6 Gbps real-time optical quantum random number generator based on vacuum fluctuation

Ziyong Zheng¹, Yichen Zhang¹, Weinan Huang¹, Song Yu¹, * and Hong Guo²

¹State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China and ²State Key Laboratory of Advanced Optical Communication Systems and Networks, School of Electronics Engineering and Computer Science, Center for Quantum Information Technology, Center for Computational Science and Engineering, Peking University, Beijing 100871, China

We experimentally demonstrate a real-time optical quantum random number generator by measuring vacuum fluctuation. Analysis towards the impact of practical system components is done to obtain higher min-entropy, in which min-entropy represents extractable quantum randomness. The corresponding min-entropy is calculated as 6.93 bits per sample in our experiment when system components’ parameters are suitably adjusted. To bridge the speed gap between the fast randomness generation and the slow randomness extraction, we propose an optimized extraction algorithm based on parallel implementation of Toeplitz hashing to reduce the influence of classical noise due to the imperfection of devices. Notably, the final rate of real-time randomness extraction reaches the highest speed of 6 Gbps. And this supports the generation of 6 Gbps real-time random numbers, which is the fastest among the reported experiments based on the same entropy source.

I. INTRODUCTION

Random numbers are the basis for applications in statistics, simulation [1], cryptography [2] and fundamental science [3]. The randomness of random numbers will directly affect the overall security of corresponding application systems. Classical random number generation methods, for example pseudo random number generators (RNG) based on determined algorithms, provide a cost-efficient and portable method to produce pseudo random numbers at a high speed, which satisfies the demand for random numbers of most applications. However, due to the deterministic and predictable features of the algorithms, pseudo RNG are not suitable for certain applications where true randomness is required. In cryptography applications, random numbers with untrusted randomness will result in safety issues, since hackers can access the information of random numbers and thus crack the encryption systems [5]. The rapid development of quantum cryptography technologies such as quantum key distribution [6–10] which require secure, real-time and high-speed random number generation, unarguably accelerate the researches about true random number generation.

Distinct from pseudo RNG, the optical quantum random number generators (QRNG) based on the intrinsic randomness of fundamental quantum processes are guaranteed to produce nondeterministic and unpredictable random numbers [11–14]. Such advantages attract researchers’ attention and many related generator protocols are proposed. And substantial practical QRNG protocols have been demonstrated to realize high-speed random number generation with relatively low cost, including measuring photon path [14, 15], photon arrival time [16–20], photon number distribution [21–24], vacuum fluctuation [25–28, 30, 31], phase noise [32–39] and amplified spontaneous emission noise of quantum states [40–44], etc. Typically, protocol based on the measurement of vacuum fluctuation is a more applied and valuable QRNG protocol, for its convenience of state preparation, insensitivity of detection efficiency and high generation speed.

In this paper, we propose an optimized optical QRNG scheme based on measuring vacuum fluctuation. Analysis towards the influences of each system component are performed, to help achieve a higher randomness extraction ratio so as to reduce the influence of classical noise and increase the secure random number generation speed. To fill the gap between the rapid randomness generation and the slow randomness extraction, we propose an optimized Toeplitz hashing [45, 46] algorithm to support the realization of high-speed generators. And the final real-time random number generation rate can finally reach 6 Gbps, which is much faster than the ever reported 2 Gbps scheme [27] based on the same entropy source. The final generated random bits sequences have passed the NIST tests.

II. BOUND OF EXTRACTABLE QUANTUM RANDOMNESS

In this section, the methods to quantify and increase the extractable quantum randomness of QRNG based on measuring vacuum fluctuation will be discussed. Since the QRNG system contains of four main modules, which are the entropy source, the balanced homodyne detector, the analog-to-digital converter (ADC) and the randomness extractor, we will illustrate how we can increase the secure randomness extracting bound by adjusting the parameters of different modules and thus improve the system performance.

