An Unbiased Quantum Random Number Generator Based on Boson Sampling

Jinjing Shi,* Tongge Zhao, Yizhi Wang, Chunlin Yu, Yuhu Lu, Jiajie Wu, Ronghua Shi, Shichao Zhang, Shaoliang Peng,* and Junjie Wu*

It is proven that Boson sampling is a much promising model of optical quantum computation, which is applied to designing quantum computer successfully, such as “Jiuzhang”. However, the meaningful randomness of Boson sampling results has not been utilized or exploited. In this research, Boson sampling is applied to design a quantum random number generator (QRNG) by fully exploiting the randomness of Boson sampling results, and its prototype system is constructed with the programmable silicon photonic processor, which can generate unbiased random sequences and overcome the shortcomings of the existing discrete QRNGs such as source-restricted, high demand for the photon number resolution capability of detector and slow self-detection generator speed. Boson sampling is implemented as a random entropy source, and random bit strings with satisfactory randomness and uniformity can be obtained after post-processing the sampling results. It is the first approach for applying the randomness of Boson sampling results to develop a practical prototype system for actual tasks, and the experiment results demonstrate that the designed Boson sampling-based QRNG prototype system passes 15 tests of the NIST SP 800-22 statistical test component, which proves that Boson sampling has great potential for practical applications with desirable performance besides quantum advantage.

J. Shi, T. Zhao, Y. Lu, R. Shi, S. Zhang
School of Electronic Information
Central South University
Changsha 410083, P. R. China
E-mail: shijinjing@csu.edu.cn
T. Zhao, C. Yu, J. Wu
China Greatwall Technology Group Co., Ltd
China Greatwall Research Institute
Shenzhen 518057, P. R. China
Y. Wang, J. Wu
Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer Science and Technology
National University of Defense Technology
Changsha 410073, P. R. China
E-mail: junjiewu@nudt.edu.cn
S. Peng
College of Computer Science and Electronic Engineering
Hunan University
Changsha 410082, P. R. China
E-mail: slpeng@hnu.edu.cn

1. Introduction

Random numbers play an important role in different kinds of applications and provide essential resources,[1] such as cryptography,[2] lottery industry,[3] genetics, scientific simulations,[4,5] etc. While the generation of good randomness is an obviously difficult problem.[6] In the classical field, there are many random number generator (RNG) schemes, most of which involve deterministic algorithms and start from a small bit string called seed, such as the linear congruential RNG based on number theory,[7] the Mersenne Twister based on linear shift feedback registers,[8] etc. Those schemes can simply generate random numbers at an advantage effective rate, while they cannot be considered as true RNGs, called pseudorandom number generators (PRNGs). When the small string random seed is leaked, the random numbers generated by those schemes may be exactly known. The important requirement for the unpredictability of random number generators limits the application scope of classical PRNGs.

Fortunately, the intrinsic randomness of quantum physics makes quantum systems a good source of RNG,[9] and many quantum random number generators (QRNGs)[10] are proposed, including Branching path generator,[11] Photon counting generator,[12] etc. Branching path generator generates random numbers by measuring the path superposition state or polarization superposition state,[13] which depends on the input source that once the superposition state is controlled by a third-party, the measurement result may be controlled as well. Photon counting generator obtains the random number by detecting the photon number of the coherent states,[12] whose efficiency depends on the dead time and the photon resolving capability of photon detectors. The non-local correlation between two particles can also generate the randomness,[11] which provides an important resource in RNG protocols, like randomness expansion,[14,15] and random amplification.[16] These methods for constructing QRNGs are called device independent or self-testing QRNGs,[17–19] while their generation bit rate is relatively slow that they lack wide applications. In general, discrete QRNGs still have the following possible problems: source-restricted, high demand for the photon number resolution capability of the detector.
and slow self-detection generator speed. Thus, the principle and implementation of QRNGs need to be improved urgently, and more and more new methods are expectedly proposed to design QRNGs.\textsuperscript{20–22}

On the other hand, at the very beginning of noisy intermediate-scale quantum (NISQ) era,\textsuperscript{23} quantum supremacy\textsuperscript{24} has been proposed that certain computing tasks may be executed exponentially faster on current quantum computers than on classical computers.\textsuperscript{25} Boson sampling is considered as a powerful candidate for experimental verification of quantum supremacy\textsuperscript{26} which samples the probability distribution generated by the evolution of single photons through a linear optical network including phase shifters and beam splitters. The application of Boson sampling has attracted the attention of researchers,\textsuperscript{27,28} e.g., Boson sampling-based one-way function,\textsuperscript{29} Boson sampling-based random unitary encryption\textsuperscript{30} and Boson sampling-based hash function\textsuperscript{31} have been proposed, respectively. The branches of applications of Boson sampling shorten the research process of solving practical problems with Boson sampling. However, the meaningful randomness of Boson sampling results, whose correctness and significance were proved from a specific quantum mechanical distribution,\textsuperscript{32} has not been fully utilized or exploited.

