Quantum random number generator based on quantum tunneling effect

Article · November 2017

CITATIONS
4

READS
180

5 authors, including:

Dong Pan
Tsinghua University
8 PUBLICATIONS **58** CITATIONS
SEE PROFILE

Gui Lu Long
Tsinghua University
480 PUBLICATIONS **18,278** CITATIONS
SEE PROFILE

Quantum random number generator based on quantum tunneling effect

Junlin Li′, Haihan Zhou′, Dong Pan, and Guilu Long*
[1]*State Key Laboratory of Low-Dimensional Quantum Physics, Tsinghua University, Beijing 100084, China*

In this paper, we proposed an experimental implementation of quantum random number generator(QRNG) with inherent randomness of quantum tunneling effect of electrons. We exploited InGaAs/InP diodes, whose valance band and conduction band shared a quasi-constant energy barrier. We applied a bias voltage on the InGaAs/InP avalanche diode, which made the diode works under Geiger mode, and triggered the tunneling events with a periodic pulse. Finally, after data collection and post-processing, our quantum random number generation rate reached 8Mb/s, and final data was verified by NIST test and Diehard test. Our experiment is characterized as an innovative low-cost, photonic source free, integratable or even chip-achievable method in quantum random number generation.

PACS numbers:

I. INTRODUCTION

Random numbers are crucial in many fields, for instance, the physical simulation[1], information processing[2],quantum communication protocols[3], quantum cryptography[4] and quantum computation[5]. Under most circumstances, security is directly associated with its unpredictability and uncopyablity. However, the prevalent pseudo-random number or chaotic random number[6] are theoretically pre-determined or not proven to be unpredictable. Meanwhile, it is of great significance to develop true random number generator. Fortunately, uncertainty is a fundamental property of quantum mechanics. So, numerous studies, on true random number generation, has focused on the application of quantum inherent uncertainty or probability , such as the path choice of single photon with fixed polarization after passing a PBS[7][8]; the uncertainty of the arrival time of single photons[9][10]; or the phase fluctuation of photons[11][12]. And more recently, Bowels proposed a protocol of self-testing quantum random number generator[13] with the measurement of 'dimension witness'[14]. It made a quantative analysis on the true randomness of a given system. Also, Ma studied how to generate true randomness with an untrustworthy random source[15]. Moreover, Xu introduced a robust quantum random number generator via the high dimensional interference[16]. The generation speed of these protocols varies from bps to Gbps. Noteworthy, all these pervasive protocols exploited photonic sources, or, even single-photon sources.

In light of the difficulty of integration and the vulnerability to the environmental influence of photonic source, together with other flaws that impede the pragmatic application of quantum random number generators, we focused on another intrinsic randomness of quantum mechanics—the tunneling probability of electrons[17][18][19], which aborted the essence of photonic source and turn to the electronic source. Consequently, our QRNG could be highly integratable.

In this paper, we introduced an efficient protocol of quantum random number generation via the application of intrinsic indeterministic property of quantum tunneling effect and experimentally realized this protocol via the widely applied InGaAs/InP avalanche diode[20][21][22], with the generation speed reaching 8Mb/s. Furthermore, higher speed, up to 20Mb/s, can be reached by changing the frequency of trigger pulses. On the other hand, a more efficient system which could respond to a higher frequency of trigger pulse is competent to augment the generation speed, as stable high frequency voltage pulses up to Gb/s could be realized in a precise way in nowadays electronic controlling. Also, post-processing program can be easily transplanted into our data-collecting FPGA, which enable a real-time output of quantum random number sequence.

II. PROTOCOL

Consider electrons trapped in a potential well, we apply a periodic bias voltage, whose peak value is U_H on this system, which could induce tunneling events with a constant probability p within each single period, and then record a sequence of these signal with '0' when no tunneling occurs in a single pulse period and '1' when it occurs. Here, the tunneling probability p can be determined theoretically [23]. Finally, post-processing of the sequence was operated and we obtained the eligible random number sequences[24]. This protocol is also summarized in Fig1:

We noticed that Shelan Khasro Tawfeeq has exploited the dark counts of InGaAs/InP avalanche diode in random number generation[25]. However, our protocol is utterly distinct with hers. This difference is interpreted in the next section.

