Refined Stationary Randomness of Quantum Random Sequences on Variant Maps

Jeffrey Zheng, Yamin Luo and Zhefei Li

Abstract In this chapter, a testing model is used to apply statistical probability in multiple distributions on three maps for a selected sequence to check refined stationary randomness on quantum sequences. Three random data sequences are collected from two quantum random resources: one from Australian National University (ANU) and two (initial and secure) from University of Science and Technology of China (USTC). Multiple results are created on three maps, and measurements of stationary randomness are illustrated and compared. Three samples show distinct stationary properties.

Keywords Variant maps · Quantum random sequence · Chaotic random sequence Ordered measures · Maximal; Stationary randomness

1 Introduction

In advanced social network environment, multimedia signal sequences of big data streams are composed of time series processes. Quantum experiments in quantum satellite using quantum key distribution (QKD) systems [1] is the most advanced ICT

This work was supported by the Key Project on Electric Information and Next Generation IT Technology of Yunnan (2018ZI002), NSF of China (61362014), Yunnan Advanced Overseas Scholar Project.

J. Zheng (✉)
Key Laboratory of Quantum Information of Yunnan, Yunnan University, Kunming, China
e-mail: conjugatelogic@yahoo.com

J. Zheng
Key Laboratory of Software Engineering of Yunnan, Yunnan University, Kunming, China

Y. Luo · Z. Li
Yunnan University, Kunming, China
e-mail: 1047668416@qq.com

Z. Li
e-mail: 576167164@qq.com

J. Zheng (ed.), *Variant Construction from Theoretical Foundation to Applications*,
https://doi.org/10.1007/978-981-13-2282-2_20

development to establish ultra-secure quantum communications. For a QKD system, a truly random number generator [2] play a key role. From an analysis viewpoint, it is necessary to test stationary randomness in time variations. In this section, a list of relevant schemes: pseudo/truly random sequences, P_value, statistical probability distribution, optical statistics, stationary properties, and variant maps, are discussed.

1.1 Pseudo/True Random Sequences

1.1.1 Pseudorandom Sequences

Traditional stream ciphers [3] on linear feedback shift register structure (LFSR) are used as pseudorandom number generators. The LFSR stream ciphers are the core in classical stream ciphers.

The new generation of stream ciphers has being shifted from LFSR [3] to nonlinear modes: NLFSR, clock control [4] and nonlinear functions, etc. It is difficult to use nonlinear mathematical theories, recursive models, descriptive tools, and implementing schemes in nonlinear dynamic environments.

1.1.2 True Random Sequences

Differently from pseudorandom sequences generated by stream ciphers, high-quality stochastic oscillators of truly random sequences are generated from special hardware devices such as laser photonics [5], nonlinear optics, quantum optics [6], quantum noises, thermal noise, chaos, and fractal nonlinear dynamics [7].

1.2 Testing Schemes

1.2.1 P_value Schemes

Various statistic testing packages measure randomness properties on a given random sequence. NIST 800-22 package [8] is a typical representative to provide more than 15 testing schemes. Using the package, it is essential to check whether P_value >0.01 for the sequence. Since such measuring scheme provides a static condition, it is difficult to use only P_value parameter to express complex dynamic behaviors involved in random sequences.

1.2.2 Multiple Statistical Probability Distributions

Measuring random sequences under segment conditions, multiple statistical probability schemes are useful to create various distributions to illustrate complex spatial relationships.

Multivariate normal probability distributions are the most important and powerful tools to test stochastic characteristics of a random data sequence under the framework of probability, stochastic process and statistics [9] for nonlinear problems. In this kind of measuring models, when a data sequence is sufficiently long, the high dimensional probability distribution of the sequence [10] is converged to a continuous Gaussian distribution. Multivariate Gaussian probability distributions support various schemes to analyze complex stochastic data set of measuring sequences in continuous conditions.

1.2.3 Photon Statistic in Quantum Optics

Photon statistics is the theoretical and experimental approach on the statistical distributions in photon counting experiments to analyze the statistical nature of photons in a light source.