We are so excited to discover that there are three favorable factors for taking advantages and exploiting the randomness of Boson sampling to design QRNG. First, the Boson sampling result is a superposition state before the photon output detection that the output is random and has no strict restriction on the input state. Second, we merely need a normal single-photon detector instead of a photon number resolver in concluding the output of Boson sampling since we only concern whether a mode has photons instead of the specific number of photons. Third, it is possible to generate multi-bit random numbers for sampling only once with multi-mode Boson sampling, which may be more efficient compared to the generators for single-bit random numbers with one sampling. Moreover, the Boson sampling-based QRNG corresponding to above three factors is capable to overcome the defects of the existing QRNGs for the requirements of reliable safe input source, high photon number resolution and improved bit rate potentially. Boson sampling is a sampling problem that is closely related to random number generation indeed. As early as 1999, Petrie et al. electronically amplified and sampled natural phenomena such as heat or shot noise signals to generate random numbers.\textsuperscript{33} Zhou et al. sampled vacuum fluctuations to design practical quantum random number generation.\textsuperscript{34} In 2021, Bai et al. performed homodyne detection and sampling on the vacuum state to realize the fastest and miniaturized QRNG at present.\textsuperscript{35} In the field of experiments, many ingenious experiments have implemented small-scale Boson sampling.\textsuperscript{36,37} At the same time, the Boson sampling model has also been extended, i.e., Scattershot Boson sampling,\textsuperscript{38} Lossy Boson sampling,\textsuperscript{39,40} Gaussian Boson sampling\textsuperscript{41,42} etc. In 2019, Wang et al. realized the 20-photons 60-modes Boson sampling experiment.\textsuperscript{43} In 2020 and 2021, quantum computing prototypes jiuzhang and jiuzhang 2.0 were proposed,\textsuperscript{44,45} respectively, which proved the advantages of quantum computing in the optical quantum system.

In order to overcome the above shortcomings of the existing QRNGs and in the interest of fully exploiting the randomness of Boson sampling results, we present an exploratory work in this paper to utilize Boson sampling as an entropy source to generate quantum random numbers, where the sampling results have no strict restriction on the input state, only a normal single-photon detector is required without photon number resolution, and the generator is quite efficient and effective with ideal post-processing. The Von Neumann correction method for post-processing is applied to generate uniform and unbiased random numbers. A Boson sampling-QRNG prototype system is constructed with the programmable silicon photonic processor to implement the experiments for NIST SP 800-22 statistical test\textsuperscript{46} of the proposed scheme.

The rest of this paper is organized as follows. A brief review of Boson sampling and QRNGs using optical systems are introduced in Section 2. And then, we propose the scheme of Boson sampling-based QRNG and construct a Boson sampling-based QRNG prototype system using the programmable silicon photonic processor in Section 3. In Section 4, experiments on the Boson sampling-based QRNG prototype system are conducted to implement NIST SP 800-22 statistical test for the proposed scheme. In Section 5, the performance and advantages of the method are analyzed. Finally, this research is concluded in Section 6.

2. Preliminaries

In this section, we first briefly review the basic knowledge of Boson sampling, and then introduce the design methods of using quantum optical systems to construct QRNGs.

2.1. Boson Sampling Model

The problem of Boson sampling is proposed by Aaronson and Arkhipov in 2013,\textsuperscript{26} claiming that the Fock state is input into the passive linear optical interferometer, and the output distribution is sampled with the photon detectors, as shown in the Figure 1a. Without the exponential cost of time or resources, the sampling outcome cannot be predicted with a classical computer.\textsuperscript{47,48} For Boson sampling model of m modes linear transformation and n indistinguishable Bosons, the output probability is calculated by a tricky matrix function called permanent

\begin{equation}
P_{1,O} = |\langle O| U \otimes U \cdots \otimes U |1\rangle|^2 = \frac{\left| \text{Per}(U_{1,O}) \right|^2}{j_1 j_2 \cdots j_m n_1 n_2 \cdots n_m}
\end{equation}

where \( |1\rangle = |j_1 j_2 \cdots j_m\rangle \) is the input state satisfying \( j_1 + j_2 + \cdots + j_m = n \), i.e., the number of photons input to the i-th mode, \( |O\rangle = |g_1 g_2 \cdots g_m\rangle \) is the output state, \( U_{1,O} \) is the sub-matrix of the unitary transformation matrix \( U \) for the linear optical interferometer.