A. Quantum randomness evaluation

In our framework, the QRNG exploits the quantum uncertainty of continuous observables, which is quadrature amplitude of vacuum state to generate true random numbers [25]. The measurement of the quadrature amplitude collapses the ground-state wave function, which is a Gaussian function centered around \( x = 0 \), into quadrature eigenstate. The asso-
associated outcome named $M$ obeys Gaussian distribution. For ideal cases, the measurement output $M$ equals to the quadrature amplitude of the vacuum state. While practical imperfect devices used in QRNG systems will inevitably introduce classical side information $E$ to the measurement results, such as electronic noise. The superimposition will lead to the security compromise of final random numbers, for the adversary, in principle, can control or monitor the classical noise and gain partial information about the raw data numbers. We consider the measured signal as $M = Q + E$. $Q$ and $E$ can be modeled as two uncorrelated Gaussian distributions, respectively. Thus the conditional probability of $M$ with a Gaussian distribution is given by

$$P_{M|E}(m|e) = \frac{1}{2\pi (\sigma_M^2 - \sigma_E^2) \sigma_Q} \exp \left[ -\frac{(m-e)^2}{2(\sigma_M^2 - \sigma_E^2)} \right]$$

for $m \in M$ and $e \in E$, where the measurement variance $\sigma_M^2 = \sigma_Q^2 + \sigma_E^2$.

To eliminate the effect of classical noise involved in the raw data and obtain more true random numbers, we refer to the notion of min-entropy to evaluate the secure bound of secure random numbers that can be extracted from raw data. Min-entropy characterizes the maximum probability of correctly guessing the outcome sequences and it helps to get the lower bound of secure random numbers can be extracted from raw data. The min-entropy for variable $X$ with a probability distribution of $P_X(x_i)$ is defined as:

$$H_{\text{min}}(X) = -\log_2 \max_{x \in X} P_X(x)$$

So the corresponding extractable randomness of our measurement outcomes conditioned on the existing classical side information can be written as:

$$H_{\text{min}}(M|E) = -\log_2 \max_{e \in E} \max_{m \in M} P_{M|E}(m|e)$$

$$= -\log_2 \left( 2\pi \left( \sigma_M^2 - \sigma_E^2 \right) \right)^{1/2}$$

$$= \log_2 \left( 2\pi \right)^{1/2} + \log_2 \sigma_Q$$.

The reality of imperfect devices, such as inevitable classical noise, coarse-grained homodyne measurement, will undoubtedly influence the measurement results of $M$ and $E$ and thus influence the analysis of $H_{\text{min}}(M|E)$. This drives us to do a further research of the influence of different components. And we seek for a higher and more secure extracting bound by adjusting the parameters of these components.

B. Methods for increasing the bound of extractable quantum randomness

For an actual QRNG system, its random number generation speed can be described, in unit of bits per second, as

$$R = S \cdot H_{\text{min}}(M|E),$$

where $S$ represents the sampling frequency. Obviously larger sampling frequency $S$ and $H_{\text{min}}(M|E)$ can lead to a higher
generation speed. In Ref. [26], the sampling frequency is determined as \( 2f_0/N \) to achieve a lower correlation between samples, where \( f_0 \) is equal to the 3 dB cut-off frequency of the homodyne detector and \( N \) is a positive integer. Thus the equation can be transformed as

\[
R = \frac{2f_0 \cdot H_{\text{min}}(M|E)}{N}, \quad N = 1, 2, 3, \ldots \quad (5)
\]

Here, we focus on promoting \( H_{\text{min}}(M|E) \). The generic flow of QRNG system is as follows. The quadrature amplitude of the vacuum state is regarded as the entropy source; the detection is realized by a homodyne detector and sampled by the ADC; and the measurement result is processed by a randomness extractor. Steps can be conducted to promote the achievable \( H_{\text{min}}(M|E) \) when certain components of the system are determined and unchangeable.

As the Eq. (3) shows, \( H_{\text{min}}(M|E) \) is positively related to the value of \( \sigma_Q \). We assume the variance of initial vacuum fluctuation is \( \sigma_V^2 \), the LO power is \( P \) and the gain of the homodyne detector is \( A \). In this context, the variance of amplified vacuum fluctuation can be described as

\[
\sigma_Q^2 = k \cdot P \cdot A^2 \cdot \sigma_V^2, \quad (6)
\]

where \( k \) is a constant coefficient resulting from factors such as the bandwidth limitation of the detector and so on. Obviously, increasing optical power and detector gain performance can enlarge \( \sigma_Q^2 \) thus increase \( H_{\text{min}}(M|E) \). Since the gain of a given detector is confirmed, a greater \( \sigma_Q^2 \) can be achieved when we input the LO light with higher power according to Eq. (6).

Generally, an \( n \)-bit ADC would be used to quantize the analog signals. For an ADC with fixed input voltage range, promoting the LO power does not necessarily increase \( \max P_X(x_i) \). And analysis has been done in Ref. [28, 29] on the relation between signal and dynamic input voltage range. As shown in Fig. 1, the 8-bit ADC with different dynamic input voltage ranges can finally get different \( \max P_X(x_i) \).