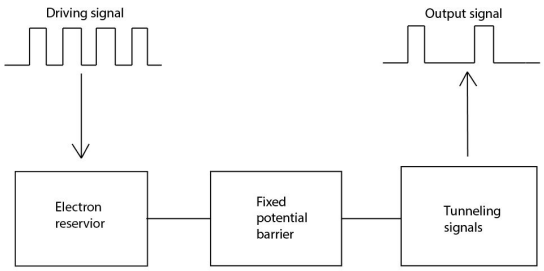

FIG. 1: Brief summary of the tunneling-based QRNG

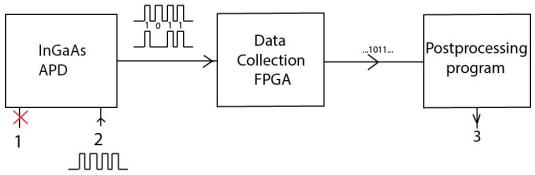

FIG. 2: Experimental setup of tunneling-based QRNG. 1: Optical input channel; 2: External clock input channel(trigger signal input channel);3: Final random number output channel.

III. EXPERIMENTAL IMPLEMENTATION

The key problem in our experiment is setup of the electron reservoir, bounded by a stable potential barrier, as the electronic realization of precise bias voltage pulses is not a challenge. After several pre-tests, we utilized the InGaAs/InP avalanche diode. Although the InGaAs/InP avalanche diode is prevailing in the photon detectors, our experiment is totally irrelevant to photonic source. On the contrary, we just take advantage of the quasi static barrier it possessed. As concoluded in [26], an InGaAs/InP avalanche diode consists four parts in its energy band diagram. And in our experiment, trigger signals were applied to accelerate electrons in the $P^+ - InP$ section. These electrons tunneled through junction between $P^+ - InP$ section and $n - InP$ section with certain probability determined on the peak voltage of trigger signals U_H. Subsequently, we recorded the tunneling signals and came to raw data.

Setup of our experiment was shown in Fig.2. And 3 showed the circuit of out experiment. We confined the InGaAs/InP diode in a seal box. Hence, no environmental photons could contribute to the signals received by the receptor module.

As we mentioned above, the QRNG source is the tunneling effect of electrons in InGaAs/InP avalanche diode, which is irrelevant to the photons and was considered as part of the dark counts in the previous study[27].

Dark counts of InGaAs/InP avalanche diode can be

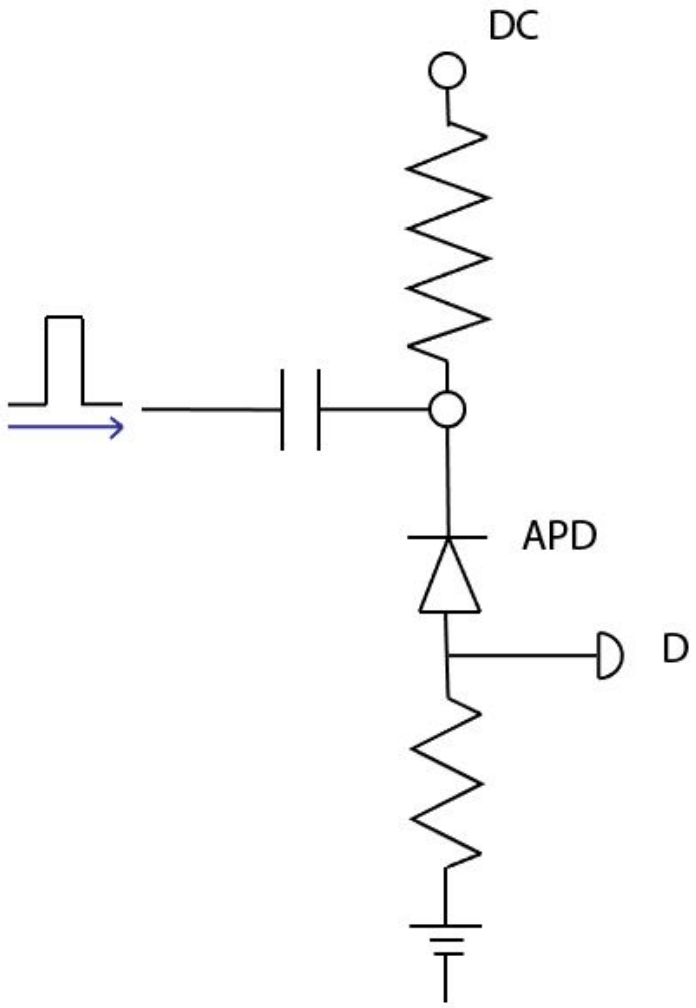

FIG. 3: Circuit of tunneling-based QRNG.

characterized into 3 kinds[28]

1— Dark counts induced by heat motion of electrons.