2.2. Quantum Random Number Generator

The uncertainty of quantum systems is guaranteed by the inherent randomness of quantum physics, where true randomness is a basic feature of quantum mechanics.\textsuperscript{49} With the development of
quantum optics, the inherent randomness in many parameters of the quantum states of light provides options for the realization of QRNGs.\textsuperscript{10}

Branching path QRNGs generate random numbers based on the measurement of path superposition state. The light source is input into a balanced beam splitter, where the transmittance and reflectivity are equal. The output is zero when \( D_1 \) detects a photon, and the output is one when \( D_2 \) detects a photon,\textsuperscript{9} as shown in the Figure 1b. Photon counting QRNGs generate random numbers based on the number of photons detected on the coherent state.\textsuperscript{12} Coherent states can be described as a superposition of fock states

\[
|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle
\]  

(2)

where \( \alpha \) is a complex number, the amplitude \( |\alpha|^2 \) corresponds to the mean photon number of the state. The number of photons arriving at the detector in a fixed time follows a Poisson distribution. The probability of detecting \( n \) photons in \( T \) time is

\[
P(n) = \frac{(\lambda T)^n}{n!} e^{-\lambda T}
\]  

(3)

Boson sampling can be handled with optical quantum systems, of which the necessary elements can be implemented with the current technologies, i.e., sources, linear evolution, and detection. The result of Boson sampling is random and can be used as a method of realizing a QRNG.

3. Quantum Random Numbers Generator Based on Boson Sampling

In this section, we describe the overall scheme and individual modules of the Boson sampling-based QRNG. The Boson sampling-based QRNG prototype system is constructed on a programmable silicon photonic processor.

3.1. The Scheme of Boson Sampling-Based QRNG

The QRNGs are divided into well-defined independent modules according to their functions, as shown in Figure 2a, where the most important parts are the entropy source and the post-processing. The entropy source is composed of a quantum system and measurement operations to output initial random data. Since noise exists in the entire system and the measurement process, the initial random data is not necessarily in the form of random bits. Therefore, post-processing operations are required, such as encoding, random extraction, random amplification, etc., ensuring the random sequence obtained at the final output can become a uniform random number sequence with unbiased and independent bit 0 and bit 1. The post-processing step processes and filters the generated original quantum information to eliminate potential deviations and correlations and further enhance randomness.

In the Boson sampling-based QRNG scheme, we designed, five major components are included as described in Figure 2b, i.e., input Boson source, linear optical network, photon detection, post-processing, and output. The entropy source is described by the Boson sampling, in which the quantum system is composed of the input Boson source and the linear optical network, and the measurement process is detected by the photon detectors.

With high probability, the Boson sampling distribution created by a haar-random matrix \( U \) is far away from the uniform distribution.\textsuperscript{50} The Von Neumann correction method\textsuperscript{51} as shown in Table 1 is applied to the random numbers obtained directly from the Boson sampling to get a completely uniform and unbiased random binary bit sequence. The specific steps of the post-processing are summarized as follows.

Step 1 Perform a Boson sampling and record the sampling result as \( S_1 \).

Step 2 Perform Boson sampling again and record the result as \( S_2 \).

Step 3 Comparing \( S_1 \) with \( S_2 \), the output code of a mode is 0 bit if it detects photon in \( S_1 \) but does not detect photon in \( S_2 \). Similarly, a mode does not detect photon in \( S_1 \) but detects photon in \( S_2 \), then the output code of this mode is 1 bit. No coding in other cases.

Step 4 The coded bits of the modes numbered 1 to \( M \) are output in order to obtain the result of the random number generator.

Step 5 Repeat Step 1 to Step 4 until the required number of random numbers are generated.
Figure 2. a) Block structure of QRNG. The block structure consists of the entropy source and the post-processing. The entropy source includes the quantum system and the measurement process, generating the initial random numbers. The post-processing ensures the random number sequence can be uniform and unbiased with 0 bit and 1 bit derived on equal probability. b) The structure of Boson sampling-based QRNG. The sampling results are post-processed with Von Neumann correction method to obtain a uniform 01-bit sequence.

