Real-Time Source-Independent Quantum Random Number Generator Based on a Cloud Superconducting Quantum Computer

Yuanhao Li
State Key Laboratory of Mathematical Engineering and Advanced Computing
Weilong Wang
State Key Laboratory of Mathematical Engineering and Advanced Computing
Yangyang Fei (fei_yy@foxmail.com)
State Key Laboratory of Mathematical Engineering and Advanced Computing
Xiangdong Meng
Henan Key Laboratory of Network Cryptography Technology
Hong Wang
State Key Laboratory of Mathematical Engineering and Advanced Computing
Qianheng Duan
State Key Laboratory of Mathematical Engineering and Advanced Computing
Zhi Ma
State Key Laboratory of Mathematical Engineering and Advanced Computing

Research Article

Keywords: quantum random number generator, source-independent, quantum computer

Posted Date: June 14th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-583001/v1

Real-time source-independent quantum random number generator based on a cloud superconducting quantum computer

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

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

ABSTRACT

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, quantum computer can be used as a true random number generator. However, in practice, the implementation of quantum computer is subject to various noise sources which affect the randomness of the generated random numbers. To solve this problem, we propose a source-independent QRNG (SI-QRNG) scheme based on quantum computer which is motivated by the SI-QRNG scheme in quantum optics. The scheme can provide certified randomness by estimating the preparation error of superposition states in real time even when the source is untrusted, under the assumption that the measurement operation is trusted. Our analysis takes into account the readout error of quantum state and further gives the final extracted number of random bits. And the estimation method of preparation error of superposition state in randomness source. We also provide a parameter optimization method to increase the generation rate of random bits. In addition, by utilizing the cloud superconducting quantum computer of IBM, we experimentally demonstrate the practicality of our SI-QRNG scheme and achieve the generation of true random numbers.

Keywords: quantum random number generator, source-independent, quantum computer

1 Introduction

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].

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 quantum optics are proposed by using different randomness sources, including single photon detection[6–8], vacuum state fluctuation[9–11], laser phase fluctuation[12,13] and amplified spontaneous emission noise[14,15]. There are already some commercial QRNG products implementing these protocols. In general, 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[16], including superconducting quantum circuits[17,18], nuclear magnetic resonance[19,20] and optical systems[21]. Some companies have all launched cloud quantum computer which enables users to send quantum programs to use quantum computer[22,23]. Furthermore, due to the presence of superposition state, quantum computer can be considered as an unbiased QRNG to generate random numbers[24]. 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 the initial state $|0\rangle$. Thus, repeating measurements on the qubit in the $\{|0\rangle, |1\rangle\}$ basis, the 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 the 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 provide side information to eavesdroppers in practice. To enhance the security of QRNG, a self-testing or device-independent (DI) QRNGs are proposed which do not need to trust the generated quantum state and the measurement devices[25–27]. 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 loophole-free Bell test, and the random number generation rate is very low, which cannot satisfy the demands of the practical applications. In order 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[28–30].

Among SDI-QRNG schemes, source-independent (SI) QRNG has gathered lots of attention[31–33]. With reasonable assumptions that measurement devices are well-calibrated and the source is untrusted, the SI-QRNG can generate secure random numers and achieve considerable random number generation rate. Most of the SI-QRNG protocols are realized by the quantum optics devices. Utilizing a laser as randomness source, Zhu et al proposed a SI-QRNG scheme and realized a randomness generation rate of over 5000 *bps*[33], and Marco et al proposed a continuous-variable version of SI-QRNG protocol and realized a generation rate of 17 *Gbps*[34].

In addition to the quantum optics based SI-QRNG, the SI-QRNG scheme can also realized by using the quantum computer. In practice, the existing quantum computers are noisy and vulnerable to various types of errors such as gate error, initial state error, readout error and etc, which cause the randomness source to be untrusted. Motivated by the discrete-variable SI-QRNG based on quantum optics, we propose a scheme that can be quantify the randomness of quantum computer in real time and the final extraction rate of random number is given. Using the cloud superconducting quantum computer of IBM, we experimentally examine the effectiveness of the proposed SI-QRNG protocol.

The rest of this article is organized as follows. In Sec. 2, the protocol of SI-QRNG based on cloud superconducting quantum computer is briefly introduced. In Sec. 3, we analyze the protocol, where the final extracted number of random bits is further given with the readout error, and the estimation method and optimization of parameter are provided. In Sec. 4, an experimental demonstration of the scheme is performed with the cloud superconducting quantum computer of IBM. Finally, we conclude this paper in Sec. 5.

2 Source-independent QRNG

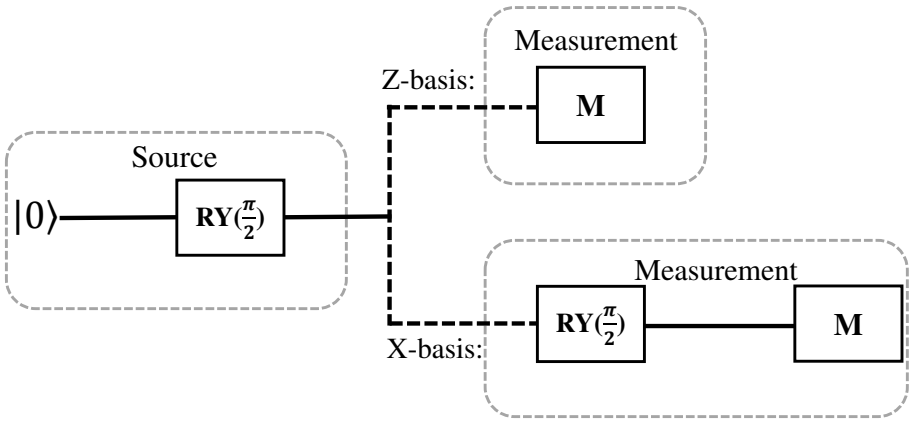


Figure 1. Quantum circuits for the proposed SI-QRNG. The qubit state is randomly measured in the X-basis or Z-basis.