2— Dark counts induced by quantum tunneling effect.

3— Dark counts induced by after-pulse effect.

When proper bias voltage is applied on the InGaAs/InP avalanche diode, it works under the Geiger mode[21]. Under this circumstance, the accelerated electrons triggered avalanche effect in the 'accelerating section', which could induce current signals. While the bias voltage varies, the tunneling probability changes, so does the data properties(data entropy, data auto-correlation parameter and the final data generation speed).

And as mentioned in the previous section, our protocol focus more on the 'Dark counts induced by quantum tunneling effect', where the voltage of the trigger signal's high level U_H dominates the tunneling probability in a single period T. While Shelan's work emphasized more about the pulsewidth of a fixed trigger signal. The afterpulse effect could responsible for her thesis, which is not

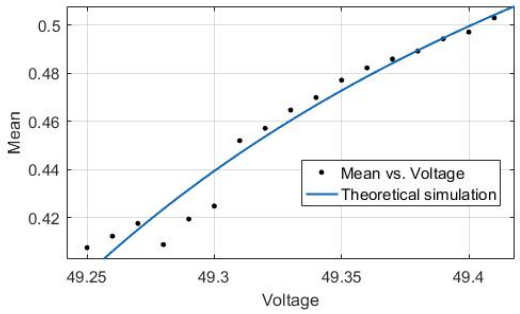

FIG. 4: Mean of output data under different voltage. $R^2 = 0.964$

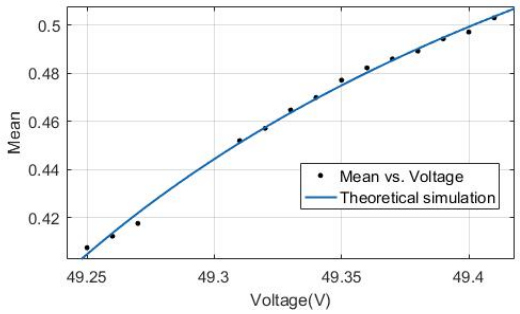

FIG. 5: Mean of output data under different voltage(without $49.28V, 49.29V$ and $49.30V$). $R^2 = 0.9996$

credited with quantum property.

In order to restrain the $fisrt$ effect mentioned above, the working environment is monitored at $200K$ by the semiconductor cooling system. Under this circumstance, the I type dark counts was reduced to $500/s$, which is equivalent to $10^{-5}/pulse$ in a $50Mhz$ bias voltage pulse triggered system. Meanwhile, the III type dark counts is partly circumvented by the deadtime of this system. The deadtime system ensures that after each tunneling occurs, there will be a time interval ΔT during which the detector is forced offline. Namely, the after-pulse during this time interval ΔT could not be counted. However, due to the hardware impediment and the remnant after-pulse, our raw random number data requires a further optimization, and post-processing program is applied to countervail this bias and subsequently generate true randomness.

The counting number of the tunneling-induced signals in $1s$ can be directly displayed on a screen. In our experiment, the frequency of bias voltage pulses was set to $50Mb/s$, then we adjusted the amplitude of these pulses U until the counting number reach 2.5×10^7. According to [29], we can demonstrate our tunneling probability as :

$$P(V) = Ae^{\frac{-B}{V-V_0}} \tag{1}$$

Here, A,B are parametric expression, which are determined by several indexes; V_0 is the critical voltage, under which the tunneling probability is 0. In order to determine proper voltage, we measured the mean and entropy of output data from $49.25V$ to $49.5V$, and simulated the result based on the above equation. We obtained figure 4,5,6,7.