Three types of distributions can be obtained by the light source [11]: Poissonian, super-Poissonian, and sub-Poissonian. The variance and average number of photon counts are identified for the corresponding distribution. Both Poissonian and super-Poissonian light are described by a semi-classical theory in which the light source is modeled as an electromagnetic wave and the atom is modeled by quantum mechanics. In contrast, sub-Poissonian light requires the quantization of the electromagnetic field for a proper description and is a direct measure of the particle nature of light.

1.2.4 Stationary Properties

In mathematics and statistics, a stationary process is a stochastic process [12] whose joint probability distribution does not change when shift operations performed. Consequently, parameters such as mean and variance, if they are present, also do not change over time. Stationarity is an interesting property in time series analysis.

In applied mathematics, the Wiener–Khinchin theorem [13], states that the Autocorrelation Function (ACF) of a wide-sense stationary process has a spectral decomposition given by the power spectrum of the process. One of the effective ways for identifying stationary times series is the ACF plot [14]. For a stationary time series, the ACF will drop to zero relatively quickly.

1.3 Quantum Random Resources

Quantum random numbers can be generated from a physical quantum source of a coherent laser light to be splitting a beam of light into two beams and then measuring the power in each beam. Due to the light intensity in each beam fluctuates about the mean. Those fluctuations can be converted into a source of random numbers [15–17] being a stationary Poisson distribution.

1.3.1 ANU Resource

The ANU Quantum Random Numbers Server is an open website [18] to offer true random numbers to anyone on the internet. Such random numbers are generated in real-time by measuring the quantum fluctuations of the vacuum. The electromagnetic field of the vacuum exhibits random fluctuations in phase and amplitude at all frequencies. By carefully measuring these fluctuations, ultra-high bandwidth random numbers can be generated.

About 1 GB data streams are downloaded and 100 MB data streams are used for the testing.

1.3.2 USTC Resource

In the Key Laboratory of Quantum Information, USTC, and CAS, true random number sequences are generated [16]. This type of true random sequences supports advanced quantum communication devices of QKD systems [19].

More than 20 GB quantum random number sequences are provided by USTC for random streams testing. Two data sequences are represented as USTC_0 (initial) and USTC (secure), respectively. About 100 MB data streams are selected for each sequence.

1.3.3 Refined Properties

From an analysis viewpoint, a Toeplitz hash algorithm has used to get an initial sequence USTC_0 as input and USTC sequence as output. Checking such refined variations, this is an interesting property for us to make a detailed identification.

From a random testing viewpoint, initial sequences have some difficulties to pass NIST tests and secure sequences are ensured to pass NIST tests. Some refined differences on random characteristics could be distinguished.

1.4 Variant Framework

Various schemes following the top-down strategy are explored to use multiple measures to partition special phase spaces from a top state set to multiple bottom states via multilevels of a hierarchy in combinatorial algorithms [20], image analysis and processing for many years.

The conjugate classification [21] is proposed to apply seven measures in a hierarchy to partition the kernels of four regular plane lattices on $n = \{4, 5, 7, 9\}$ cases for 2D binary images. For 1D cellular automata sequences, global random behaviors are visualized in 2D maps.

For n-tuple bit vectors, the variant logic framework [22] is proposed, various applications are explored: 3D visual method on random number sequences [23], variant Pseudorandom Number Generator (PRNG) [24], computational simulation on quantum interactions [25], noncoding DNA analysis, bat echolocation [26], and stationary randomness [27].

1.5 Proposed Scheme

For the convenience of testing stationary randomness on random sequences, we propose a testing system for a stationary random sequence with length N, multiple segments M are divided from the sequence by a given length m, a 2-tuple pair of measures can be extracted from a 0-1 segment that are the number of 1 element and the number of 1 pattern in the segment. All paired measures are composed of a sequence of M pairs of measures as an ordered measuring set with M elements.

The pairs of the measuring sequence are directly separated as two independent measuring sequences to keep each parameter in the same order. A total of three sequences of distinct measures are constructed including two sequences on single measures and one sequence on 2-tuple measures.

Following this approach, two sets of single measuring sequences are sorted as two 1D numeric arrays as statistical histograms corresponding to 1D maps and the 2-tuple measuring sequence is sorted as a 2D integer array as statistic histograms being a 2D map. Under the controlling operations on the changes of shift displacement, multiple results of the three measuring sequences are transformed into 1D statistic histograms and 2D pseudo-color maps to show effective patterns from the generated sequence under various positions and conditions on a list of shift operations.