Signal output from the detector will accumulate in the quantized two side bins when the input LO power is overlarge. The wrong maximum probabilities gained on the two side bins may be larger than the value of \( (2\pi\sigma_Q^2)^{-1/2} \), which leads to the overestimation of \( H_{\text{min}}(M|E) \). On the contrary, if the input LO power is too small, the output signal of homodyne detector only occupies the central several bins, which is of low precision and leads to a low generation speed. In general, the ADC input voltage range \( R \) is set at least eight or ten times of \( \sigma_Q \) to get a secure \( \max P_X(x_i) \).

The finite sampling precision prevents the ADC from perfectly recovering signal, resulting in the deviation of the signal and the underestimation of \( \sigma_Q^2 \). We assume the dynamic range of the \( n \)-bit ADC is \( w \) times of \( \sigma_Q \), then the quantified result will have a maximum probability value of \( w(2^n \cdot \sqrt{2\pi}) \). And thus \( H_{\text{min}}(M|E) = n + \frac{1}{2} \log_2 \pi + \frac{1}{8} - \log_2 w \), which linearly increases with \( n \) when \( w \) is determined.

**FIG. 2.** Real-time randomness extraction algorithm of each calculation module. To fill the speed gap between sample acquisition and multiplication operation, S-n/C such modules are cyclically called to realize extraction operation.

### III. REAL-TIME RANDOMNESS EXTRACTION ALGORITHM

The existence of classical noise in the practical system reduces the security of raw data, so a corresponding random extraction operation is necessary for a practical QRNG system to eliminate the influence of classical noise. And universal hashing functions, such as Toeplitz hashing [46], are proved to be informational-secure [47]. They are widely used in randomness extraction. However, for a real-time system, the extraction rate is the bottleneck of the whole system. So it is very important to design a high-speed random extraction algorithm so as to improve the overall performance of the system.

Generally, a binary Toeplitz matrix \( T \) with a size of \( j \times k \) can be constructed by \( j + k - 1 \) random bits for the reason that each descending diagonal of Toeplitz matrix is the same. And \( j \) true random bits will be generated each time by multiplying \( T \) with \( k \)-bit raw random numbers named \( D \), which means each time \( k/n \) samples are gathered and extracted into \( j \) true random bits when the sampling precision of ADC is \( n \). And the relation between \( j \) and \( k \) can be usually given by \( j \leq k \cdot H_{\text{min}}(M|E) \).

The parallel computing advantages of field programmable gate array (FPGA) make it widely used in high-speed computing applications. However, it is difficult for FPGA to perform large-scale matrix computing directly due to the limitation of FPGA resources. To meet the needs of higher performance applications, we design an optimized Toeplitz hashing extracting algorithm by taking full advantage of the concurrent computing character to realize a high-speed QRNG generation. The multiplication operation of \( T \) and \( D \) can be transformed into the exclusive or operation between columns of \( T \), which is shown in Fig. 2. We name the \( i \)th bit of \( D \) as \( D_i \) and \( i \)th column of \( T \) as \( T_i \). We assume \( Z_0 \) equals to 0 and when \( D_i = 1 \), the
IV. EXPERIMENTAL IMPLEMENTATION

To realize a practical secure, real-time and high-speed QRNG, we build a prototype system with an optimized real-time randomness extraction to generate true random numbers by measuring vacuum fluctuation. The block diagram is shown in Fig. 3.

A 1550-nm fiber-coupled laser (NKT Basic E15, linewidth 100 Hz) serves as the LO and is connected to one input port of the 50:50 beam splitter. While the other input port is blocked to provide the vacuum state. The two output ports of the beam splitter are optically coupled to the two input ports of a balanced homodyne detector (Thorlabs PDB480C, measurement bandwidth limited to 1GHz by low-pass filter). The measurement results of the balanced homodyne detector are finally sampled by a 12-bit ADC (ADS5400, sampling frequency 1 GHz and input voltage range 1.5 VPP) to acquire the raw data in real-time. A following randomness extractor based on the optimized algorithm is used to perform extraction simultaneously with raw data acquiring.