We noticed when $U = 49.28V, U = 49.29V, U = 49.30V$, the mean obviously biased from other data, so we omitted them and comes to figure 5,7.

As the forward tunneling probability is too complicated to have an analytical expression[23], we quantitatively fitted the data with curves shown above.

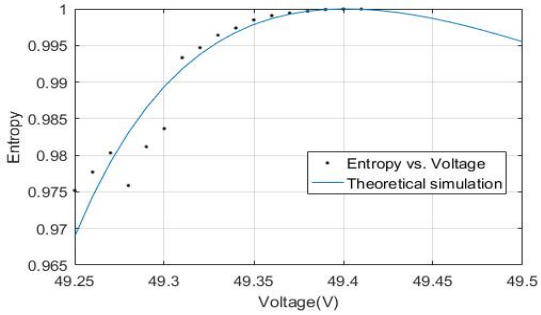

FIG. 6: Entropy of output data under different voltage.

Finally, we chose $U_H = 49.40V$. And we designed a $FPGA$ module to collect all tunneling data and saved it into a $.txt$ document. The speed of raw data collection is about $20Mb/s$, which is restricted by the USB communication serial port.

IV. POST-PROCESSING

The post-processing program is realized by the application of Toeplitz-hashing extractor[24].

Min-entropy estimation— We measure the minimum

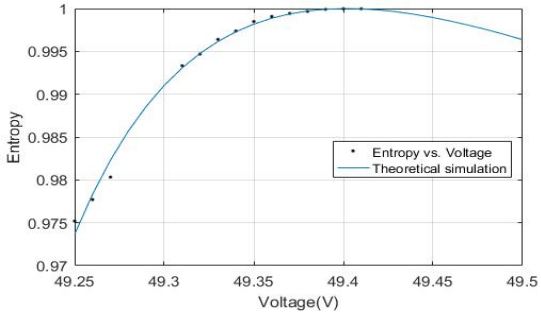

FIG. 7: Entropy of output data under different voltage(without $49.28V, 49.29V$ and $49.30V$).

entropy H_m of our raw data[30].

$$H_m = -log_2(\max_x P[x]) \tag{2}$$

Here x refers to all the possible sequence that $0, 1^n$ could reach. In our scheme, we took $n = 8$, namely, we divide our raw data into $8 - bits$ sequences. And then calculate maximum probability of these segments and the min-entropy. In our experiments, $H_m = 5.1204$.

Toeplitz-hashing extractor— After the min-entropy estimation, we characterized the raw data with the proportion of quantum randomness. Namely, independent $2.8 - bits$ quantum random code can be extracted from each $8 - bits$ raw data segment. Subsequently, we generate a Toeplitz matrix T with two independent random seeds $s_A = \{s_{A1}, s_{A2}, \cdots, s_{Am}\}$, $s_B = \{s_{B1}, s_{B2}, \cdots, s_{Bn}\}$. m and n are determined by the min-entropy and the length of raw data l. And s_A, s_B consisted the row and column of T, respectively.

$$\begin{aligned} n &= l \\ m &= l \times \frac{H_m}{H_0} - 2log_2(\epsilon) \end{aligned} \tag{3}$$

Notice that, ϵ is the secure parameter, and $H_0 = log_2(l)$, H_m is the min-entropy of the raw data.

Scheme of postprocessing— For a raw data sequence d with length l, eligible quantum random sequence $d^{'}$ can be obtained as follows:

$$d \times T = d^{'}$$

$$\underbrace{(d_1, \cdots, d_l)}_{l} \times \underbrace{\begin{pmatrix} s_{A1} & \cdots & s_{Am} \\ \vdots & \ddots & \vdots \\ s_{Bn} & \cdots & s_{A1} \end{pmatrix}}_{m} = \left(d_1^{'}, \cdots, d_m^{'}\right) \tag{4}$$

Here, we noticed a systematic bias ascribed to the low peak-peak value of our QRNG. Briefly, the lower level in our experiment was supposed to be low enough so that no tunneling could occur and the after-pulse could be relieved. Unfortunately, restricted by the inner set of the driven module in InGaAs/InP trigger module, the difference between high level and low level is fixed at $\Delta U = 4V$, which means that even the low level$U_L = U_H - 4V$, and could result in tunneling current. Inevitably, the InGaAs/InP APD self-protecting program, which compels the InGaAs/InP APD out of avalanche effect, was activated automatically as the InGaAs/InP APD works at avalanche mode in a prolonged period. Thus, we could see a set of 0s in our raw data periodically.