1.6 Organization of the Chapter

This chapter uses a testing system for a stationary random sequence on the system architecture in Sect. 2. In Sect. 3, test results are provided for two quantum random sequences. From the results of the visual maps in Sect. 3, result analysis and brief comparison are described in Sect. 4. And finally in Sect. 5, the main results are summarized.

2 Testing System

To describe the testing system, diagrams are shown in Fig. 1.

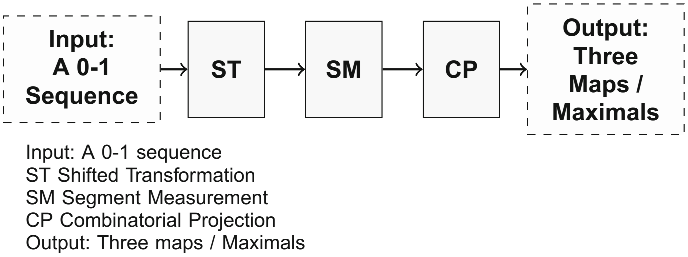
Input: A 0-1 Sequence
ST
SM
CP
Output: Three Maps / Maximals
Input: A 0-1 sequence
ST Shifted Transformation
SM Segment Measurement
CP Combinatorial Projection
Output: Three maps / Maximals

Fig. 1 The architecture of testing stationary random sequences

2.1 System Architecture

This system is composed of five parts: Input, Shifted Transformation (ST), Segment Measurement (SM), Combinatorial Projection (CP), and Output.

The input of the testing system is a selected 0-1 sequence and its output is composed of three maps, two in 1D and one in 2D for visual distributions, and three maximals to be processed by ST, SM, and CP modules, respectively.

Further technical details are described in Chapter. Stationary Randomness of Three Types of Six Random Sequences on Variant Maps of this book.

3 Testing Results

Three quantum random sequences are selected from ANU and USTC resources.

Typical results of testing stationary properties for three sequences in nine maps are shown in Fig. 2. Three sets of results are shown in Fig. 3a, b. In Fig. 3a, six values of $r = \{0, 16, 32, 96, 112, 128\}$ are selected to show three pairs of corresponding maps: 1DP, 2DPQ, and 1DQ for three sequences on the top part. Nine 2D maps of maximal curves for $r = 0 - 128$ are shown to illustrate refined properties in stationary random curves on the bottom column. In Fig. 3b, three maximal curves on three 2D maps are compared. In Fig. 4a–c, three larger maps on $r = \{48, 64, 80\}$ are shown corresponding to (a) 1DP, (b) 2DPQ, and (c) 1DQ for three cases. Three larger maps of three maximal curves are shown in Fig. 5.

3.1 Quantitative Measurements

For a G map, let G_x be an average variation, ΔG_x be a region of variations and $G_x^R = \Delta G_x / G_x$ be a variation ratio. In convenient in comparison, let {Max, Min} be the {largest, smallest} value on a maximal curve; Max-Min is its difference and $|ANU - USTC|$ is an absolute difference between ANU and USTC measures.