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 applies $\pi/2$ 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 computers are 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 of each qubit may be impacted by hardware noise which cause the temporal correlation between the output bits[35]. Moreover, the single-qubit gate $RY(\theta)$ may also exit error due to the imperfections in the control mechanism. These errors cause the randomness source to be untrusted. At the same time, the readout error also cannot be ignored which leads to the bias of output bits.

Motivated by the quantum optics based SI-QRNG protocol proposed in Ref.[33], we implement the SI-QRNG protocol on quantum computer and give the quantum circuits, as shown in Fig. 1. Here, we assume that the randomness source is untrusted and the measurement operations can be characterized. That is to say, the readout errors in quantum computer are known for legitimate users. Eavesdropper may control the preparation of the initial state and the operation of quantum gate to acquire the information of randomness source. But if the preparation of initial state exists significant errors, malicious attackers cannot prepare the desired quantum state and eavesdrop on the information of the generated random numbers. And the preparation of initial state is generally perfect in a real quantum computer. Thus, we can make a reasonable assumption that the error in the preparation of initial state is negligible.

By estimating the conditional min-entropy based on the error of the X-basis measurement, the true random numbers can be extracted from the results of the Z-basis measurement. The details 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 $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. The quantum state might be correlated with the untrusted party Eve or the hardware noise. Then, the prepared superposition state is transmitted to the trusted measurement box of Alice.

(2) Random sampling: By utilizing a short random seed, Alice randomly chooses the X basis quantum circuit or Z-basis quantum circuit to measure the received quantum state. 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, quantum circuit is executed n times, including n_x in the X-basis quantum circuit and n_z 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, respectively. Therefore, a result of $|0\rangle$ means an error. Alice estimates 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[33]

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

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 choice X-basis 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, Alice aborts the protocol.

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

(5) Randomness extraction: Alice uses the Topelitz-matrix hashing method to extract true random numbers. The number of final random bits is

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

where 2^{-t_e} is the failure probability of the randomness extraction[36]. In practice, Alice needs to construct a Topelitz matrix of size $n_z \times [n_z - n_z H(e_z) - t_e]$ for randomness extraction, which requires the length of $n_z + n_z - n_z H(e_z) - t_e$ random bits and consumes $n_z H(e_z) + t_e$ bits to correct the errors of state $|+\rangle$. According to the leftover hash lemma[37], the final output random bits are not affected by the random bits used in the construction of the Topelitz matrix.

3 Analysis

3.1 Measurement with readout error

In the protocol of SI-QRNG based on quantum computer, except focusing on the untrusted source, the imperfections of measurement operation cannot be ignored. In what follows, we give the method to solve the problem and recalculate the number of final extracted random bits. In practice, the readout operation of quantum state is imperfect due to the presence of hardware noise or environment noise. Generally, the readout errors of $|0\rangle$ and $|1\rangle$ are different. The readout error of $|0\rangle$, r_0, means that $|0\rangle$ is prepared but the measurement outcome is $|1\rangle$. Similarly, the readout error of $|1\rangle$, r_1, means that $|1\rangle$ is prepared but the measurement outcome is $|0\rangle$. In the IBM's quantum computer, the measurement of a qubit yields an outcome of 0 or 1, and the

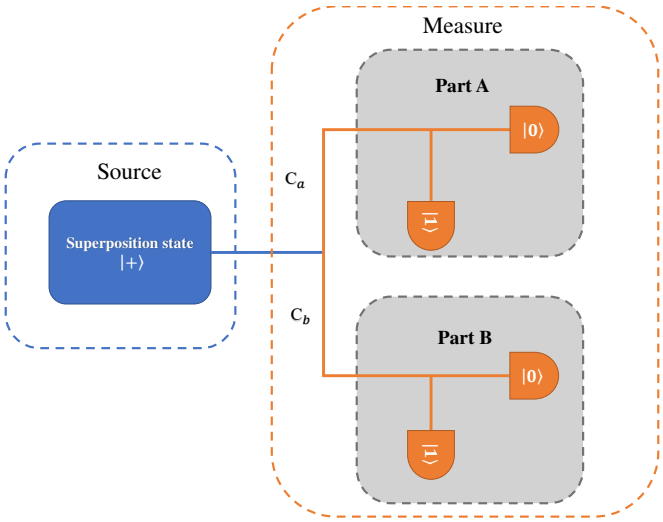


Figure 2. Equivalence of SI-QRNG under the different readout errors of quantum state.

difference between r_0 and r_1 leads to the asymmetry in the 1/0 ration of measurement outcomes. The readout error impacts the randomness and security of the output bits.

Motivated by the method of detector efficiency mismatch in quantum key distribution[38] and quantum optics based QRNG[39], we analyze the scenario that the readout errors of $|0\rangle$ and $|1\rangle$ are different in SI-QRNG protocol based on quantum computer. 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 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 no genuine randomness can be extracted. 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_1 is larger than r_0. 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 the output bits in Part B cannot extract any random numbers in which all information is stolen by Eve, the mutual information between Alice and Eve is

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

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

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

By observing Eq. 3 and Eq. 7, we can find that the two formulas are the same when $r_1 = r_0$ (i.e., the readout error is same for $|0\rangle$ and $|1\rangle$). To extract true random numbers from the original data in Z-basis measurements, the number of random bits consumed in the error correction is given by $n_z(1 - r_1 + r_0)H(e_z) + t_e$.

3.2 Parameter estimation

In practice, the various noise source affect the preparation of superposition state $|+\rangle$ and the operation of measurement. The results of X-basis measurement is used to estimate the preparation error of superposition state in source, which can monitor the conditional min-entropy in real time. As shown in Fig. 1, the errors in the preparation of $|+\rangle$ state e_z can be mainly divided

into two parts, one is the error in the preparation of initial state $|0\rangle$, and the other is the error in the operation of single-qubit $RY(\pi/2)$ gate. To eavesdrop on the information of the generated random numbers, the eavesdropper may control the quantum gate operation to prepare the desired quantum state under the condition that the initial state is perfectly prepared. Therefore, we only need to consider the error in quantum gate to estimate the preparation error of superposition state in randomness source. Note that the quantum gate operation and the readout operation can be considered as unaltered in a short time.

