Chinese Physics Letters **40**, 070303 (2023) **Express Letter**

A High-Randomness and High-Stability Electronic Quantum Random Number Generator without Post Processing

Yu-Xuan Liu(刘宇轩), Ke-Xin Huang(黄可馨), Yu-Ming Bai(白玉明), Zhe Yang(杨哲), and Jun-Lin Li(李俊林)*

State Key Laboratory of Low-Dimensional Quantum Physics; Department of Physics, Tsinghua University, Beijing 100084, China

(Received 13 June 2023; accepted manuscript online 16 June 2023)

Random numbers are one of the key foundations of cryptography. This work implements a discrete quantum random number generator (QRNG) based on the tunneling effect of electrons in an avalanche photo diode. Without any post-processing and conditioning, this QRNG can output raw sequences at a rate of 100 Mbps. Remarkably, the statistical min-entropy of the 8,000,000 bits sequence reaches 0.9944 bits/bit, and the min-entropy validated by NIST SP 800-90B reaches 0.9872 bits/bit. This metric is currently the highest value we have investigated for QRNG raw sequences. Moreover, this QRNG can continuously and stably output raw sequences with high randomness over extended periods. The system produced a continuous output of 1,174 Gbits raw sequence for a duration of 11,744 s, with every 8 Mbits forming a unit to obtain a statistical min-entropy distribution with an average value of 0.9892 bits/bit. The statistical min-entropy of all data (1,174 Gbits) achieves the value of 0.9951 bits/bit. This QRNG can produce high-quality raw sequences with good randomness and stability. It has the potential to meet the high demand in cryptography for random numbers with high quality.

DOI: 10.1088/0256-307X/40/7/070303

Random numbers have broad applications in scientific research fields such as many-body Monte Carlo algorithms, simulated annealing, evolutionary algorithms, and experiments related to verifying Bell's inequalities.[1] Meanwhile, they are one of the cores of cryptography. The security of quantum communication relies on the unpredictability of random numbers. Researchers have shown that the security of the quantum key distribution (QKD) protocol is compromised when an attacker can effectively predict the random selection of measurement bases.[2,3]

Pseudorandom number generators (PRNGs) are based on deterministic algorithms, which means that their outputs can be determined if the algorithm and the seed are known. Therefore, the output sequence is not truly random. Since PRNGs are finite-state machines, after a finite number of outputs, they will return to the same state and repeat the previous sequence.[1,4] PRNGs with periodicity and determinism cannot meet the requirements of cryptography. For example, the most commonly used PRNG in various programming languages and software is the MT 19937, the standard implementation of the Mersenne Twister with a period of $2^{19937}-1$, while its internal state can be deduced after obtaining enough output sequences.[5]

Random numbers generated from classical physical processes typically rely on system noise or sensitivity to the initial conditions of chaotic systems. These types of sources do not suffer from periodicity issues, such as optical heterodyne chaos,[6] multimode ring lasers,[7] random Raman fiber lasers,[8] and stochastic memristor.[9,10] However, classical physical processes can be described by deterministic dynamic equations. The system state evolves continuously. It is theoretically predictable. Even if it is difficult to give an accurate dynamic description for a highly complex physical system, the sequential signals inevitably correlate within a local time because of the limited bandwidth.

Quantum random numbers are generated by the collapse of the quantum state. According to von Neumann's interpretation of quantum measurement, the result of collapse is random and its randomness relies on the intrinsic randomness of the wave function; the time of collapse is infinitesimal, hence its effective bandwidth is infinite and the output data has no correlation.[11] Therefore, the randomness generated according to quantum mechanics is certifiable.[12] Since 2000, quantum random number generators (QRNGs) have gradually attracted widespread attention.[13] QRNGs based on photon systems are most commonly used, such as branching in path,[13–15] time of arrival,[16–18] photon phase noise,[19–25] vacuum fluctuations,[26–30] amplified spontaneous emission,[31,32] and others. Some electronic QRNG schemes have been proposed in recent years, such as QRNGs based on Si diodes,[33] tunneling diodes,[34,35] and van der Waals heterojunctions.[36] The advantage of electronic QRNG lies in its no need for electro-optical-electro conversion, simple structure, stability, compatibility with semiconductor technology, and the potential for integration.

