be extracted from the Z-basis measurement is 741006 which is calculated by using Eq. (7), and the corresponding random bits' generation rate $r_{yorktown}$ is 0.9045. Utilizing the same method, the parameter e_z and the final extracted random bits K_{lima} in the *IBMQ_lima* device can be calculated. The numbers of 0 and 1 in the X-basis of *IBMQ_lima* are $N_0 = 1186$ and $N_1 = 23914$. By calculating, we can obtain $e_{bx} = 0.039318$, $e_z = 0.0397301$, $K_{lima} = 621729$ and the corresponding random bits' generation rate r_{lima} is 0.7589.

After obtaining the raw data and the estimated e_z, we apply the Toeplitz matrix hashing on the raw data to obtain the final random numbers[46]. To evaluate the randomness of the final data, we perform the NIST Statistical Test on the final random numbers[47]. Since the length of the final data cannot satisfy some test items of the NIST Statistical Test, the final data is only subjected to the nine test items from the NIST Statistical Test which are the frequency test, frequency within a block test, runs test, longest runs within a block test, FFT test, approximate entropy test, Matrix Rank Test and the cumulative sums test (forward, backward). Each test item produces a corresponding P-value and the significance level α is set as 0.01 in our test. If the P-value $\geq \alpha$, the final data is considered as true random numbers with $1 - \alpha$ of confidence level. The results of the NIST Statistical Test on the two final sequences with a length of 600,000 bits are shown in Table 2. From Table 2, one can see that all the P-values are larger than 0.01, which indicates the final data of *IBMQ_5_yorktown* and *IBMQ_lima* pass all test items.

Furthermore, we calculate the autocorrelation coefficients of the final data to test the independence between neighboring bits of final data. The autocorrelation coefficient is defined as $a(k) = \frac{\Xi[(X_i-\mu)(X_{i+k}-\mu)]}{\sigma^2}$, where Ξ stands for expectation, X_i denotes the value of the i_{th} bit in the sequence, μ and σ^2 are the average and the variance

Test	*IBMQ_5_yorktown*	*IBMQ_lima*
Frequence	0.706196	0.434013
Block frequency	0.444177	0.754105
Runs	0.760474	0.120287
Longest run	0.668568	0.653644
FFT	0.981097	0.915088
Approximate entropy	0.325238	0.162457
Rank	0.891846	0.653728
Cumulative sums (forward)	0.916711	0.782753
Cumulative sums (backward)	0.834860	0.628746
Result	Success	Success

Table 2. The NIST Statistical Test results and corresponding P-value of final data.



(a) *IBMQ_5_yorktown* (b) *IBMQ_lima*

Figure 7. The absolute value of the autocorrelation function of the final data generated by *IBMQ_5_yorktown* and *IBMQ_lima*. The red dashed line is the three-standard-deviation line.

of the sequence[16]. The final data with length of n_l is considered as true random numbers when all autocorrelation coefficients are greater than the three-standard-deviation value $a_{3\sigma}$ with $a_{3\sigma} = 3/\sqrt{n_l}$. We choose a sequence with a length of 600,000 bits to perform the autocorrelation test and the corresponding $a_{3\sigma}$ is approximately 0.003873. The results of the autocorrelation test of the two final sequences are shown in Fig. 7. The red dashed line stands for the corresponding three-standard-deviation value $a_{3\sigma}$. It can be seen that all the absolute values of autocorrelation coefficients are below $a_{3\sigma}$. From the results of the NIST Statistical Test and autocorrelation test, we can know the randomness of the final data generated by *IBMQ_5_yorktown* and *IBMQ_lima* can be guaranteed.

Conclusion

Due to the presence of noise and the imperfection of the control mechanism, there exit errors in the initialization, quantum gate and readout in the quantum computer, which leads to the bias of the output data. Motivated by the SI-QRNG based on optics[34], we propose and implement a QRNG scheme using a cloud superconducting quantum computer. Our proposed protocol can estimate the preparation error of superposition state $|+\rangle$ and give the final number of extracted random bits, which guarantees the security of generated random numbers. The readout errors of $|0\rangle$ and $|1\rangle$ are generally different in the quantum computer, which impacts the randomness of generated random numbers. Utilizing the method for solving the imperfection of detector in origin SI-QRNG protocol, we firstly give the final extracted number of random bits K_{final} with readout error. Then, by further considering the errors in the preparation of initial state and quantum gate, the estimation methods for parameter e_z are given, where the quantum gate error includes the deviation of the rotation angle around the Y-axis δ and the rotation angle around the Z-axis ϕ. Moreover, we optimize the ratio of X-basis measurements q_x to increase the final random number generation rate.