In the SI-QRNG 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 angle of rotation 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 angle of rotation around the Y-axis is δ and the angle of rotation around the Z-axis is ϕ. Therefore, the actual angle of rotation 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 $\begin{bmatrix} e^{-i\frac{\phi}{2}} & 0 \\ 0 & e^{i\frac{\phi}{2}} \end{bmatrix}$.

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 quantum state

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

Therefore, the qubit state prepared in the randomness source is in the superposition of $|+\rangle$ state and $|-\rangle$ state, where the probability of $|+\rangle$ state is $(\frac{cos(\frac{\pi}{4}+\frac{\delta}{2})e^{-i\frac{\phi}{2}}+sin(\frac{\pi}{4}+\frac{\delta}{2})e^{i\frac{\phi}{2}}}{\sqrt{2}})^2$ and the probability of $|-\rangle$ state is $(\frac{cos(\frac{\pi}{4}+\frac{\delta}{2})e^{-i\frac{\phi}{2}}-sin(\frac{\pi}{4}+\frac{\delta}{2})e^{i\frac{\phi}{2}}}{\sqrt{2}})^2$. Applying the same $RY(\frac{\pi}{2}+\delta)$ gate and $RZ(\phi)$ gate on the quantum state $|\varphi_1\rangle$, resulting the quantum state is

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

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

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

In the SI-QRNG 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., $e_{bx}=\frac{cos(\frac{\pi}{4}+\frac{\delta}{2})e^{-i\frac{\phi}{2}}-sin(\frac{\pi}{4}+\frac{\delta}{2})e^{i\frac{\phi}{2}}}{\sqrt{2}}^2=sin^2\frac{\phi}{2}cos^2\frac{\delta}{2}+sin^2\frac{\delta}{2}cos^2\frac{\phi}{2}$.

By solving Eq. 10, the value of n_0 and n_1 can be obtained. In a real quantum computer, the deviation of angle of rotation 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 $e_{bx}=sin^2\frac{\phi}{2}cos^2\frac{\delta}{2}+sin^2\frac{\delta}{2}cos^2\frac{\phi}{2}$.

For example, suppose $\frac{N_0}{n_x}=0.151$, $\frac{N_1}{n_x}=0.849$, $r_0=0.05$ and $r_1=0.95$, 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 $cos^2\delta$, the range value of δ results in $(-0.24747,0.2474)$. With Eq. 11, the deviation of rotation angle around the Z-axis ϕ is determined, and the relationship between δ and ϕ is given by Fig. 4(b). Utilizing the

determined value of δ and ϕ, the error e_{bx} can be calculated, and the relationship between δ, ϕ and e_{bx} is shown in Fig. 3. Fig. 4(a) shows the relationship between δ and e_{bx}. We can discover that the parameter e_{bx} has a maximum value when $\delta = 0$, i.e., $e_{bx} \leq 0.05998$. This means that the preparation error of $|+\rangle$ state in the X-basis achieve the max value when all errors are attributed to the deviation of the rotation angle δ around the Y-axis. According to Eq. 1, the bound of error e_z can be determined.

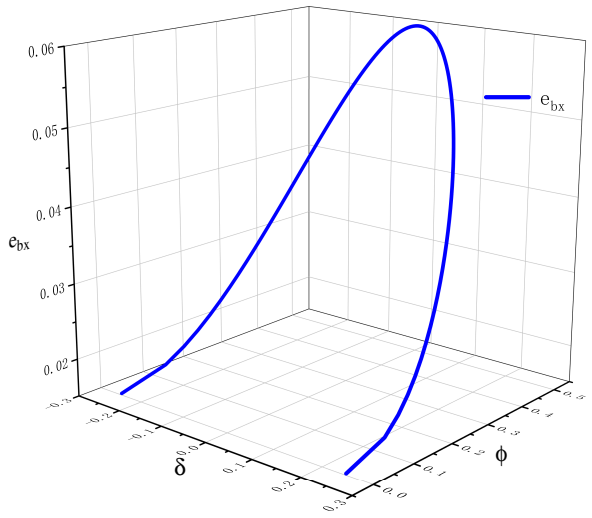


Figure 3. Relationships between e_{bx}, δ and ϕ. Simulated results with varying δ and ϕ.

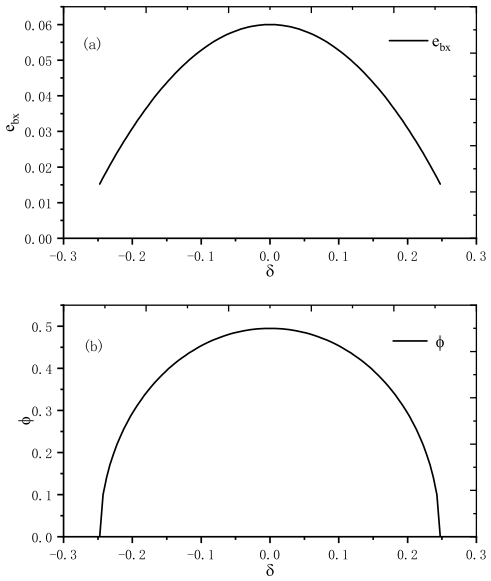


Figure 4. (a) Projection of the xz plane of Fig. 3. Relationship between rotation angle error δ and preparation error of $|+\rangle$ state e_{bx}, (b) Projection of the xy plane of Fig. 3. Relationship between errors in the rotation angle around Y-axis δ and Z-axis ϕ.

3.3 Parameter Optimization

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 QRNG protocol, parameter should be optimized. Here, we consider the influence of the finite data size on the parameter estimation and optimize the ratio of X-basis measurements q_x.