Randomness and stability are important metrics for a random number generator. Randomness can be measured by entropy, which has been used as a measure of system uncertainty in various fields. The concept of entropy was introduced into information theory by Shannon in 1948.[37]

*Corresponding author. Email: center@mail.tsinghua.edu.cn
© 2023 Chinese Physical Society and IOP Publishing Ltd

To quantify the entropy of a system, the National Institute of Standards and Technology (NIST) of the United States has proposed the relevant standard NIST SP 800-90B for entropy sources.[38] It examines the randomness of entropy sources and can effectively compare different entropy sources. The stability of a QRNG refers to its ability to produce a stable random sequence over a long period, without being disturbed by the environment. According to our investigation, there is no clear standard for testing the stability of the long-term continuous output sequence of a QRNG system. In this study, the stability of the QRNG system is evaluated by the min-entropy distribution of the long-term continuous output sequence and how the min-entropy changes with the length of the sequence.

According to the NIST SP 800-90B standard, post-processing and conditioning can be included in the design.[38] Post-processing and conditioning, which usually require buffering the output of the noise source, are mathematical operations that convert the original sequence of the noise source into a sequence that is more uniform.[39] For QRNGs, these mathematical operations are classical, which may introduce some classical information. Consequently, the corresponding relationship between sequences and quantum source signals no longer exists. Especially, when post-processing and conditioning are used for passing statistical tests, the randomness of the output may not be purely attributed to the quantum entropy source. Therefore, QRNG systems without post-processing and conditioning are more ideal.[40]

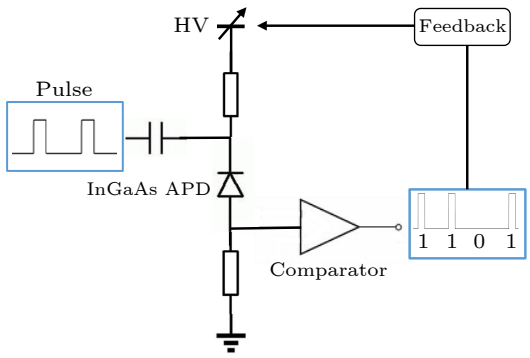

Fig. 1. The schematic diagram of our QRNG. A pulsed voltage is applied to the avalanche photo diode (APD), and the comparator is used to detect the APD electron tunneling signal to output the raw sequence. The system is controlled through feedback to ensure that the raw sequence has a ratio of "0" and "1" close to 50 : 50. HV: high voltage.

Our group achieved the first discrete QRNG system based on the tunneling effect of electrons in the avalanche photo diode (APD) in 2017,[41] and our present work is significant progress upon it. In our system, the 8,000,000 bits statistical min-entropy is valued to be 0.9944 bits/bit and the min-entropy validated by NIST SP 800-90B reaches 0.9872 bits/bit, both obtained at an output rate of 100 Mbps without any post-processing and conditioning. Moreover, we have demonstrated that the system can maintain high randomness under long-term continuous outputting.

Methods. The schematic diagram of our system is shown in Fig. 1. The APD operates in an environment of −20 ℃, with temperature fluctuations not exceeding 0.002 ℃. The electronic tunneling signal of the APD is measured through a 100 MHz pulse voltage excitation, and raw random sequences are output at a rate of 100 Mbps.

After applying a high voltage (below the avalanche voltage) to the APD, an additional 100 MHz pulsed voltage is applied to induce the APD into the Geiger mode. When an electron tunneled or not, it would produce a voltage signal measured by the comparator to determine whether the tunneling effect of electrons occurred during each pulse period. If it did, the output would be 1; if not, the output would be 0.