To prove the practicability of our protocol, we perform our proposed protocol on the cloud superconducting quantum computer of IBM. The random numbers generated by *IBMQ_5_yorktown* and *IBMQ_lima* are post-processed by Toeplitz matrix hashing to obtain the final random numbers. The results of the NIST Statistical Test and autocorrelation test show that the final random numbers could be considered as true random numbers. Utilizing the SI-QRNG scheme, the error in the preparation of quantum superposition state $|+\rangle$ can be monitored, and we realize the generation of true random numbers in quantum computers with noise.

Received: 2 June 2021; Accepted: 30 November 2021
Published online: 13 December 2021

References

1. Shannon, C. E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **28**, 656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x (1949).
2. Metropolis, N. & Ulam, S. The Monte Carlo method. *J. Am. Stat. Assoc.* **44**, 335–341. https://doi.org/10.1080/01621459.1949.10483310 (1949).
3. Pangratz, H. & Weinrichter, H. Pseudo-random number generator based on binary and quinary maximal-length sequences. *IEEE Trans. Comput.* **28**, 637–642 (1979).
4. Maheshwari, R., Gupta, S., Sharma, V. & Chauhan, V. VRS algorithm a novel approach to generate pseudo random numbers. In *2014 IEEE International Advance Computing Conference (IACC)*, 7–10 (2014).
5. Xu, F., Curty, M., Qi, B., Qian, L. & Lo, H. K. Discrete and continuous variables for measurement-device-independent quantum cryptography. *Nat. Photon.* **9**, 772–773 (2015).
6. Pirandola, S. *et al.* Advances in quantum cryptography. *Adv. Opt. Photon.* **12**, 1012–1236 (2020).
7. Wayne, M. A. & Kwiat, P. G. Low-bias high-speed quantum random number generator via shaped optical pulses. *Opt. Express* **18**, 9351–9357. https://doi.org/10.1364/OE.18.009351 (2010).
8. Fürst, H. *et al.* High speed optical quantum random number generation. *Opt. Express* **18**, 13029–13037. https://doi.org/10.1364/OE.18.013029 (2010).
9. 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**, 145–266 (2011).
10. Gabriel, C. *et al.* A generator for unique quantum random numbers based on vacuum states. *Nat. Photon.* **4**, 711–715 (2010).
11. 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).
12. Zhou, Q., Valivarthi, V. R. R., John, C. & Tittel, W. Practical quantum random number generator based on sampling vacuum fluctuations. *Quantum Eng.* (2017).
13. Xu, F. *et al.* Ultrafast quantum random number generation based on quantum phase fluctuations. *Opt. Express* **20**, 12366 (2012).
14. 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. https://doi.org/10.1364/OL.35.000312 (2010).
15. Wei, S. *et al.* Compact quantum random number generator based on superluminescent light-emitting diodes. *Rev. Sci. Instrum.* **88**, 123115 (2017).
16. Wei, W., Xie, G., Dang, A. & Hong, G. High-speed and bias-free optical random number generator. *IEEE Photon. Technol. Lett.* **24**, 437–439 (2012).
17. Alexeev, Y. *et al.* Quantum computer systems for scientific discovery. *P. R. X. Quantum* **2**, 017001. https://doi.org/10.1103/PRXQuantum.2.017001.1912.07577 (2021).
18. Dicarlo, L. *et al.* Demonstration of two-qubit algorithms with a superconducting quantum processor. *Nature* **460**, 240–4 (2009).
19. Devoret, M. H. & Schoelkopf, R. J. Superconducting circuits for quantum information: An outlook. *Science* **339**, 1169–1174. https://doi.org/10.1126/science.1231930 (2013).
20. Zu, C. *et al.* Experimental realization of universal geometric quantum gates with solid-state spins. *Nature* **514**, 72 (2014).
21. Jelezko, F., Gaebel, T., Popa, I., Gruber, A. & Wrachtrup, J. Observation of coherent oscillations in a single electron spin. *Phys. Rev. Lett.* **92**, 076401 (2004).
22. Knill, E., Laflamme, R. & Milburn, G. J. A scheme for efficient quantum computation with linear optics. *Nature* **409**, 46–52 (2001).
23. Preskill, J. Quantum computing in the NISQ era and beyond. *Quantum* **2**, 79. https://doi.org/10.22331/q-2018-08-06-79 (2018).
24. LaRose, R. Overview and comparison of gate level quantum software platforms. *Quantum* **3**, 130. https://doi.org/10.22331/q-2019-03-25-130 (2019).