Table 1. The post-processing with the Von Neumann correction method

| mode | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | ... | MM |
|------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|
| The first sampling result $S_1$ | ⬤ | ⬤ | ◯ | ⬤ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ... | ◯ |
| The second sampling result $S_2$ | ◯ | ⬤ | ◯ | ⬤ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ... | ⬤ |
| Coding | 0 | * | * | 0 | 1 | * | 0 | 1 | * | 1 | * | 0 | ... | 1 |
| The final random number sequence | 0010110...1 |

○ represents one or more photons is detected ◯ represents no photon is detected

3.2. The Boson Sampling-Based QRNG Prototype System

We have constructed a QRNG prototype system using the programmable silicon photonic processor\cite{52} and observed two Bosons sampling statistics after a five-mode Haar random unitary process $U_5$, as shown schematically in Figure 3. To simulate a state of two Bosons created in modes 1 and 2, we first generate the two-photon entangled state

$$\frac{1}{\sqrt{2}}(|1⟩_s|2⟩_i + |2⟩_s|1⟩_i)$$

(4)

where $|k⟩ (k = 1, 2, 3, 4, 5)$ denotes the path of a photon, $s$ and $i$ denote the signal and idler photon from coherently generated photon pairs. Each photon is then routed to a universal linear optical network, which applies the unitary transformation $U_5$ with fixed input. Finally, photons are detected off the chip, and two-photon coincidence events are recorded, from which we extract the correlated detection probability $P_{rq}$ of measuring a photon at output $r$ and $q$ of two networks, respectively. According to the simulating scheme, we obtain $\Gamma_{rq}$, the probability to measure two Bosons occupying modes $r$ and $q$ after the unitary process $U_5$, as $\Gamma_{rq} = P_{r,q}$ (shown in the Figure 4a).

4. Experiments and Results

In this subsection, we use the Boson sampling-based QRNG prototype system to experimentally generate random numbers. Furthermore, the statistical test suite is performed on the random numbers obtained from experiments to test the randomness.

4.1. Experimental Setup

Bright light with the wavelength of 1549.3 nm is collected from a continuous-wave tunable laser and further amplified up to 50 mW using an optical erbium-doped fiber amplifier. After spectrally filtered by a dense wavelength division multiplexing module and tuned by a polarization controller, the bright light is then injected into the silicon photonic chip (shown in Figure 3) via a V-Groove fiber array. The chip mainly integrates two spontaneous four-wave mixing spiral sources, 22 simultaneously running thermo-optic phase shifters, 32 multimode interferometer beam splitters, and 16 optical grating couplers. The two SFWM sources are pumped by 50:50 split laser and create possible (signal-idler) maximally entangled photon pairs. The two five-mode universal linear optical networks comprised of beam splitters and phase shifters arranged in Reck et al.-style are used to...
Figure 3. The programmable silicon photonic processor chip. The silicon chip integrates two functional parts: i) creating two-photon entangled state through spontaneous four-wave mixing (SFWM) and ii) applying arbitrary 5D unitary transformations with fixed inputs through configurable linear optical networks.

Figure 4. a) The theoretical probability distribution and experimental probability distribution of each output state. b) The experimental results pass the 15 tests of the NIST SP 800-22 random number statistical tests. The $P$-value of each test is greater than the confidence level $\alpha = 0.01$.

Implement arbitrary five-mode unitary transformation with fixed inputs. In our prototype demonstration, we apply a Haar-random generated unitary operator $U_5$ as

$$
0.0131 + 0.3301 \ast I \\
0.1475 + 0.4779 \ast I \\
0.3235 + 0.0451 \ast I \\
0.3581 - 0.4678 \ast I \\
-0.3111 + 0.3001 \ast I
$$

Photons from different chip outputs are collected by the same fiber array and detected by superconducting nanowire single-photon detectors. With the coincidence counting logic, two-photon coincidences are recorded by using a time-interval-analyzer in a 468.75ps integration window. During the continuous running time, a total of 914286 two-photon coincidence events are recorded.

4.2. Standard Statistical Randomness Test

A total of 1.8772 Mbit 01bit sequences were obtained after post-processing using the Von Neumann correction method, where

the probabilities of 0 and 1 bit are 0.49999814 and 0.50000186, respectively, implementing an unbiased distribution of random number sequences. We use the NIST SP 800-22 statistical test suite to test the randomness, which is based on hypothesis testing, containing 15 tests in total, as shown in Table 2. A $p$-value is calculated for each test item summarizing the degree of evidence rejecting the null hypothesis, which is the function of...
data. Choosing the significance level \( \alpha = 0.01 \), if the \( p \)-value obtained by the statistical test is greater than or equal to 0.01, it indicates that the sequence has passed the test, and the resulting sequence is random. If the \( p \)-value is less than 0.01, it indicates that the sequence has failed the test. The \( p \)-values of all test items are showed in Figure 4b, which are all greater than 0.01, indicating that the bit sequence obtained by the experiment has superior performance at random.