For a random variable X with n bits, its min-entropy is defined as

$$H_\infty(X) = -\log_2[\max_{x\in[0,1]^n} \Pr(X = x)], \tag{1}$$

where $\Pr(X = x)$ represents the probability of the random variable X taking the value x. For convenience of comparisons between different random variables, it is common to normalize the min-entropy, resulting in the normalized min-entropy:

$$H^0_\infty(X) = \frac{H_\infty(X)}{n} = -\frac{1}{n}\log_2[\max_{x\in[0,1]^n} \Pr(X = x)]. \tag{2}$$

All mentions of min-entropy in this study refer to the normalized min-entropy. When calculating the min-entropy, it commonly treats every 8 bits in sequence as a variable, referred to as an 8-bit value. The frequency of each 8-bit value is counted, and Eq. (2) is used to calculate the min-entropy of the dataset. The min-entropy value is 1 bits/bit for an ideal random sequence.

When analyzing long random sequences of continuous outputs, two methods are used to calculate the min-entropy: (1) Divide the data into units of 8,000,000 bits and calculate the min-entropy using the above method to obtain the distribution of min-entropy. (2) Calculate the min-entropy for sequences of increasing lengths by starting from the beginning of the sequence and doubling the length each time, which yields a curve of the min-entropy as a variable of sequence length. Both methods can reflect the stability of the system during long periods of continuous output.

The min-entropy calculated according to Eq. (2) is referred to as statistical min-entropy in this study.

According to NIST SP 800-90B, a sequential dataset and a restart dataset are required. The sequential dataset requires a continuous output sequence of 8,000,000 bits. The restart dataset involves restarting the system 1,000 times and outputting 8,000 bits of sequence each time. Every 8 bits of the restart dataset is treated as a symbol, generating a $10^3 \times 10^3$ matrix, where each row corresponds to the data output from each restart.

The NIST SP 800-90B first checks the independent and identically distributed (IID) properties of the sequence by using chi-square tests and permutation tests to detect the independence and uniformity in the distribution of the sequence. If both the sequential dataset and the restart dataset pass the tests, the QRNG output is validated as IID; otherwise, it is non-IID. For IID sequences, the NIST

SP 800-90B uses the most common value (MCV) to estimate the min-entropy of the entropy source; for non-IID sequences, alternative evaluation methods are used.

To calculate the MCV entropy, the proportion of the most frequently value $\hat{P}$ is estimated by

$$\hat{P} = \max_i \{P(x_i)\}, \quad i = 1, 2, \ldots, k, \tag{3}$$

where $P(x_i)$ is the proportion of the symbol taking the value of x_i. The upper bound of the actual distribution probability value P_u is estimated using the $\hat{P}$:

$$P_u = \min\left\{1, \hat{P} + 2.576\sqrt{\frac{\hat{P}(1-\hat{P})}{L-1}}\right\}, \tag{4}$$

where L is the total number of symbols. The final MCV entropy value is $H_{\mathrm{MCV}} = -\log_2(P_u)$, normalized as

$$H^0_{\mathrm{MCV}} = -\frac{1}{n}\log_2 P_u. \tag{5}$$

NIST SP 800-90B requires the calculation of both MCV entropy for 8-bit symbols (H_{symbol}) and MCV entropy for binary string ($H_{\mathrm{bitstring}}$), and the smaller value of them is taken as the initial min-entropy of NIST SP 800-90B.

Finally, NIST SP 800-90B requires the sanity test and entropy estimation on the two datasets. The sanity test checks the deviation of the min-entropy obtained by the system after each restart, then the system performs entropy estimation (using MCV entropy estimation for IID data, and estimating the sequential dataset and the rows and columns of the restart dataset). The minimum value of the calculated min-entropy is considered to be the validated min-entropy of NIST SP 800-90B.