V.DATA ANALYSIS

In our final experiment, we set the frequency of trigger pulse to $50MHz$, with $0ns$ deadtime. And the bias voltage was fixed to $49.40V$. As showed above, the min-entropy $H_m = 5.12$, for $8 - bits$ sequences. Combined with a secure parameter $\epsilon = 2^{-100}$, data length $l = 3000$, the random bits generation rate was $8.3Mb/s$.

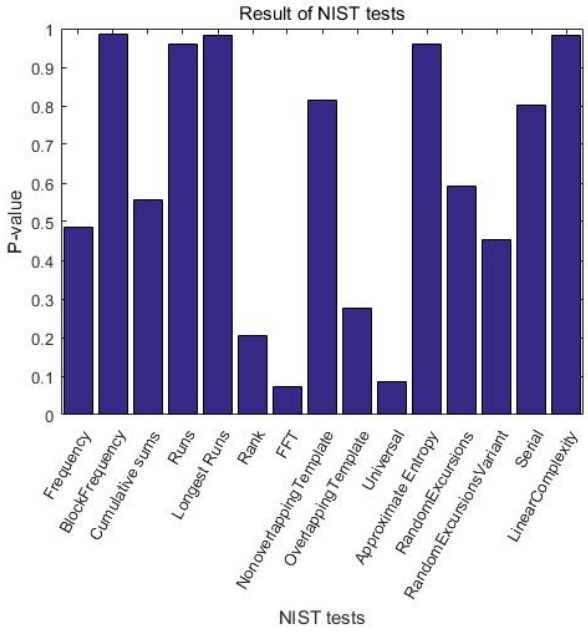

FIG. 8: Upper is the result of NIST test of our final random sequence while the lower is the eligible rate of sequences decomposed from the original final sequence. The voltage of high level $V_h = 49.40V$ and the data size of original final sequence is 5Gb.

After a set of $5Gb$final data, we applied the $NIST-sts$ Test and *Diehard* Test. See Figure5 and Figure6. Aside from these two tests, the auto-correlation function is also drew from the data sheet, as shown by Figure7. And more details of the test data is provided in the *Appendix*.

It is apparently that all our random number passed these two tests and the auto-correlation got a dramatic decline after postprocessing with Toeplitz-hashing extractor. Noteworthy, that the improvement on the data collection module and the optimization of the trigger module is approachable certifies realization of higher generation rate.

VI. CONCLUSION

In this paper, we proposed a QRNG protocol based on the tunneling effect in InGaAs/InP avalanche diode. And thus no photonic sources is required in our experiments. Moreover, with the application of integrated module in InGaAs/InP single photon detector, we implemented a photonic-source-free QRNG, whose generation rate could reach $8.3Mb/s$. Moreover, this rate can be lifted up to $20Mb/s$ with the facilities we have. Our further study

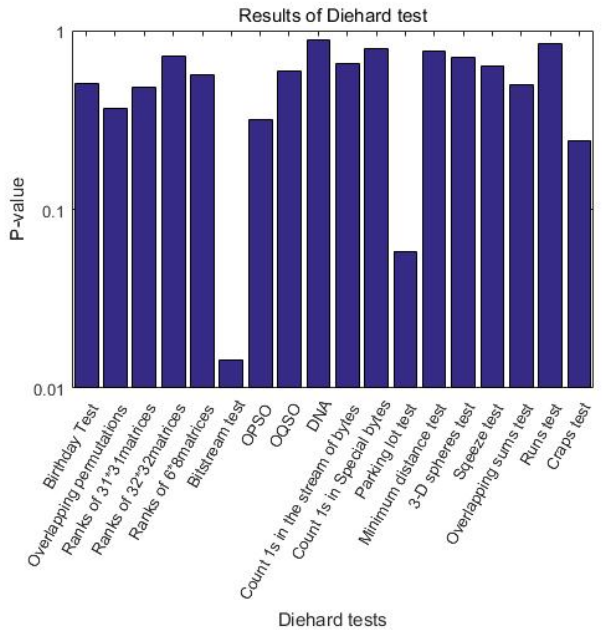

FIG. 9: Upper is the result of Diehard test of our final random sequence . The voltage of high level $V_h = 49.40V$ and the data size of original final sequence is 5Gb.