5. Discussion

In this section, we describe the influence of circuit parameters on QRNG randomness, and analyze some attractive properties of the Boson sampling-based QRNG.

5.1. Influence of Boson Sampling Circuit Parameters on Randomness

We use mathematical entropy function to measure the uncertainty and randomness of the Boson sampling circuit output in the information theory, where different entropy values reflect the degree of surprise for the result. Shannon entropy is calculated as \( H(A) = -\sum_{\alpha \in \mathcal{X}} P_{\alpha}(a) \log_{2} P_{\alpha}(a) \), where \( P_{\alpha}(a) \) is the probability distribution of random variable \( A \), \( P_{\alpha}(a) \) is the probability of getting output \( \alpha \), and \( \mathcal{X} \) is a discrete set of values of random variable \( A \). \( \text{Rényi entropy} \) is an extension of the usual Shannon entropy. The \( \text{Rényi entropy} \) of order \( \beta \) is calculated as \( H_{\beta}(A) = \frac{1}{1-\beta} \log_{2} \sum_{\alpha \in \mathcal{X}} P_{\alpha}(a)^{\beta} \). When \( \beta \rightarrow 1 \), the \( \text{Rényi entropy} \) corresponds to Shannon entropy. When \( \beta \rightarrow \infty \), the \( \text{Rényi entropy} \) corresponds to the Min-entropy. In another way, the Min-entropy \( H_{\infty} \) can be defined as \( H_{\infty} = -\log_{2} \max_{\alpha \in \mathcal{X}} P_{\alpha}(a) \). 2\(^{-H_{\infty}}\) describes the probability of hitting the first guess from a random variable \( A \) with a known probability distribution.

In the case of fixed input Boson sampling, different linear interferometer unitary matrices are constructed to obtain the output probability distribution of Boson sampling by adjusting the rotation parameters of the linear optical network phase shifters. As shown in Figures 5 and 6, the Shannon entropy and Min-entropy of the Boson sampling output distribution vary with different circuit parameters in the range of \([0, 2\pi]\). The parameters of the 11 and 21 interferometers have a greater impact on the randomness of the circuit output probability distribution, which are the first optical device that the photons entering the optical network from the light source needed to pass. The general trend of each entropy curve is ascending, descending, ascending, descending, and repeating. The experimental results show that for a fixed input five modes two photons Boson sampling, the randomness of the output of the Boson sampling system can be effectively increased by selecting appropriate linear optical network parameters to improve the random numbers generation rate of Boson sampling-based QRNG.

5.2. Performance Analysis

The output probability distribution of Boson sampling is not close to the uniform distribution in variation distance,\(^{(50)}\) which is the advantage of Boson sampling compared with other sampling distributions. A uniform distribution of 01 bits in the output sequence is an important feature required by the random number generator, where the probability of each bit being 0 or 1 is both 0.5, which is unbiased (otherwise the possibility of “guessing” successfully increases). The Von Neumann correction method is used to achieve unbiasedness in the proposed scheme. However, we have not changed the output probability distribution generated by Boson sampling, which is still far from the uniform distribution. After finishing the post-processing, the probability of each mode coded as 0 and 1 is equivalent, the 01 bits in the final random number sequence are also a uniform distribution at the same time. Different from other schemes that directly change the probability distribution of quantum systems, this scheme has the advantage that it retains the non-uniform distribution of boson sampling. Besides, the Boson sampling-based QRNG composed of physical devices can generate real quantum random numbers in principle, guaranteeing the security of the QRNG proposed in this paper. In addition, the Boson sampling-based QRNG has several attractive properties.

5.2.1. Unpredictability

The entire system is in a superposition state of \( |\psi_{\text{out}}\rangle = \sum \lambda_{i} |n_{1}, n_{2}, \ldots, n_{m}\rangle \) before being detected by photon detectors, the measurement may destroy the coherence of the superposition state. According to the Born rule,\(^{(54)}\) when a quantum superposition state is observed and measured, the probability that the state collapses at a specified position is proportional to the square of the coefficient of the state. The measurement result of a quantum system is related to probability, which can never be predicted better than blindly guessing. At the same time, Boson sampling is a process of sampling in the probability distribution obtained by the evolution of the Boson through the beam splitters and the phase shifters, where the final output result is random and unpredictable. Although the experiment scale is not very large, the random numbers generated by the prototype system come from
Figure 5. a–j) present the curves of Shannon entropy and Min-entropy changing with circuit rotation angle parameters $\theta_2, \theta_1, \theta_1E, \theta_4, \theta_3, \theta_3E, \theta_5, \theta_5E, \theta_8I$, respectively.