Results. The experimental system obtained the sequential dataset and the restart dataset without any post-processing and conditioning. All datasets passed the IID test and Restart test of NIST SP 800-90B. The NIST SP 800-90B validated min-entropy is 0.9872 bits/bit, and the statistical min-entropy of the sequential dataset is 0.9944 bits/bit, which is currently the highest min-entropy of the QRNG raw sequence we have investigated. Table 1 shows the statistical min-entropy and NIST SP 800-90B validated min-entropy of some QRNG systems for comparison. Table 2 shows the NIST SP 800-90B test results of this system, and Fig. 2 shows the probability distribution of the 8-bit values of the sequential dataset and the restart dataset. The min-entropy results without post-processing and conditioning prove the experimental system's ability to output random sequences with high randomness.

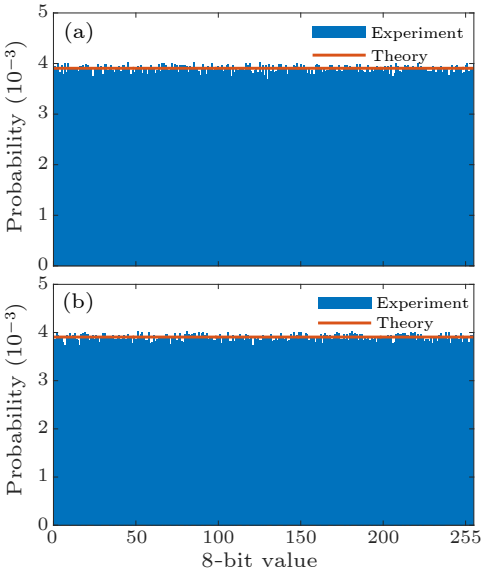

Fig. 2. Probability distributions of 8-bit values of (a) the sequential dataset and (b) the restart dataset. The sequence of 8,000,000 bits was grouped into 8-bit values, resulting in 1,000,000 samples. The probability distribution of each sample (8-bit value) was obtained by counting the occurrences of each value in the sample set. The blue bars in the figure represent the experimental statistical data, while the red line represents the ideal uniform distribution.

Table 1. Min-entropy of some QRNG raw sequences.

Year	QRNGs' principle	System	Type	Min-entropy (bits/bit)	
				Statistical min-entropy	NIST SP 800-90B validated min-entropy
2023	This work	Electronic	Discrete	0.9944	0.9872
2022	van der Waals heterojunction [36] (7 K, 10^{-4} Torr)	Electronic	Discrete	–	0.983
2021	Tunnel diodes [34]	Electronic	Discrete	0.62	–
2021	Amplified spontaneous emission [32]	Photonic	Continuous	0.77	–
2021	Vacuum fluctuations [30]	Photonic	Continuous	0.60	–
2021	Vacuum fluctuations [29]	Photonic	Continuous	0.77	–
2020	Vacuum fluctuations [27]	Photonic	Continuous	0.73	–
2020	Vacuum fluctuations [28]	Photonic	Continuous	0.80	–
2020	Phase noise [25]	Photonic	Continuous	0.83	–
2020	Phase noise [24]	Photonic	Continuous	0.86	–
2018	Phase noise [23]	Photonic	Continuous	0.70	–
2015	Phase noise [22]	Photonic	Continuous	0.88	–
2012	Phase noise [21]	Photonic	Continuous	0.84	–

For practical applications, it is necessary to study the stability of the data quality when the QRNG system outputs random sequences continuously for a long time. We let the QRNG operate continuously for about 11,744 s, outputting a sequence of 1,174,405,120,000 bits without any post-processing and conditioning. According to Eq. (2), the statistical min-entropy of every 8 Mbits of the sequence is calculated, and the distribution of the statistical min-

entropy is shown in Fig. 3(a). The average value of the statistical min-entropy of the raw sequence is 0.9892 bits/bit, and the standard deviation is 0.0208 bits/bit.

Moreover, we studied the variation of the system's min-entropy with the length of the sequence, as shown in Fig. 3(b). The min-entropy can be stabilized around 0.99 bits/bit for long sequences, indicating that the system has good long-term stability. For the entire sequence (1,174,405,120,000 bits), the statistical min-entropy is 0.9951 bits/bit.

Table 2. NIST SP 800-90B Test results.