In the SI-QRNG protocol, the preparation error of superposition state $|+\rangle$ in the Z-basis can be well approximated by e_{bx}. However, due to the statistical fluctuations, the parameter e_z cannot be estimated accurately and the method of approximating it 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 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:

$$\begin{aligned} &\textbf{Max: } K_{final}, \\ &\textbf{s.t.: } \varepsilon_e = Prob(e_z > e_{bx} + o) \leq \frac{1}{\sqrt{q_x(1-q_x)e_{bx}(1-e_{bx}n)}} 2^{-n\zeta(o)} \end{aligned} \tag{12}$$

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

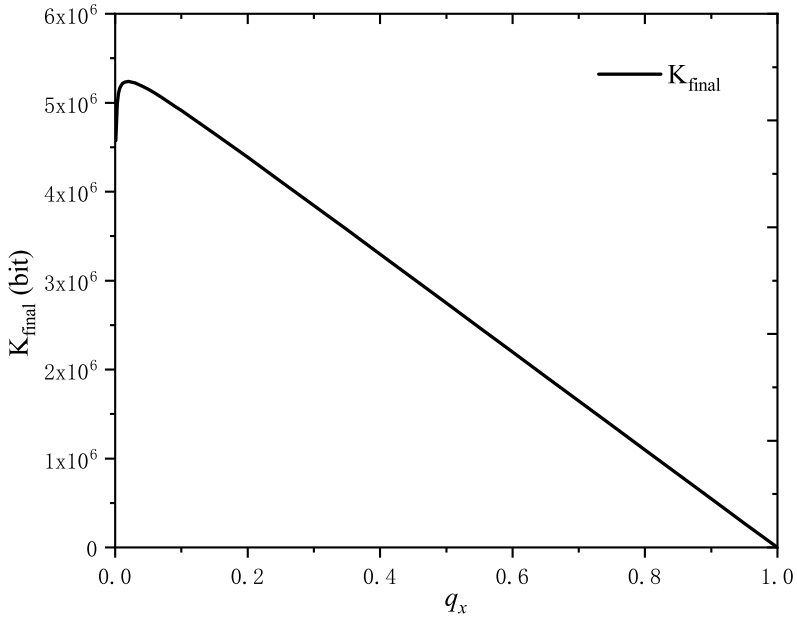


Figure 5. Relationship between basis choice rate q_x and final extracted random bits K_{final}. Here, we set $e_{bx} = 0.05$, $r_0 = 0.05$, $r_1 = 0.1$ and $n = 8.192 \times 10^6$.

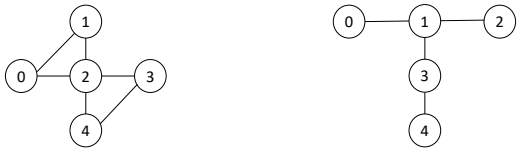
4 Experiment

In this section, we perform the SI-QRNG protocol on the cloud superconducting quantum computer of IBM to show its practicality. In the quantum computer system, 8192 is the maximum number of uninterrupted shots available. For demonstration purpose, the basis choice is achieved by running the Z-basis measurement of quantum circuit with 8192 times and the X-basis measurement of 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[40]. *IBMQ_5_yorktown* and *IBMQ_lima* both have five qubits and the readout error for each qubit is provided by Qiskit[41]. 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.

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

Readout error / Device	r_0	r_1
IBMQ_5_yorktown	0.072	0.0394
IBMQ_lima	0.0964	0.0122



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

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

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 Eq. 1 and Eq. 2, the bound of e_z is determined and equal to 0.029116. Thus, the number of random bits $K_{yorktown}$ that can be extracted from the Z-basis measurement is 647310 which is calculated by using Eq. 7. 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 $e_z = 0.0166923$ and $K_{lima} = 682495$.

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[42]. To evaluate the randomness of the final data, we perform NIST Statistical Test on the final random numbers[43]. 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 NIST Statistical Test on the two final sequences with length of 600000 bits are shown in Table. 2. From Table. 2, one can see that all the P-values are larger than 0.01, which indicates final data of *IBMQ_5_yorktown* and *IBMQ_lima* pass all test items.

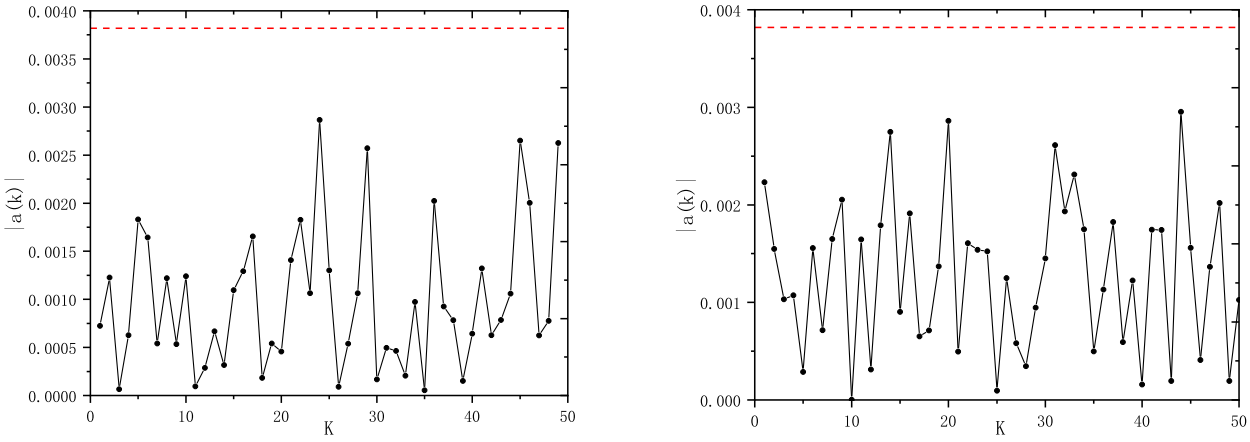
Table 2. The NIST Statistical Test results and corresponding P-value of final data.

Test	*IBMQ_5_yorktown*	*IBMQ_lima*
Frequence	0.987640	0.497098
Block Frequency	0.654699	0.935037
Runs	0.573521	0.084211
Longest Run	0.156405	0.302244
FFT	0.704611	0.075561
Approximate Entropy	0.154169	0.427700
Rank	0.585572	0.188018
Cumulative Sums(forward)	0.986036	0.838213
Cumulative Sums(backward)	0.981962	0.652511
Result	Success	Success

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 i_{th} bit in the sequence, μ and σ^2 are the average and the variance of the sequence[15]. 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 length of 600000 bits to perform 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 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 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.