A suitable LO power maximize the extractable randomness $H_{\text{min}}(M|E)$ as Eq. (6) and Eq. (3) introduced. It illustrates that a greater difference between $\sigma_{M}$ and $\sigma_{E}$ results to a larger $H_{\text{min}}(M|E)$. The LO power is increased by adjusting the variable attenuator from 0 mW with a step size of 0.5 mW to seek for the optimal $\sigma_{E}$. Simultaneously the voltage variance of each measured raw data is calculated and recorded, as shown in Fig. 4. When the LO power is set to 0 mW, the measured voltage variance of the raw data is treated as $\sigma_{E}$, which has an average calculated value of $3.13e^{-5}V^2$. And Fig. 4 indicated

![Block Diagram](image)

**FIG. 3.** Experimental demonstration of real-time optical QRNG based on vacuum fluctuation. The CW beams emitted by the laser diode enter one input port of the 50:50 BS. The other input port of the BS is blocked to provide the vacuum state. And a following measurement operation is realized by a homodyne detector and an ADC. The measurement result is finally processed by a randomness extractor to distill the final random bits.

![Variance vs LO Power](image)

**FIG. 4.** Variance vs LO power. This figure shows the voltage variance of the sampled raw data as a function of the LO power. The LO power is increased by adjusting the variable attenuator from 0 mW with a step size of 0.5 mW. And the voltage variance of the raw data enhances linearly with LO power in the range of 0 mW to 9.5 mW. The slope of the trend curve will decrease when the LO power is larger than 9.5 mW.
that the voltage variance of the raw data enhances linearly with LO power in the range of 0 mW to 9.5 mW. The slope of the trend curve will decrease when the LO power is larger than 9.5 mW. An average $\sigma^2_M$ value of $3.16e^{-2}V^2$ can be obtained by setting the LO power to 9.5 mW. And $H_{\text{min}}(M|E)$ is thus calculated as 6.93 bits per sample or 0.61 bits per raw data bit, which means that 57.75% random bits can be generated from each sample.

And the bandwidth of the homodyne detector affects the sampling frequency, that is, a suitable sampling frequency $2f_0/N$ minimizes the autocorrelation between raw data numbers. As shown in Fig. 5, we can see that the power of vacuum fluctuations is well above that of the electrical noise within the 3 dB bandwidth range $f_0$, which is approximately 0-1 GHz. And the average difference between quantum noise and classical noise is 10.04 dB when the LO power is set to 9.5 mW.

The following 12-bit ADC with a sampling frequency of 1 GHz then quantifies the signals into digital data. And 96 extracting operation blocks with a synchronized calculation frequency $C$ of 125 MHz are performed in parallel on FPGA in real time. For our implementation of Toeplitz hashing extraction, we set $j = 256$ and $k = 512$ so that the extraction ratio is $j/k=50\%$, which is smaller than 57.75% derived from the calculated $H_{\text{min}}(M|E)$.

Thus the information theoretic security bound $\varepsilon$, which means the statistical distance between the extracted random sequence and the uniform sequence, can be calculated by the leftover hash lemma, $j = k \cdot H_{\text{min}}(M|E)/n - 2 \cdot \log_2(1/\varepsilon)$. The calculated $\varepsilon$ is approximately $2^{-20}$. With such configuration, the real-time random number generation rate can finally achieve 6 Gbps. The final generated random bits sequences have passed all the NIST tests. And the test result is shown as Fig. 6.

V. CONCLUSION AND DISCUSSION

In this paper, we have proposed and experimentally demonstrated a high-speed, security-proved and real-time random number generation system by analyzing the influence of system components. And then we focus on enhancing the min-entropy to promote the randomness generation speed. In particular, an optimized random extraction algorithm is proposed and realized to bridge the speed gap between fast randomness generation and slow randomness extraction. The extraction operation eliminates potential security issues caused by classical noise. And the final real-time random number generation speed reaches 6 Gbps which is much faster than the ever reported 2 Gbps scheme based on measuring vacuum fluctuation.

The LO power is assumed to be constant and it is relatively stable in our experiment. But the LO power fluctuation should be investigated in further research, for the LO power can be influenced or even controlled by Eve in practical issues. Meanwhile, further research can be done by proposing various defense methods against hacker attacks, such as real-time min-entropy monitoring, to enhance the practical security of quantum random number generators.

ACKNOWLEDGEMENT

This work was supported by the Key Program of National Natural Science Foundation of China under Grant 61531003, the National Natural Science Foundation under Grant 61427813, the National Basic Research Program of China (973 Pro-gram) under Grant 2014CB340102 and the Fund of State Key Laboratory of Information Photonics and Optical Communications.
[1] A. M. Ferrenberg, D. P. Landau, and Y. P. Wong, “Monte Carlo simulations: Hidden errors from ‘good’ random number generators”, Phys. Rev. Lett. 69, 3382 (1992).