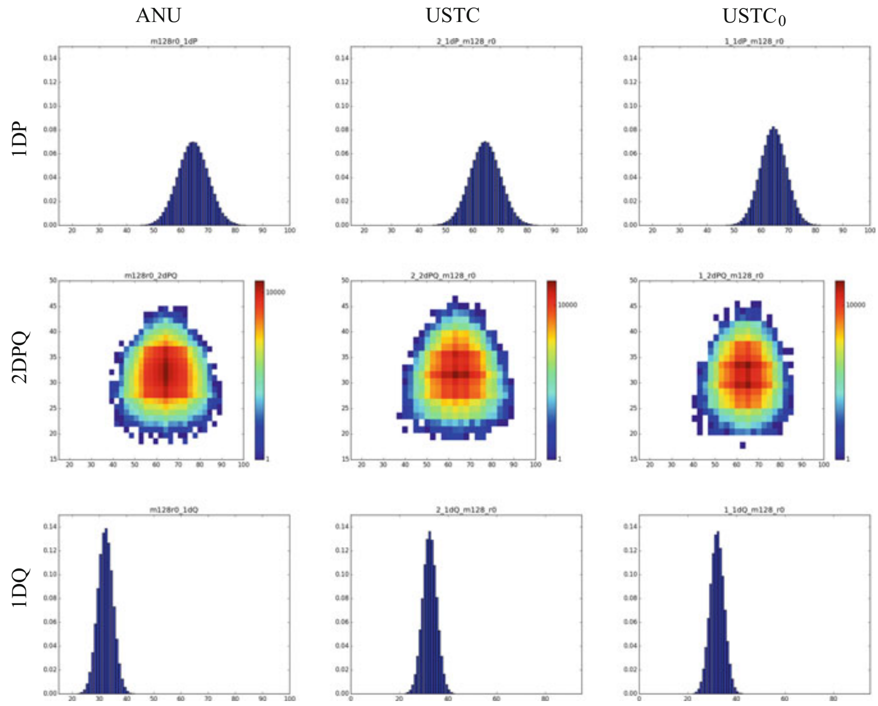

Fig. 2 ANU, USTC and USTC$_0$ random sequences on 1DP, 2DPQ, and 1DQ maps

Let $(Max - Min)/|ANU - USTC|$ be a relative ratio between (Max-Min) and $|ANU - USTC|$.

4 Result Analysis

Nine maps in Fig. 2 are in three columns. Three 1DP maps have similar distributions in bell shapes to illustrate Poissonian distributions. Three 2DPQ maps are 2D distributions and there are different symmetric distributions. Maximal elements in ANU, USTC, and USTC$_0$ maps show stronger vertical oriented features. Three maps have a symmetry on left/right directions and have a broken symmetry on up/down directions. Pseudo-color pixels on three maps are shown in 3D shapes. Compared with three 1DP maps, three 1DQ maps have similar distributions and more narrow bell shapes to illustrate sub-Poissonian distributions.

Six groups of results on shift $r : \{0, 16, 32, 96, 112, 128\}$ are shown in Fig. 3a on the top columns and each group contains nine distributions in three columns. Three random sequences have stronger stationary randomness that makes all maps in the similar style with minor changes on shift operations. Larger maps on $r = \{48, 64, 80\}$