Figure 6. a) denotes the curves of Shannon entropy changing with circuit rotation angle parameters. b) denotes the curves of Min-entropy changing with circuit rotation angle parameters.

the Boson sampling device with significant quantum random characteristics, where the output results are unpredictable and completely different from the pseudo-randomness of the classical theory, ensuring the security of this QRNG.

5.2.2. No Strict Restriction on the Input State

In the traditional QRNGs, the random numbers are generated by three stages: input source, measurement operation, and post-processing, where the original input source of QRNGs must be fully trusted. If the input source is controlled by a third-party, for example, he/she fixes your source to a combination sequence of ground state $|0\rangle$ and $|1\rangle$ instead of the superposition state $|+\rangle$, when measuring the state on the Z basis, you may “look” to get “random” 0 and 1 bits, which are controlled by the third-party. In the proposed Boson sampling-based QRNG, a haar random linear optical network is placed between the initial input source and the measurement operation, where the Boson source can be detected and measured by the photon detectors at the output modes after the evolution of the interference. Since the output state is an
unknown superposition state ensured by the interference effect, the result obtained after the measurement cannot be completely determined. In addition, we can also increase the random sampling process before post-processing. Perform boson sampling $T$ times to obtain $T$ sample sets ($T > 2$), from which two sets of samples are randomly selected for post-processing to obtain the output sequence, avoiding the attack problems caused by continuously changing the input source. We change the input source to other states instead of $|11000\rangle$ state to simulate the situation that the input source is controlled by the third party. Evolving in the same unitary matrix of the linear optical network, the probabilities of 1 bit in the output random sequence are shown in Figure 7, where the obtained random numbers are still unbiased, which are independent of changing input sources. On the other hand, when the third-party controller alternately gives us different input sources, as shown in Figure 7, the probability of generating 1 bit in the random sequence has obvious deviations, which can be easily identified. The random bits will be discarded when there is a significant bias in the 01 bits. Therefore, regardless of whether the input source is mastered by a third-party, we can generate unbiased random numbers or identify the enemy and discard the generated random numbers, the proposed QRNG has no strict restriction on the input state.

**5.2.3. Uniform**

After the Von Neumann correction post-processing, the probability of getting 0 bit and 1 bit in the random number sequences can be equivalent. For the $x$-th output mode of Boson sampling, the probability of outputting 0 (1) bit is

$$P_x(0) = P_x(\text{detecting photon in } S_1) \times P_x(\text{not detecting photon in } S_2)$$

$$P_x(1) = P_x(\text{not detecting photon in } S_1) \times P_x(\text{detecting photon in } S_2)$$

In the case of the same input photon source and linear optical network, two consecutive Boson sampling experiments are independent, where $P_x(\text{detect photon in } S_1) = P_x(\text{detect photon in } S_2)$, so $P_x(0) = P_x(1)$. Therefore, the probability of 0 and 1 in the final random number sequence is both 50%, leading to a physically unbiased QRNG in this work.

**5.2.4. Unsimulateability**

The complexity theory analysis demonstrates that under the plausible conjectures about the permanent of i.i.d. Gaussian matrices,[26] the problems of accurate and approximate Boson sampling can not be effectively solved by classical computers unless

$$\text{PP} = \text{PostBQP} = \text{PostBPP} \subseteq \text{BPP}^{\text{NP}}$$

which means that the polynomial hierarchy collapses to the third level according to Toda’s theorem.[51] The output probability distribution of Boson sampling is calculated by the permanent of the unitary transformation matrix of the linear optical network, which is a $\#P – hard$ task on classical computer. The time complexity of the classic algorithm to calculate the matrix permanent is $O(2^n n^2)$, where the demand for classical computer resources exponentially increases with $n$.[56,57] The computational time and resources required to simulate a large-scale Boson sampling device with a classical computer increase exponentially with the number of photons, and the random numbers generated by large-scale Boson sampling cannot be effectively simulated with classical method.