Chi-square tests: PASSED						
Statistic	Sequential			Restart		
	Score	Degrees of freedom	P value	Score	Degrees of freedom	P value
Chi-square independence	65450.794328	65280	0.317709	65348.118952	65280	0.424536
Chi-square goodness of Fit	2191.175821	2295	0.938988	2289.951808	2295	0.525804

Length of longest repeated substring test: PASSED					
Sequential			Restart		
P_col	Length of LRS	Pr($X \geqslant 1$)	P_col	Length of LRS	Pr($X \geqslant 1$)
0.003907	5	0.365768	0.003907	5	0.365770

IID Permutation tests: PASSED						
Statistic	Sequential			Restart		
	$C_{i,0}$	$C_{i,1}$	$C_{i,2}$	$C_{i,0}$	$C_{i,1}$	$C_{i,2}$
Excursion test statistic	19	0	6	6	0	30
Number of directional runs	48	0	6	6	0	12
Length of directional runs	3	6	0	2	6	0
Number of increases and decreases	107	0	6	43	0	6
Number of runs based on the median	6	0	7	5	1	13
Length of runs based on median	3	3	3	3	3	25
Average collision test statistic	42	0	6	6	0	98
Maximum collision test statistic	6	0	8	6	0	8
Periodicity test statistic (lag = 1)	6	0	49	11	1	5
Periodicity test statistic (lag = 2)	29	0	6	7	1	5
Periodicity test statistic (lag = 8)	5	1	543	6	0	29
Periodicity test statistic (lag = 16)	6	0	50	6	0	66
Periodicity test statistic (lag = 32)	19	1	5	96	0	6
Covariance test statistic (lag = 1)	6	0	6	36	0	6
Covariance test statistic (lag = 2)	61	0	6	69	0	6
Covariance test statistic (lag = 8)	28	0	6	6	0	18
Covariance test statistic (lag = 16)	15	0	6	6	0	6
Covariance test statistic (lag = 32)	16	0	6	6	0	22
Compression test statistics	6	0	23	6	0	32

Restart sanity check: PASSED		
Entropy estimate (bits/symbol)		
Sequential	Columns	Rows
7.897736	7.900547	7.900547
Min-entropy = 7.897736/8 = 0.9872 bits/bit		

Both results indicate that the system can maintain high randomness of the raw sequence during a long period of continuous outputting.

Discussion. Compared to many current QRNG systems, our scheme generates random sequences directly from the quantum entropy source without any post-processing and conditioning. The randomness of the sequence comes entirely from the intrinsic randomness of wave function collapse, rather than mathematical operations. We use NIST SP 800-90B to demonstrate the good randomness of our entropy source.

In practical applications, QRNGs often need to continuously output random sequences for a long time, and require all sequences to have high randomness. Therefore, the stability of continuously outputting random sequences for a long time is an important metric for practical QRNGs, but there are currently no clear standards and few relevant studies on it. We used two methods to estimate the long-term stability of the output sequence. First, for the convenience of comparison with other works, we use every 8 Mbits (the same size as the NIST SP 800-90B specification) as the min-entropy calculation unit in the sequence that is continuously output for a long time. We use Eq. (2) to calculate the statistical min-entropy. Second, we calculate the min-entropy using Eq. (2) with different sequence lengths. The results in Fig. 3 reflect the stability of the system's continuously output random sequences.

The reason for not using formula (5) is that the MCV estimation is a min-entropy estimation of the entropy source based on finite data. In the analysis of a large amount of data, MCV estimation is not necessary.

Furthermore, our system can generate real-time online random sequences without requiring analog-to-digital (A/D) sampling and buffering, and has no requirements

for low temperatures (only APD works in an environment of about −20 ℃). It has high stability, and is minimally affected by the environment. Therefore, our electronic QRNG is highly practical.