5 Conclusion

Motivated by the SI-QRNG based on the quantum optics, we propose and implement a source-independent and loss-tolerant QRNG scheme based on a cloud superconducting quantum computer. Due to the presence of noise and the imperfection of control mechanism, there exits errors in the preparation and readout of superposition state in the quantum computer which results in challenge to being a true random generator. By trusting the measurement operation, we propose the SI-QRNG scheme that can estimate the preparation error of superposition state in randomness source in real time, which guarantees the security of generated random numbers. In the quantum computer, the readout errors of $|0\rangle$ and $|1\rangle$ are generally different. Considering the condition, we further give the final extracted number of random bits. Considering the deviation of the rotation angle around the Y-axis and the axis of rotation, an estimation method for parameter e_z is given. Furthermore, we optimize the ratio of X-basis measurements q_x to increase the final random number generation rate. By utilizing the cloud superconducting quantum computer of IBM, we perform the SI-QRNG scheme and the practicability and effectiveness of our scheme are proved.. 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 NIST Statistical Test and autocorrelation test show that the final random numbers



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

Figure 7. The absolute value of autocorrelation function of the final data generated by *IBMQ_5_yorktown* and *IBMQ_lima*.

could be considered as true random numbers. Utilizing the SI-QRNG scheme, the conditional min-entropy of superconducting quantum computer can be monitored in real time, and we realize the generation of true random numbers in quantum computer with noise.

Author contributions

Y.-y. Fei, H. Wang and Z. Ma conceived the project. Y.-h. Li, W.-l. Wang and Y.-y. Fei performed the calculation and analysis. Y.-h. Li, X.-d. Meng and Q.-h. Duan wrote the paper. All authors reviewed the manuscript.

Funding

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).

References

1. Shannon, C. E. Communication theory of secrecy systems. *The Bell System Technical Journal* **28**, 656–715 (1949). DOI 10.1002/j.1538-7305.1949.tb00928.x.

2. Metropolis, N. & Ulam, S. The monte carlo method. *Journal of the American Statistical Association* **44**, 335–341 (1949). URL https://www.tandfonline.com/doi/abs/10.1080/01621459.1949.10483310. DOI 10.1080/01621459.1949.10483310. PMID: 18139350.

3. Pangratz & Weinrichter. Pseudo-random number generator based on binary and quinary maximal-length sequences. *IEEE Transactions on Computers* **C-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. *Nature Photonics* **9**, 772–773 (2015).

6. Wayne, M. A. & Kwiat, P. G. Low-bias high-speed quantum random number generator via shaped optical pulses. *Opt. Express* **18**, 9351–9357 (2010). URL http://www.opticsexpress.org/abstract.cfm?URI=oe-18-9-9351. DOI 10.1364/OE.18.009351.

7. Fürst, H. *et al.* High speed optical quantum random number generation. *Opt. Express* **18**, 13029–13037 (2010). URL http://www.opticsexpress.org/abstract.cfm?URI=oe-18-12-13029. DOI 10.1364/OE.18.013029.

8. Wahl, M. *et al.* An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements. *Applied Physics Letters* **98**, 145–266 (2011).

9. Gabriel, C. *et al.* A generator for unique quantum random numbers based on vacuum states. *Nature Photonics* **4**, 711–715 (2010).

10. 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).

11. Zhou, Q., Valivarthi, V. R. R., John, C. & Tittel, W. Practical quantum random number generator based on sampling vacuum fluctuations. *Quantum Engineering* (2017).

12. Xu, F. *et al.* Ultrafast quantum random number generation based on quantum phase fluctuations. *Optics Express* **20**, 12366 (2012).

13. 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). URL http://ol.osa.org/abstract.cfm?URI=ol-35-3-312. DOI 10.1364/OL.35.000312.

14. Wei, S. *et al.* Compact quantum random number generator based on superluminescent light-emitting diodes. *Review of Scientific Instruments* **88**, 123115 (2017).

15. Wei, W., Xie, G., Dang, A. & Hong, G. High-speed and bias-free optical random number generator. *IEEE Photonics Technology Letters* **24**, 437–439 (2012).

16. Alexeev, Y. *et al.* Quantum Computer Systems for Scientific Discovery. *P. R. X. Quantum.* **2**, 017001 (2021). DOI 10.1103/PRXQuantum.2.017001. 1912.07577.

17. Dicarlo, L. *et al.* Demonstration of two-qubit algorithms with a superconducting quantum processor. *Nature* **460**, 240–4 (2009).

18. Devoret, M. H. & Schoelkopf, R. J. Superconducting circuits for quantum information: An outlook. *Science* **339**, 1169–1174 (2013). URL https://science.sciencemag.org/content/339/6124/1169. DOI 10.1126/science.1231930. https://science.sciencemag.org/content/339/6124/1169.full.pdf.

19. Zu, C. *et al.* Experimental realization of universal geometric quantum gates with solid-state spins. *Nature* **514**, 72 (2014).

20. Jelezko, F., Gaebel, T., Popa, I., Gruber, A. & Wrachtrup, J. Observation of coherent oscillations in a single electron spin. *Physical Review Letters* **92**, 076401 (2004).

21. Knill, E., Laflamme, R. & Milburn, G. J. A scheme for efficient quantum computation with linear optics. *Nature* **409**, 46–52 (2001).

22. Preskill, J. Quantum Computing in the NISQ era and beyond. *Quantum* **2**, 79 (2018). URL https://doi.org/10.22331/q-2018-08-06-79. DOI 10.22331/q-2018-08-06-79.

23. LaRose, R. Overview and Comparison of Gate Level Quantum Software Platforms. *Quantum* **3**, 130 (2019). URL https://doi.org/10.22331/q-2019-03-25-130. DOI 10.22331/q-2019-03-25-130.

24. 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).

25. Pironio, S. *et al.* Random numbers certified by bell's theorem. *Nature* **464**, 1021 (2010).

26. Christensen, B. G., Mccusker, K. T., Altepeter, J. B., Calkins, B. & Kwiat, P. G. Detection-loophole-free test of quantum nonlocality, and applications. *Physical Review Letters* **111**, 130406 (2013).