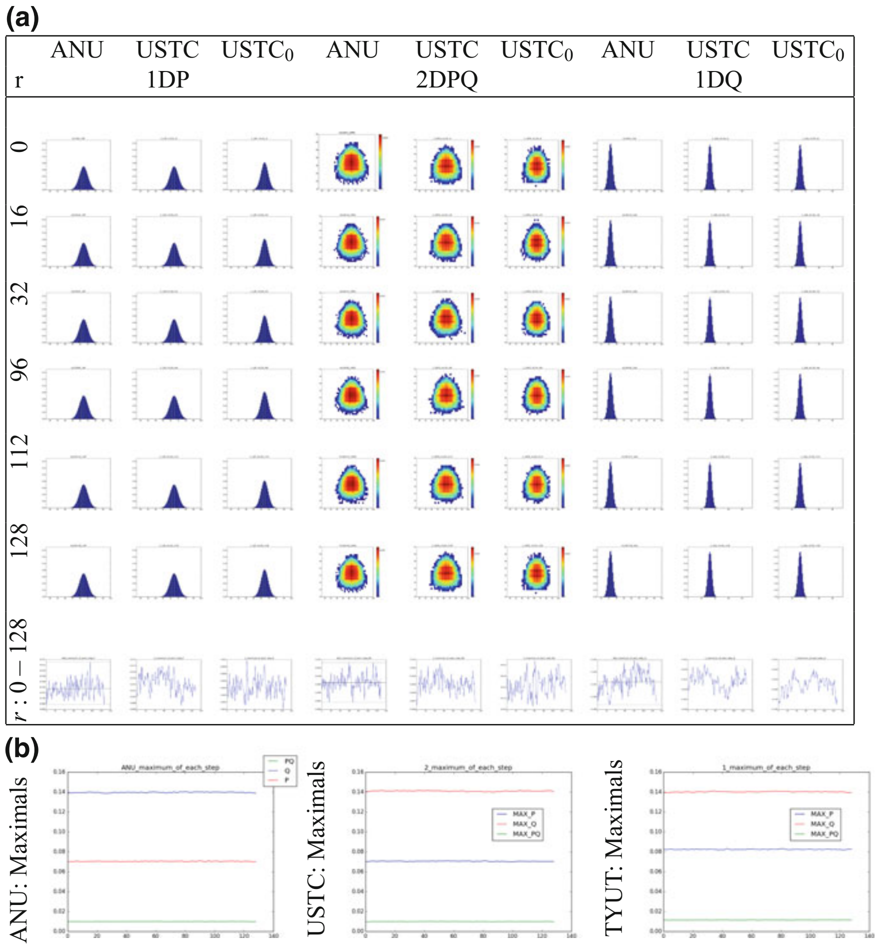

Fig. 3 ANU, USTC and USTC$_0$ random sequences on three maps and maximals (**a**), (**b**); **a** Three pairs of nine variant maps in six groups and three pairs of nine maximal maps; **b** Three 2D maps of three maximal curves for ANU, USTC, and USTC$_0$

in Fig. 4a–c provide refined visual information to show their variations in details. Enlarged and larger maximal curves are shown in Figs. 3b and 5 for $r : 0 - 128$ as nine 2D maps with values of average variation and region of variations. From the maximal and minimal stationary regions, there are 1–2% variation ratios for 1DP and 1DQ and 5% variation ratios for 2DPQ observed. Three curves of maximals on three 2D maps are illustrated in Figs. 3b and 5.