25. Shikano, Y. Unpredictable random number generator. In *Application of Mathematics in Technical and Natural Sciences: 12th International On-line Conference for Promoting the Application of Mathematics in Technical and Natural Sciences - AMiTaNS'20* (2020).
26. Pironio, S. *et al.* Random numbers certified by Bell's theorem. *Nature* **464**, 1021 (2010).
27. Christensen, B. G., Mccusker, K. T., Altepeter, J. B., Calkins, B. & Kwiat, P. G. Detection-loophole-free test of quantum nonlocality, and applications. *Phys. Rev. Lett.* **111**, 130406 (2013).
28. Colbeck, R. & Kent, A. Private randomness expansion with untrusted devices. *J. Phys. A Math. Theor.* **44** (2010).
29. Bowles, J., Quintino, M. T. & Brunner, N. Certifying the dimension of classical and quantum systems in a prepare-and-measure scenario with independent devices. *Phys. Rev. Lett.* **112**, 140407 (2013).
30. Cao, Z., Zhou, H. & Ma, X. Loss-tolerant measurement-device-independent quantum random number generation. *New J. Phys.* **17**, 125011 (2015).
31. Ma, J., Hakande, A., Yuan, X. & Ma, X. Coherence as a resource for source-independent quantum random-number generation. *Phys. Rev. A* **99** (2019).
32. Zhang, J., Zhang, Y., Zheng, Z., Chen, Z. & Yu, S. Finite-size analysis of continuous variable source-independent quantum random number generation. *Quantum Inf. Process.* **20** (2021).
33. Michel, T. *et al.* Real-time source independent quantum random number generator with squeezed states. *Phys. Rev. Appl.* **12** (2019).
34. Cao, Z., Zhou, H., Yuan, X. & Ma, X. Source-independent quantum random number generation. *Phys. Rev. X* **6**, 011020. https://doi.org/10.1103/PhysRevX.6.011020 (2016).
35. Marco Avesani, M., G., D., Vallone, G. & Villoresi, P. Source-device-independent heterodyne-based quantum random number generator at 17 gbps. *Nat. Commun.* **9** (2018).
36. Neumann, V. J. Various techniques used in connection with random digits. *J. Res. Nat. Bur. Stand. Appl. Math. Ser.* **3**, 36–38 (1951).
37. Samuelson, P. Constructing an unbiased random sequence. *J. Am. Stat. Assoc.* **63**, 1526–1527 (1968).
38. Tamura, K. & Shikano, Y. Quantum random number generation with the superconducting quantum computer ibm 20q tokyo. Cryptology ePrint Archive. Report 2020/078 (2020). https://ia.cr/2020/078.
39. Landauer, R. Irreversibility and heat generation in the computing process. *IBM J. Res. Dev.* **5**, 183–191. https://doi.org/10.1147/rd.53.0183 (1961).
40. Ma, X., Fung, C.-H.F., Boileau, J.-C. & Chau, H. Universally composable and customizable post-processing for practical quantum key distribution. *Comput. Secur.* **30**, 172–177. https://doi.org/10.1016/j.cose.2010.11.001 (2011).
41. Impagliazzo, R., Levin, L. & Luby, M. Pseudorandom number generation from one-way functions (1989).
42. Vallone, G., Marangon, D. G., Tomasin, M. & Villoresi, P. Quantum randomness certified by the uncertainty principle. *Phys. Rev. A* **90**, 052327. https://doi.org/10.1103/PhysRevA.90.052327 (2014).
43. Ma, D., Wang, Y. & Wei, K. Practical source-independent quantum random number generation with detector efficiency mismatch. *Quantum Inf. Process.* **19**, 384 (2020).
44. IBM, Q. https://quantum-computing.ibm.com/ (2021).
45. Aleksandrowicz, G. *et al.* Qiskit: An Open-source Framework for Quantum Computing. https://doi.org/10.5281/zenodo.2562111 (2019).

46. Ma, X. *et al.* Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. *Phys. Rev. A* **87**, 062327 (2013).
47. Rukhin, A. *et al.* NIST Special Publication 800-22: A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications (2010).

Acknowledgements

This work was supported by the the National Natural Science Foundation of China (61901525, 61701539 and 61972413), the National Cryptography Development Fund (mmjj20180107 and mmjj20180212).

Author contributions

Y.F., H.W. and Z.M. conceived the project. Y.L., W.W. and Y.F. performed the calculation and analysis, and revised the paper. Y.L., X.M. and Q.D. wrote the paper. All authors reviewed the paper.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to Y.F. or W.W.

Reprints and permissions information is available at www.nature.com/reprints.

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