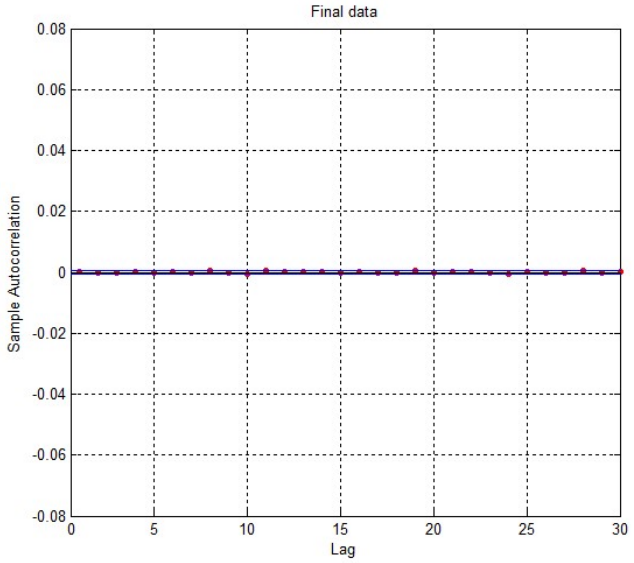

FIG. 10: Auto-correlation of the forgoing final data.

will focus on following questions:

1. Designing a trigger source with higher frequency, shorter pulse width and larger peak-peak voltage value.

2. Seeking a more stable and robust physical system as the tunneling source, in light of the disadvantages of our InGaAs/InP avalanche diode system.

3. Combination of this tunneling protocol and other QRNGs, as mentioned in [13][15][16][31].

Statistical Test	P-value	Proportion	Assessment
Frequency	0.484838	0.993355	Success
BlockFrequency	0.984047	0.986711	Success
CumulativeSums	0.557001	0.993355	Success
Runs	0.958728	0.996678	Success
LongestRun	0.981358	0.983389	Success
Rank	0.204974	0.986711	Success
FFT	0.071125	0.986711	Success
NonOverlappingTemplate	0.814243	0.976744	Success
OverlappingTemplate	0.274627	0.993355	Success
Universal	0.084015	0.983389	Success
ApproximateEntropy	0.959407	1.000000	Success
RandomExcursions	0.592779	0.977011	Success
RandomExcursionsVariant	0.452699	0.977011	Success
Serial	0.800792	0.990033	Success
LinearComplexity	0.982786	0.986711	Success

TABLE I: Result of NIST test for a $5Gb$ final data, The minimum pass rate for each statistical test with the exception of the random excursion (variant) test is approximately = 292 for a sample size = 301 binary sequences. The minimum pass rate for the random excursion (variant) test is approximately = 168 for a sample size = 174 binary sequences. As the confidence parameter $\alpha = 0.01$, our data passed the NIST test.

ACKNOWLEDGMENTS

We acknowledge Weixing Zhang and Hua Yuan for their assistance on the hardware designing. And we thank Pro.Xiongfeng Ma and Dr.Zhen Zhang for crucial discussions and Xinyu Liu, Nan Jiang for their guidance on the application of several sets of test software. Also, we thank the NSFC for its financial support.

APPENDIX: DETAILED RESULT OF RANDOMNESS TESTS

The detailed data analysis by NIST test is obtained by the official program 'sts' version 2.1.2, as shown in TABLE . And the detailed data analysis by Dihard test is shown as the following TABLEII:

* Electronic address: gllong@tsinghua.edu.cn

[1] J. E. Gentle, Random number generation and Monte Carlo methods pp. 1–60 (2003).
[2] J. Emerson, Y. S. Weinstein, M. Saraceno, S. Lloyd, and D. G. Cory, Science **302**, 2098 (2003).
[3] F.-G. Deng, G. L. Long, and X.-S. Liu, Phys. Rev. A **68**, 042317 (2003), URL `http://link.aps.org/doi/10.1103/PhysRevA.68.042317`.
[4] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Journal of cryptology **5**, 3 (1992).
[5] M. A. Nielsen and I. Chuang, *Quantum computation and quantum information* (2002).