27. Colbeck, R. & Kent, A. Private randomness expansion with untrusted devices. *Journal of Physics A Mathematical and Theoretical* **44** (2010).

28. Bowles, J., Quintino, M. T. & Brunner, N. Certifying the dimension of classical and quantum systems in a prepare-and-measure scenario with independent devices. *Physical Review Letters* **112**, 140407 (2013).

29. Cao, Z., Zhou, H. & Ma, X. Loss-tolerant measurement-device-independent quantum random number generation. *New Journal of Physics* **17**, 125011 (2015).

30. Ma, J., Hakande, A., Yuan, X. & Ma, X. Coherence as a resource for source-independent quantum random-number generation. *Physical Review A* **99** (2019).

31. Zhang, J., Zhang, Y., Zheng, Z., Chen, Z. & Yu, S. Finite-size analysis of continuous variable source-independent quantum random number generation. *Quantum Information Processing* **20** (2021).

32. Michel, T. *et al.* Real-time source independent quantum random number generator with squeezed states. *Physical Review Applied* **12** (2019).

33. Cao, Z., Zhou, H., Yuan, X. & Ma, X. Source-independent quantum random number generation. *Phys. Rev. X* **6**, 011020 (2016). URL https://link.aps.org/doi/10.1103/PhysRevX.6.011020. DOI 10.1103/PhysRevX.6.011020.

34. Marco Avesani, M., G., D., Vallone, G. & Villoresi, P. Source-device-independent heterodyne-based quantum random number generator at 17 gbps. *Nature Communications* **9** (2018).

35. Landauer, R. Irreversibility and heat generation in the computing process. *IBM Journal of Research and Development* **5**, 183–191 (1961). DOI 10.1147/rd.53.0183.

36. Ma, X., Fung, C.-H. F., Boileau, J.-C. & Chau, H. Universally composable and customizable post-processing for practical quantum key distribution. *Computers & Security* **30**, 172–177 (2011). URL https://www.sciencedirect.com/science/article/pii/S0167404810001021. DOI https://doi.org/10.1016/j.cose.2010.11.001.

37. Impagliazzo, R., Levin, L. & Luby, M. Pseudorandom number generation from one-way functions (1989).

38. Fung, C.-h. F., Tamaki, K., Qi, B., Lo, H.-K. & Ma, X. Security proof of quantum key distribution with detection efficiency mismatch. *Quantum Info. Comput.* **9**, 131–165 (2009).

39. Ma, D., Wang, Y. & Wei, K. Practical source-independent quantum random number generation with detector efficiency mismatch. *Quantum Information Processing* **19**, 384 (2020).

40. IBM, Q. https://quantum-computing.ibm.com/ (2021).

41. Aleksandrowicz, G. *et al.* Qiskit: An Open-source Framework for Quantum Computing (2019). URL https://doi.org/10.5281/zenodo.2562111.

42. Ma, X. *et al.* Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. *Phys. Rev. A* **87**, 062327 (2013).

43. 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. *NIST Special Publication 800-22* (2010).

Figures

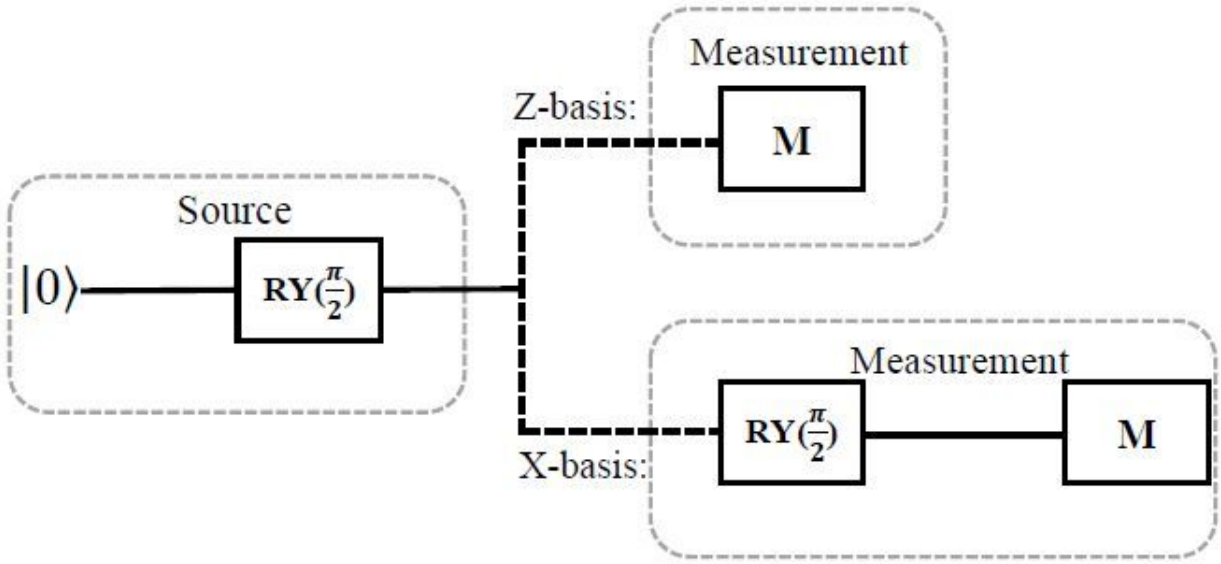


Figure 1

Quantum circuits for the proposed SI-QRNG. The qubit state is randomly measured in the X-basis or Z-basis.