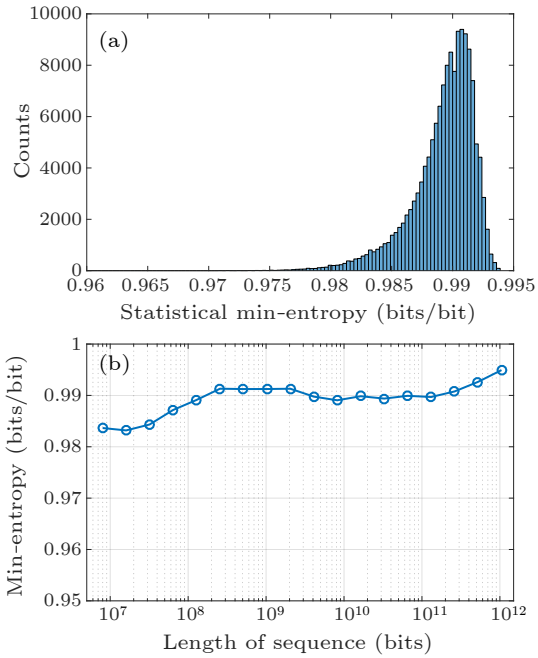

Fig. 3. (a) Frequency distribution of the statistical min-entropy with a bin size of 0.0003 bits/bit. (b) Variation of the statistical min-entropy with sequence length.

In summary, we have developed a discrete QRNG system based on the tunneling effect of electrons in APD, which exhibits superior randomness and stability in continuous output. The raw sequence generated by our QRNG achieves a statistical min-entropy of 0.9946 bits/bit and the NIST SP800-90B validated min-entropy of 0.9872 bits/bit without any post-processing and conditioning. Moreover, after a continuous output of 11,744 s, we obtain a sequence of 1,174 Gbits, where the average of the 8 Mbits statistical min-entropy is 0.9892 bits/bit, and the statistical min-entropy of the entire raw sequence is 0.9951 bits/bit. Our QRNG scheme has strong practicality with a great potential for optimization in terms of generation rate and randomness. It is expected to meet the demand for high-quality random numbers in cryptography.

Acknowledgement. This work was supported by the National Natural Science Foundation of China (Grant No. 51727805).