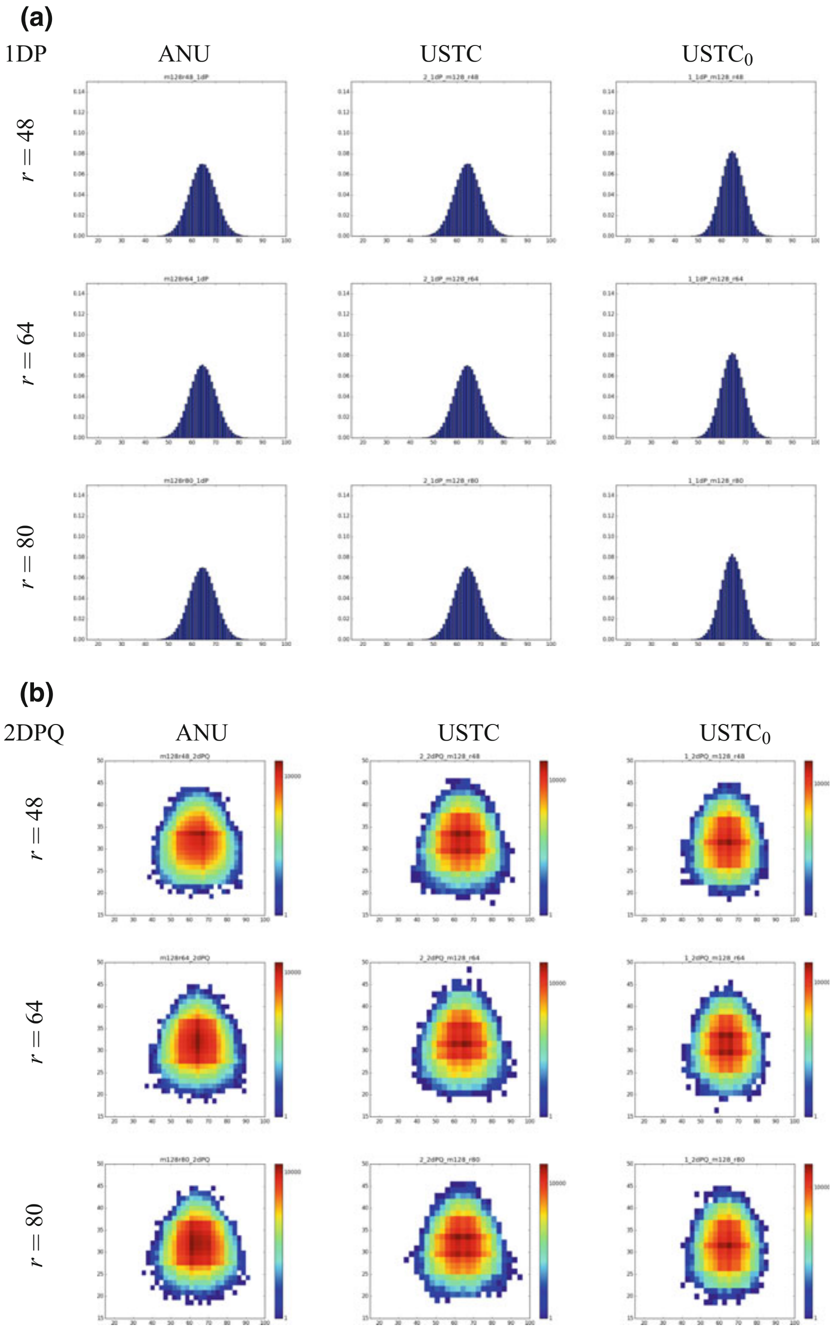

Fig. 4 ANU, USTC, and USTC$_0$ random sequences random sequences on enlarged maps, $r = \{48, 64, 80\}$; **a** 1DP; **b** 2DPQ; **c** 1DQ

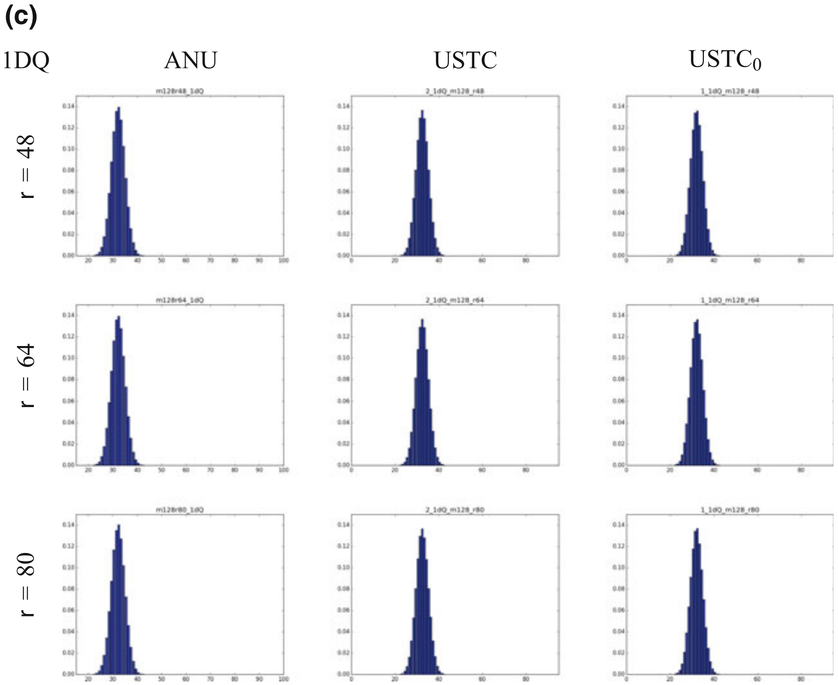

Fig. 4 (continued)

4.1 *Relative Ratios on Differences*

Details of three maximal measures are compared in Table 1. Three parameters $\{Q_x, \Delta Q_x, Q_x^R\}$ on 1DQ maps have 1 values on Max-Min and $|ANU - USTC|$ ratios; there are 81 on P_x and 1.6 on P_x^R and there are 65 on PQ_x and 7.9 on PQ_x^R observed.

From this set of testing results, two samples of ANU and USTC are showing similar stationary properties and USTC$_0$ with different stationary properties among the three sequences. Significant differences of relative ratios are observed from 2DPQ variation measurements.

Fig. 5 Three enlarged 2D maps of three maximal curves for ANU, USTC, and USTC$_0$