StatisticalTest	P-value	Assessment
BirthdayTest	0.505898	Success
OverlappingPermutation	0.368835	Success
RanksOf31 × 31matrices	0.481990	Success
RanksOf32 × 32matrices	0.714278	Success
RanksOf6 × 8matrices	0.566601	Success
BitstreamTest	0.01443	Success
OPSO	0.317900	Success
OQSO	0.592000	Success
DNA	0.883100	Success
Count1$s$inTheStreamOfBytes	0.648895	Success
Count 1sInTheSpecialBytes	0.790766	Success
ParkingLotTest	0.058110	Success
MinimumDistanceTest	0.762900	Success
$3-D$ SpheresTest	0.705579	Success
SqueezeTest	0.634944	Success
OverlappingSumsTest	0.501220	Success
Runs	0.846631	Success
Craps	0.242872	Success

TABLE II: Result of Diehard test for a $5Gb$ final data, All of these indexes lies in$(0, 1)$, our data passed the Diehard test.

[6] T. Stojanovski and L. Kocarev, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications **48**, 281 (2001).

[7] J. Rarity, P. Owens, and P. Tapster, Journal of Modern Optics **41**, 2435 (1994).

[8] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, Journal of Modern Optics **47**, 595 (2000).

[9] Y.-Q. Nie, H.-F. Zhang, Z. Zhang, J. Wang, X. Ma, J. Zhang, and J.-W. Pan, Applied Physics Letters **104**, 051110 (2014).

[10] M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn, and O. Benson, Applied Physics Letters **98**, 171105 (2011).

[11] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, Optics letters **35**, 312 (2010).

[12] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, Optics express **20**, 12366 (2012).

[13] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Physical review letters **114**, 150501 (2015).

[14] J. Bowles, M. T. Quintino, and N. Brunner, Physical review letters **112**, 140407 (2014).

[15] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, et al., Phys. Rev. X **6**, 011024 (2016), URL `http://link.aps.org/doi/10.1103/PhysRevX.6.011024`.

[16] F. Xu, J. H. Shapiro, and F. N. Wong, Optica **3**, 1266 (2016).

[17] A. O. Caldeira and A. J. Leggett, Physical Review Letters **46**, 211 (1981).

[18] R. Banerjee and B. R. Majhi, Journal of High Energy Physics **2008**, 095 (2008).

[19] D. Schwartz, B. Sen, C. N. Archie, and J. Lukens, Physical review letters **55**, 1547 (1985).

[20] H. Kanbe, N. Susa, H. Nakagome, and A. Hiroaki, Electronics Letters **16**, 163 (1980).

[21] D. Renker, Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment **567**, 48 (2006).

[22] B. F. Aull, A. H. Loomis, D. J. Young, R. M. Heinrichs, B. J. Felton, P. J. Daniels, and D. J. Landers, Lincoln Laboratory Journal **13**, 335 (2002).

[23] J. L. Moll (1964).

[24] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, Physical Review A **87**, 062327 (2013).

[25] S. K. Tawfeeq, Journal of Lightwave Technology **27**, 5665 (2009).

[26] N. Susa, H. Nakagome, O. Mikami, H.-i. Ando, and H. Kanbe, IEEE Journal of Quantum Electronics **16**, 864 (1980).

[27] A. Tosi, A. Dalla Mora, F. Zappa, S. Cova, M. Itzler, and X. Jiang, in *SPIE OPTO: Integrated Optoelectronic Devices* (International Society for Optics and Photonics, 2009), pp. 72221G–72221G.

[28] G. Ribordy, J.-D. Gautier, H. Zbinden, and N. Gisin, Applied Optics **37**, 2272 (1998).

[29] S. R. Forrest, R. F. Leheny, R. E. Nahory, and M. A. Pollack, Applied Physics Letters **37**, 322 (1980), ISSN 0003-6951, URL `<GotoISI>://WOS:A1980KE04200028`.

[30] R. Konig, R. Renner, and C. Schaffner, IEEE Transactions on Information theory **55**, 4337 (2009).

[31] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, arXiv preprint arXiv:1510.08957 (2015).