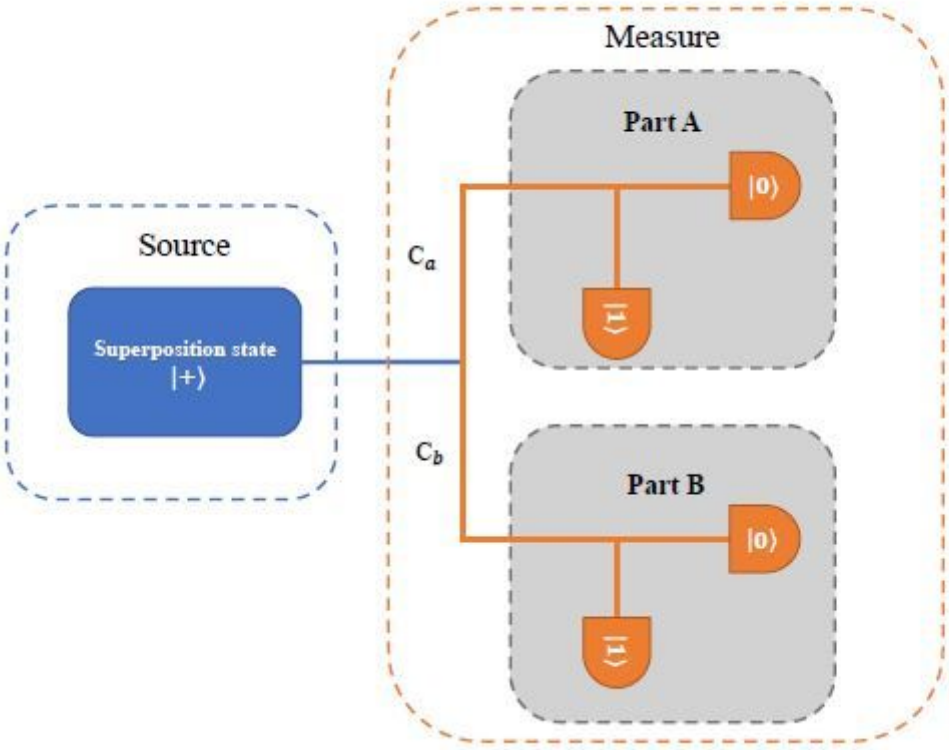


Figure 2

Equivalence of SI-QRNG under the different readout errors of quantum state.

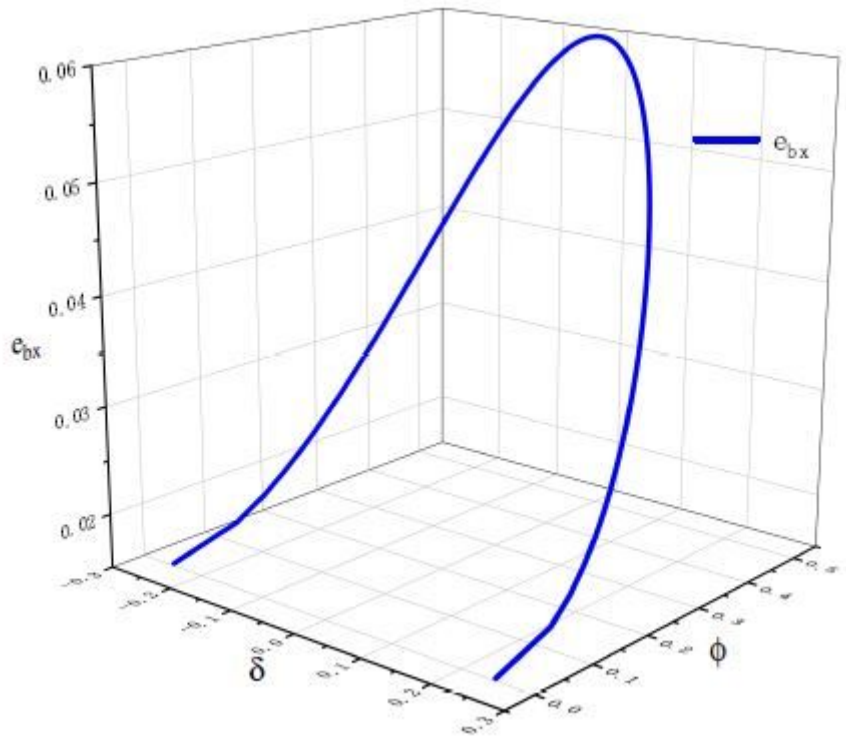


Figure 3

please see the manuscript file for the full caption

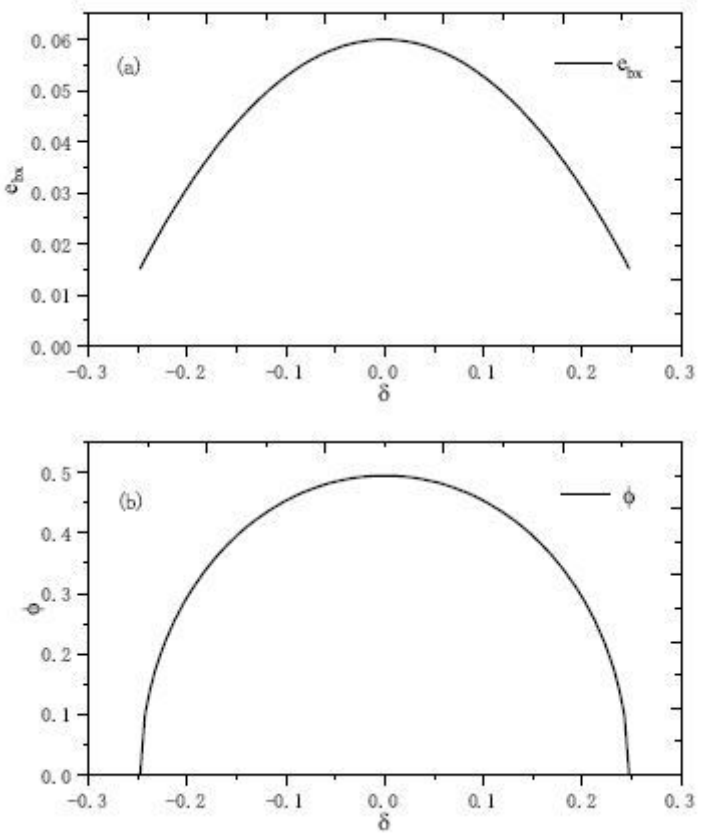


Figure 4

(a) Projection of the xz plane of Fig. 3. Relationship between rotation angle error d and preparation error of j+i state ebx, (b) Projection of the xy plane of Fig. 3. Relationship between errors in the rotation angle around Y-axis d and Z-axis f.