References

[1] Herrero-Collantes M and Garcia-Escartin J C 2017 *Rev. Mod. Phys.* **89** 015004
[2] Bouda J, Pivoluska M, Plesch M, and Wilmott C 2012 *Phys. Rev. A* **86** 062308
[3] Li H W, Yin Z Q, Wang S, Qian Y J, Chen W, Guo G C, and Han Z F 2015 *Sci. Rep.* **5** 16200
[4] Bhattacharjee K and Das S 2022 *Comput. Sci. Rev.* **45** 100471
[5] Matsumoto M and Nishimura T 1998 *ACM Trans. Model. Comput. Simul.* **8** 3
[6] Yoshiya K, Terashima Y, Kanno K, and Uchida A 2020 *Opt. Express* **28** 3686
[7] Serrano R, Duran C, Hoang T T, Sarmiento M, Nguyen K D, Tsukamoto A, Suzaki K, and Pham C K 2021 *IEEE Acc.* **9** 105748
[8] Monet F, Boisvert J S, and Kashyap R 2021 *Sci. Rep.* **11** 13182
[9] Jiang H, Belkin D, Savelév S E *et al.* 2017 *Nat. Commun.* **8** 882
[10] Kim G, In J H, Kim Y S, Rhee H, Park W, Song H, Park J, and Kim K M 2021 *Nat. Commun.* **12** 2906
[11] Von Neumann J 2018 *Mathematical Foundations of Quantum Mechanics* (New Jersey: Princeton University Press) vol 53
[12] Zhang Y B, Lo H P, Mink A, Ikuta T, Honjo T, Takesue H, and Munro W J 2021 *Nat. Commun.* **12** 1056
[13] Jennewein T, Achleitner U, Weihs G, Weinfurter H, and Zeilinger A 2000 *Rev. Sci. Instrum.* **71** 1675
[14] Stefanov A, Gisin N, Guinnard O, Guinnard L, and Zbinden H 2000 *J. Mod. Opt.* **47** 595
[15] Hoese M, Koch M K, Breuning F, Lettner N, Fehler K G, and Kubanek A 2022 *Appl. Phys. Lett.* **120** 044001
[16] Wei W and Guo H 2009 *Opt. Lett.* **34** 1876
[17] Ren M, Wu E, Liang Y, Jian Y, Wu G, and Zeng H 2011 *Phys. Rev. A* **83** 023820
[18] Wahl M, Leifgen M, Berlin M, Röhlicke T, Rahn H J, and Benson O 2011 *Appl. Phys. Lett.* **98** 171105
[19] Guo H, Tang W, Liu Y, and Wei W 2010 *Phys. Rev. E* **81** 051137
[20] Qi B, Chi Y M, Lo H K, and Qian L 2010 *Opt. Lett.* **35** 312
[21] Xu F H, Qi B, Ma X F, Xu H, Zheng H X, and Lo H K 2012 *Opt. Express* **20** 12366
[22] Nie Y Q, Huang L, Liu Y, Payne F, Zhang J, and Pan J W 2015 *Rev. Sci. Instrum.* **86** 063105
[23] Raffaelli F, Sibson P, Kennard J E, Mahler D H, Thompson M G, and Matthews J C F 2018 *Opt. Express* **26** 19730
[24] Lei W, Xie Z, Li Y, Fang J, and Shen W 2020 *Quantum Inf. Process.* **19** 405
[25] Huang M, Chen Z, Zhang Y, and Guo H 2020 *Appl. Sci.* **10** 2431
[26] Shen Y, Tian L, and Zou H 2010 *Phys. Rev. A* **81** 063814
[27] Huang M, Chen Z, Zhang Y, and Guo H 2020 *Entropy* **22** 618
[28] Samsonov E O, Pervushin B E, Ivanova A E, Santev A A, Egorov V I, Kynev S M, and Gleim A V 2020 *Quantum Inf. Process.* **19** 326
[29] Bai B, Huang J Y, Qiao G R, Nie Y Q, Tang W J, Chu T, Zhang J, and Pan J W 2021 *Appl. Phys. Lett.* **118** 264001
[30] Pervushin B E, Fadeev M A, Zinovev A V, Goncharov R K, Santev A A, Ivanova A E, Samsonov E O, Physics N, and C 2021 *Nanosystems: Phys. Chem. Math.* **12** 156
[31] Marosits Á, Schranz Á, and Udvary E 2020 *Infocommun. J.* **12** 12
[32] Guo Y, Cai Q, Li P *et al.* 2021 *APL Photon.* **6** 066105
[33] Zhou H H, Li J L, Zhang W X, and Long G L 2019 *Phys. Rev. Appl.* **11** 034060
[34] Aungskunsiri K, Amarit R, Wongpanya K, Jantarachote S, Yamwong W, Saiburee S, Chanhorm S, Intarapanich A, and Sumriddetchkajorn S 2021 *Appl. Phys. Lett.* **119** 074002
[35] Bernardo-Gavito R, Bagci I E, Roberts J *et al.* 2017 *Sci. Rep.* **7** 17879
[36] Abraham N, Watanabe K, Taniguchi T, and Majumdar K 2022 *ACS Nano* **16** 5898
[37] Shannon C E 1948 *Bell Syst. Tech. J.* **27** 379
[38] Turan M S, Barker E, Kelsey J, McKay K A, Baish M L, and Boyle M 2018 *NIST Special Publication* **800-90B** 102
[39] Schindler W and Killmann W 2003 *Evaluation Criteria for True (Physical) Random Number Generators Used in Cryptographic Applications.* In: Kaliski B S, Koc C K, and Paar C (eds) *Cryptographic Hardware and Embedded Systems - CHES 2002. Lecture Notes in Computer Science* (Berlin: Springer) vol 2523 p 431
[40] Wang J M, Xie T Y, Zhang H F, Yang D X, Xie C, and Wang J 2015 *IEEE Photon. J.* **7** 7100808
[41] Zhou H, Li J L, Pan D, Zhang W, and Long G 2017 arXiv:1711.01752 [quant-ph]