**5.2.5. Multiphoton**

In the post-processing process, we only record whether a certain mode detects photons instead of the specific number of detected photons. Compared with the photon counting QRNGs using photon number resolution detectors,[12] the Boson sampling-based QRNG using single-photon detector is relatively easy to realize that it only requires a binary choice between no click (no photon has been detected) and click (one or more photons are detected). Most of the proposed Boson sampling-based applications rely on collision-free conditions ($n \ll m$), where the number of photons detected in each output mode is either 0 or 1.[26] The probability of detecting multiple photons in a mode at the output is almost zero. However, the probability of multiphoton in a mode gradually increases with non-collision-free conditions, seen Figure 8a. The scheme we proposed is not limited to collision-free conditions, where multi-photon and single-photon are handled at the same time in the post-processing, which is more universal.

**5.2.6. Multiple Random Bits**

Only one bit can be generated at a time in branching path QRNGs with limited generation rate. In the scheme mentioned in this
article, the linear optical network of Boson sampling has $m$ modes, each of which places a photon detector at the end. Multiple results of the presence or absence of photons can be obtained with one measurement. According to the post-processing principle, more than one random bit can finally be obtained through Boson sampling. We find that the Boson sampling-based QRNG generates random numbers at a faster rate and generates more random numbers at a time by simulating the number of random bits generated by QRNGs of single photon and Boson sampling with $M = 16$ and $N = 6$ respectively, as shown in Figure 8b.

6. Conclusion

An available and unbiased quantum random number generator has been proposed by fully exploiting the meaningful randomness of Boson sampling results, in which the sampling result of Boson sampling is encoded to generate binary random number sequences. The experimental results on the Boson sampling-based QRNG prototype system with programmable silicon photonic processor chip passed 15 NIST SP 800-22 statistical test component, indicating that the proposed QRNG scheme performs well in randomness. Performance analysis shows that this scheme can generate random numbers that are uniform, unbiased, unpredictable, and non-classical simulation to guarantee security and generate random numbers with multiple bits at a time to speed up the generation rate simultaneously, which can solve the problems of the existing discrete QRNGs for the high demand of reliable safe input source, strong photon number resolution, and improved bit rate potentially. In addition, this scheme inherits the merits of Boson sampling, making use of the randomness of Boson sampling results to develop a physical prototype system. This fact provides additional evidence that Boson sampling is capable of solving practical application problems besides quantum advantage. At the same time, it inspires more potential applications of Boson sampling in quantum devices, such as quantum key distribution (QKD), which can be implemented by the synchronization of Boson sampling.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant no. 62272483, 61972418), the National Science Foundation for Distinguished Young Scholars of Hunan Province (Grant no. 2023JJ10078), the Science and Technology Program of Shenzhen (Grant no. JCY20220818102014029), and the Scientific Research Program of Hunan Provincial Department of Education (22B0001).

Conflict of Interest

The authors declare no conflict of interest.

Data Availability Statement

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

Keywords

boson sampling, post-processing, quantum random number generator, randomness test

Received: June 19, 2023  
Revised: September 25, 2023  
Published online: October 25, 2023

[1] R. E. Caflisch, Acta Numer. 1998, 7, 1.  
[2] C. E. Shannon, The Bell syst. tech. j. 1949, 28, 656.  
[3] S. Chelkowski, A. D. Bandrauk, Phys. Rev. A 2010, 81, 062101.  
[4] S. Milz, K. Modi, PRX Quantum 2021, 2, 030201.  
[5] A. D. King, J. Raymond, T. Lanting, S. V. Isakov, M. Mohseni, G. Poulin-Lamarre, S. Ejtemaee, W. Bernoudy, I. Ozfidan, A. Y. Smirnov, M. Reis, F. Altmare, M. Babcock, C. Baron, A. J. Berkley, K. Boothby, P. I. Bunyk, H. Christiani, C. Enderud, B. Evert, R. Harris, E. Hoskinson, S. Huang, K. Jooya, A. Khodabandelou, N. Ladizinsky, R. Li, P. A. Lott, A. J. R. MacDonald, D. Marsden, et al., Nat. Commun. 2021, 12, 1.
[6] R. Shakirov, D. Sych, V. Sharoglazova, A. Udaltsov, A. Fedorov, Y. Kurochkin, Opt. Express 2020, 28, 6209.

[7] O. Scherzer, Handbook of mathematical methods in imaging, Springer Science & Business Media, Berlin 2010.

[8] M. Matsumoto, T. Nishimura, ACM Trans. Model. Comput. Simul. (TOMACS) 1998, 8, 3.

[9] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, H. Zbinden, J. Mod. Opt. 2000, 47, 595.

[10] M. Herrero-Collantes, J. C. Garcia-Escartin, Rev. Mod. Phys. 2017, 89, 015004.