[2] R. Gennaro, “Randomness in cryptography”, IEEE Secur. Priv. 4(2), 64–67 (2006).

[3] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, “Bell nonlocality”, Rev. Mod. Phys. 86, 419 (2014).

[4] N. Nisan, “Hardness vs. Randomness”, J. Comput. Syst. Sci. 49, 149–167 (1994).

[5] J. Bouda, M. Pivoluska, M. Plesch, and C. Wiltmott, “Weak randomness seriously limits the security of quantum key distribution”, Phys. Rev. A. 86(6), 062308 (2012).

[6] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography”, Rev. Mod. Phys. 74, 145 (2002).

[7] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution”, Rev. Mod. Phys. 81, 1301 (2009).

[8] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, “Gaussian quantum information”, Rev. Mod. Phys. 84, 621 (2012).

[9] E. Diamanti, H. Lo, B. Qi, and Z. Yuan, “Practical challenges in quantum key distribution”, npj Quantum Inf. 2, 16025 (2016).

[10] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, C. Xu, X. Zhang, Z. Wang, M. Li, X. Zhang, Z. Zheng, B. Chu, X. Gao, N. Meng, W. Cai, Z. Wang, G. Wang, S. Yu, and H. Guo, “Continuous-variable QKD over 50km commercial fiber”, arXiv:1709.04618 (2017).

[11] X. Ma, X. Yuan, Z. Cao, B. Qi and Z. Zhang, “Quantum random number generation”, npj Quantum Inf. 2, 16021 (2016).

[12] M. Herrero-Collantes and J. C. Garcia-Escartin, “Quantum Random Number Generators”, Rev. Mod. Phys. 89, 015004 (2017).

[13] M. N. Bera, A. Acín, M. Kuś, M. W. Mitchell, and M. Lewenstein, “Randomness in Quantum Mechanics: Philosophy, Physics and Technology”, Rep. Prog. Phys. 80, 124001 (2017).

[14] T. Jennewein, U. Aicheltreier, G. Weihs, H. Weinfurter, and A. Zeilinger, “A fast and compact quantum random number generator”, Rev. Sci. Instrum. 71, 1675 (2000).

[15] A. Stefano, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, “Optical quantum random number generator”, J. Mod. Opt. 47, 595 (2000).

[16] H. Ma, Y. Xie and L. Wu, “Random number generation based on the arrival of single photons”, Appl. Opt. 44, 7760 (2005).

[17] J. F. Dynes, Z. Yuan, A. W. Sharpe, and A. J. Shields, “A high speed, postprocessing free, quantum random number generator”, Appl. Phys. Lett. 93(3), 031109 (2008).

[18] M. Wayne, E. Jeffrey, G. Akselrod, and P. Kwiat, “Photon arrival time quantum random number generation”, J. Mod. Opt. 56, 516–522 (2009).

[19] M. Wahl, M. Leifgen, M. Berlin, T. Röhlcicke, H. Rahn and O. Benson, “An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements”, Appl. Phys. Lett. 98, 171105 (2011).

[20] Y. Nie, H. Zhang, Z. Zhang, J. Wang, X. Ma, J. Zhang, and J. Pan, “Practical and fast quantum random number generation based on photon arrival time relative to external reference”, Appl. Phys. Lett. 104, 051110 (2014).

[21] W. Wei and H. Guo, “Bias-free true random-number generator”, Opt. Lett. 34, 1876 (2009).

[22] H. Fürst, H. Weier, S. Nauerth, D. G. Maranong, C. Kurtsiefer, and H. Weinfurter, “High speed optical quantum random number generation”, Opt. Express 18, 13029–13037 (2010).

[23] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng, “Quantum random-number generator based on a photon-number-resolving detector”, Phys. Rev. A. 83, 023820 (2011).

[24] M. J. Applegate, O. Thomas, J. F. Dynes, Z. Yuan, D. A. Ritchie, and A. J. Shields, “Efficient and robust quantum random number generation by photon number detection”, Appl. Phys. Lett. 107, 071106 (2015).

[25] C. Gabriel, C. Wittmann, D. Sych, R. F. Dong, W. Maurer, U. L. Andersen, C. Marquardt, and G. Leuchs, “A generator for unique quantum random numbers based on vacuum states”, Nat. Photonics 4, 711 (2010).