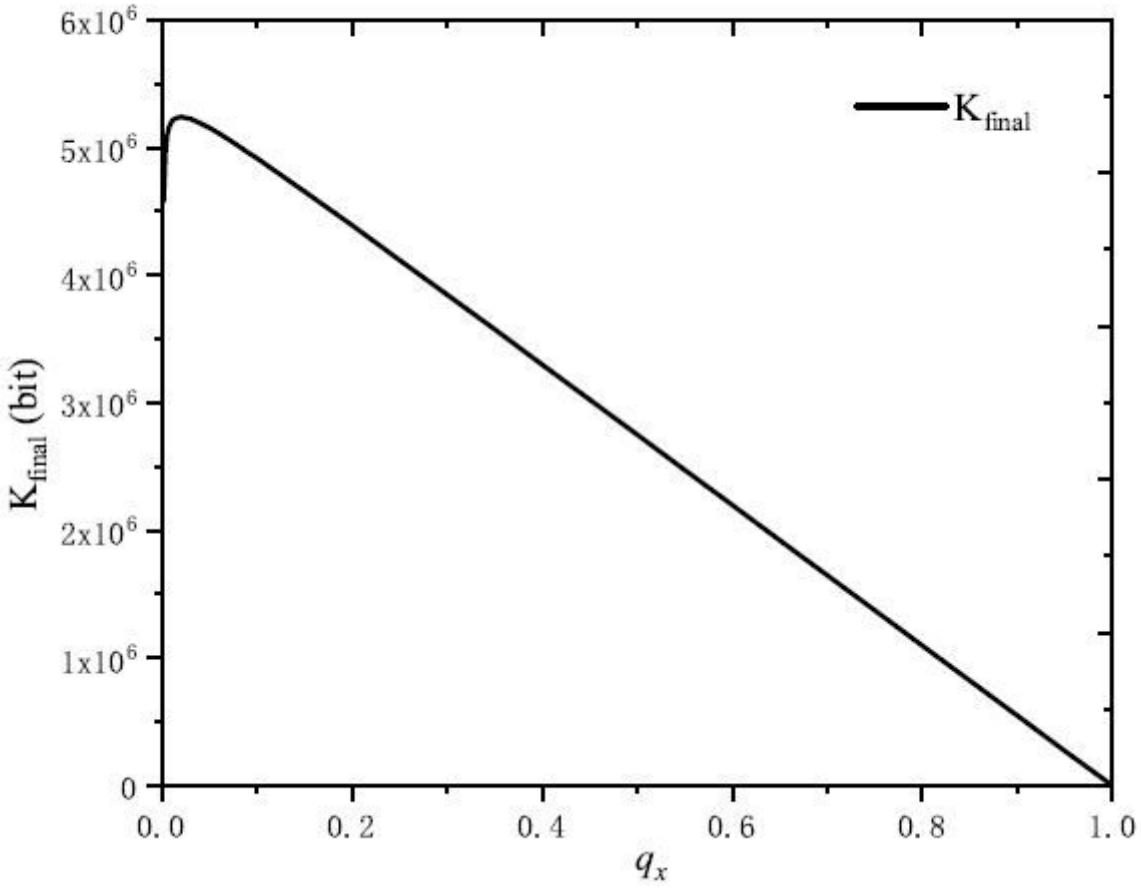


Figure 5

Relationship between basis choice rate qx and final extracted random bits Kf inal . Here, we set ebx = 0:05, r0 = 0:05, r1 = 0:1 and n = 8:192*106.

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

Figure 6

Device topology of IBMQ 5 yorktown and IBMQ lima.

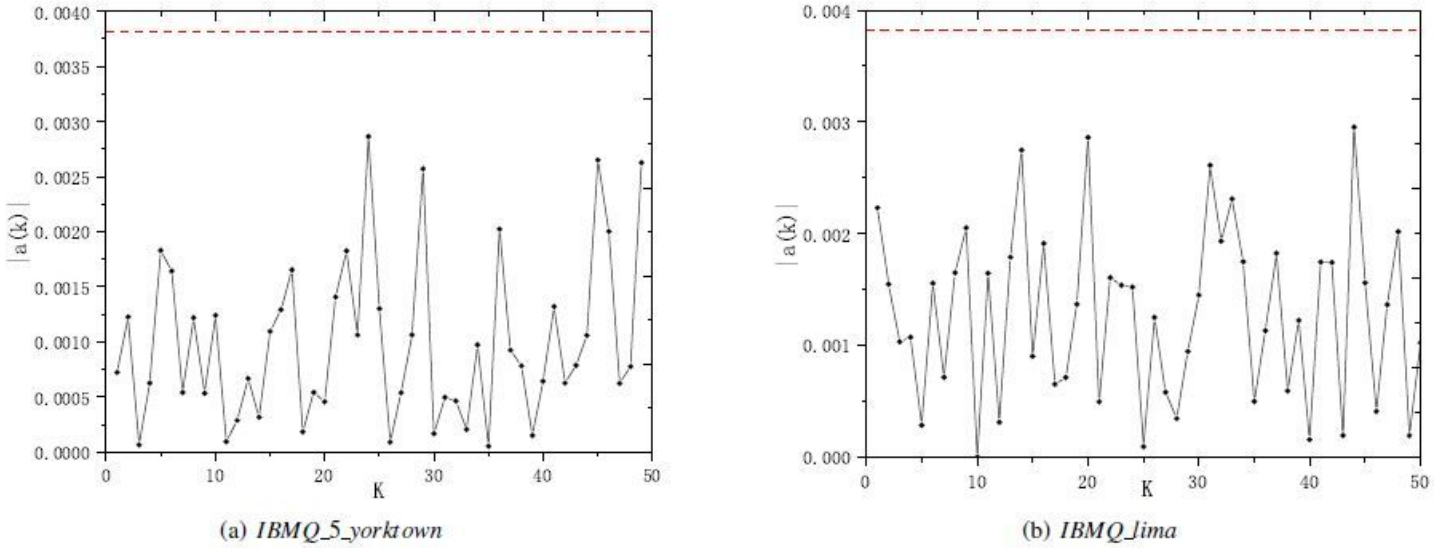


Figure 7

The absolute value of autocorrelation function of the final data generated by IBMQ 5 yorktown and IBMQ lima.