[11] T. Jennewein, U. Aichler, C. Weis, H. Weinfurter, A. Zeilinger, Rev. Sci. Instrum. 2000, 71, 1675.

[12] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, C. Monroe, Nature 2010, 464, 1021.

[13] R. Colbeck, A. Kent, J. Phys. A: Math. Theor. 2011, 44, 095305.

[14] M. Coudron, H. Yuen, in Proceedings of the forty-sixth annual ACM symposium on Theory of computing, Association for Computing Machinery, New York, 2014, pp. 427–436.

[15] A. Prokhodtsov, K. Kovalyuk, P. An, A. Golikov, R. Shakirov, V. Sharoglazova, A. Udaltsov, Y. Kurochkin, G. Goltstein, in Journal of Physics: Conference Series, Vol. 1695, IOP Publishing, Bristol 2020, pp. 012118.

[16] J. Preskill, Quantum 2018, 2, 79.

[17] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, H. Neven, Nat. Physics 2018, 14, 595.

[18] A. W. Harrow, A. Montanaro, Nature 2017, 549, 203.

[19] S. Aaronson, A. Arkhipov, Theory Comput. 2013, 9, 143.

[20] J. Shi, T. Zhao, Y. Wang, Y. Feng, J. Wu, Adv. Quantum Technol. 2023, 6, 2200104.

[21] J. Shi, Y. Tang, Y. Lu, Y. Feng, R. Shi, S. Zhang, IEEE Transactions on Knowledge and Data Engineering, 2021.

[22] G. M. Nikolopoulos, Quantum Inf. Process. 2019, 18, 1.

[23] H. Wang, W. Li, X. Jiang, Y.-M. He, Y.-H. Li, X. Ding, M.-C. Chen, J. Qin, C.-Z. Peng, C. Schneider, M. Kamp, W.-J. Zhang, H. Li, L.-X. You, Z. Wang, J. P. Dowling, S. Höfling, C.-Y. Lu, J.-W. Pan, Phys. Rev. Lett. 2018, 120, 230502.

[24] S. Aaronson, D. J. Brod, Phys. Rev. A 2016, 93, 012335.

[25] C. S. Hamilton, R. Kruse, L. Sansoni, S. Barkhofen, C. Silberhorn, I. Jex, Phys. Rev. Lett. 2017, 119, 170501.

[26] M. Born, E. Wolf, Principles of Optics, third edition, Pergamon Press, 1960.

[27] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, C. Monroe, Nature 2010, 464, 1021.

[28] R. Colbeck, A. Kent, J. Phys. A: Math. Theor. 2011, 44, 095305.

[29] M. Coudron, H. Yuen, in Proceedings of the forty-sixth annual ACM symposium on Theory of computing, Association for Computing Machinery, New York, 2014, pp. 427–436.

[30] A. Prokhodtsov, K. Kovalyuk, P. An, A. Golikov, R. Shakirov, V. Sharoglazova, A. Udaltsov, Y. Kurochkin, G. Goltstein, in Journal of Physics: Conference Series, Vol. 1695, IOP Publishing, Bristol 2020, pp. 012118.

[31] J. Preskill, Quantum 2018, 2, 79.

[32] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, H. Neven, Nat. Physics 2018, 14, 595.

[33] A. W. Harrow, A. Montanaro, Nature 2017, 549, 203.

[34] S. Aaronson, A. Arkhipov, Theory Comput. 2013, 9, 143.

[35] J. Shi, T. Zhao, Y. Wang, Y. Feng, J. Wu, Adv. Quantum Technol. 2023, 6, 2200104.

[36] J. Shi, Y. Tang, Y. Lu, Y. Feng, R. Shi, S. Zhang, IEEE Transactions on Knowledge and Data Engineering, 2021.

[37] G. M. Nikolopoulos, Quantum Inf. Process. 2019, 18, 1.

[38] Y. Feng, R. Shi, J. Shi, W. Zhao, Y. Lu, Y. Tang, J. Phys. A: Math. Theor. 2020, 53, 135301.

[39] J. Shi, Y. Lu, Y. Feng, D. Huang, X. Lou, Q. Li, R. Shi, Quantum Inf. Process. 2022, 21, 1.

[40] P. Clifford, R. Clifford, in Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms, SIAM, Philadelphia 2018, pp. 146–155.

[41] C. S. Petrie, J. A. Connelly, in 1999 IEEE International Symposium on Circuits and Systems (ISCAS), Vol. 6, IEEE, Piscataway, NJ 1999, pp. 26–29.