[26] Y. Shen, L. Tian, and H. Zou, “Practical quantum random number generator based on measuring the shot noise of vacuum states”, Phys. Rev. A. 81, 063814 (2010).

[27] T. Symul, S. M. Assad, and P. K. Lam, “Real time demonstration of high bit-rate quantum random number generation with coherent laser light”, Appl. Phys. Lett. 98, 231103 (2011).

[28] J. Y. Haw, S. M. Assad, A. M. Lance, N. H. Y. Ng, V. Sharma, P. K. Lam, and T. Symul, “Maximization of Extractable Randomness in a Quantum Random Number Generator”, Phys. Rev. Appl. 3, 054004 (2015).

[29] B. Xu, Z. Li, J. Yang, S. Wei, Q. Su, W. Huang, Y. Zhang, and H. Guo, “High Speed Continuous Variable Source-Independent Quantum Random Number Generation”, arXiv:1709.00685 (2017).

[30] Q. Zhou, R. Valivarthi, C. John, and W. Tittel, “Practical quantum random number generator based on sampling vacuum fluctuations”, arXiv:1703.00559 (2017).

[31] F. Raffaeelli, G. Ferranti, D. H. Mahaler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G Thompson, and J. C F Matthews, “A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers”, Quantum Sci. Technol. 3, 025003 (2018).

[32] B. Qi, Y. Chi, H. Lo, and L. Qian, “High-speed quantum random number generation by measuring phase noise of a single-mode laser”, Opt. Lett. 35, 312–314 (2010).

[33] H. Guo, W. Tang, Y. Liu, and W. Wei, “Truly random number generation based on measurement of phase noise of a laser”, Phys. Rev. E 81, 051137 (2010).

[34] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H. Lo “Ultrafast quantum random number generation based on quantum phase fluctuations”, Opt. Express 20, 12366 (2012).

[35] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. C. Campman, V. Pruneri, and M. W. Mitchell, ”Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode,” Opt. Express 22, 1645–1654 (2014).

[36] Y. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J. Pan, “The generation of 68 Gbps quantum random number by measuring laser phase fluctuations”, Rev. Sci. Instrum. 86, 063105 (2015).

[37] J. Yang, J. Liu, Q. Su, Z. Li, F. Fan, B. Xu, and H. Guo, ”5.4 Gbps real time quantum random number generator with compact implementation”, Opt. Express 24, 027474 (2016).

[38] X. Zhang, Y. Nie, H. Zhou, H. Liang, X. Ma, J. Zhang, and J. Pan, “Fully integrated 3.2 Gbps quantum random number generator with real-time extraction”, Rev. Sci. Instrum. 87, 076102 (2016).

[39] J. Liu, J. Yang, Q. Su, Z. Li, F. Fan, B. Xu, and H. Guo, “117 Gbits/s quantum random number generation with simple struc-
ture”, IEEE Photon. Technol. Lett. 29, 1109 (2017).

[40] C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, “Fast physical random number generator using amplified spontaneous emission”, Opt. Express 18, 23584 (2010).

[41] X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, “Scalable parallel physical random number generator based on a superluminescent LED”, Opt. Lett. 36, 1020 (2011).

[42] W. Wei, G. Xie, A. Dang, and H. Guo, “High-speed and bias-free optical random number generator”, IEEE Photon. Technol. Lett. 24, 437 (2012).

[43] Y. Liu, M. Zhu, B. Luo, J. Zhang, and H. Guo, “Implementation of 1.6 Tbs-1 truly random number generation based on a superluminescent emitting diode”, Laser Phys. Lett. 10, 045001 (2013).

[44] A. Martin, B. Sanguinetti, C. C. W. Lim, R. Houlmann, and H. Zbinden, “Quantum random number generation for 1.25-GHz quantum key distribution systems”, J. Lightwave Technol. 33, 2855 (2015).

[45] R. Impagliazzo, L. A. Levin, and M. Luby, “Pseudo-random generation from one-way functions”, Proc. 21st Annu. ACM Symp. Theory Comput. (STOC), pp.12-24, 1989.

[46] Y. Mansour, N. Nisan, and P. Tiwari, “The computational complexity of universal hashing”, Proc. 22nd Annu. ACM Symp. Theory Comput. (STOC), pp. 235-243, 1990.

[47] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H. Lo, “Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction”, Phys. Rev. A 87, 062327 (2013).