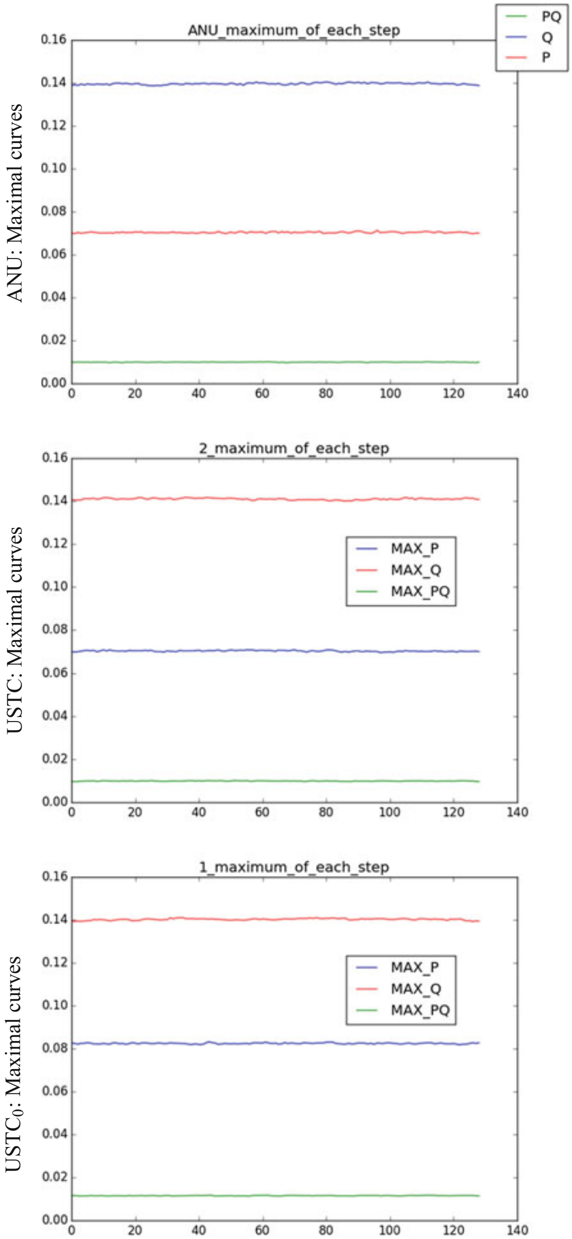

Table 1 Comparisons on three measures for ANU, USTC, and USTC$_0$ samples

	Q_x	ΔQ_x	Q_x^R
ANU:	13.961%	0.17761%	1.2722%
USTC:	14.09%	0.18%	1.27%
USTC$_0$:	14.02%	0.18%	1.27%
Min:	13.961%	0.17761%	1.27%
Max:	14.09%	0.18%	1.2722%
Max−Min:	0.129%	0.0239%	0.0022%
$\|ANU-USTC\|$:	0.129%	0.0239%	0.0022%
$(Max-Min)/\|ANU-USTC\|$:	1	1	1
	P_x	ΔP_x	P_x^R
ANU:	7.0352%	0.15472%	2.1992%
USTC:	7.05%	0.13%	1.87%
USTC$_0$:	8.24%	0.14%	1.68%
Min:	7.0352%	0.13%	1.68%
Max:	8.24%	0.15472%	2.1992%
Max−Min:	1.2048%	0.02472%	0.5192%
$\|ANU-USTC\|$:	0.0148%	0.02472%	0.3292%
$(Max-Min)/\|ANU-USTC\|$:	81	1	1.6
	PQ_x	ΔPQ_x	PQ_x^R
ANU:	0.99245%	0.04791%	4.8276%
USTC:	0.99%	0.05%	5.01%
USTC$_0$:	1.15%	0.05%	3.56%
Min:	0.99%	0.04691%	3.56%
Max:	1.15%	0.05%	5.01%
Max−Min:	0.16%	0.00209%	1.45%
$\|ANU-USTC\|$:	0.00245%	0.00209%	0.1824%
$(Max-Min)/\|ANU-USTC\|$:	65	1	7.9

5 Conclusion

It is feasible to evaluate stationary randomness for a random sequence using the testing system. From three maps {1DP, 1DQ, 2DPQ}, maximals are identified for shift $r : 0 - m$. Three 2D maps of maximal curves provide refined characteristics to evaluate stationary randomness. Further explorations and applications are required to check the testing system on other applications.

Acknowledgements Thanks to the Key project of Quantum Communication of Yunnan Province, National Science Foundation of China (61362014) and High-Level Overseas Professional Project of Yunnan Province for financial supports to this project. Thanks to the Key Laboratory of Quantum Information, USTC, CAS, and the ANU Quantum Optical Laboratory for providing quantum random sequences.

References

1. Quantum key distribution, https://en.wikipedia.org/wiki/Quantum_key_distribution
2. Random number generation, https://en.wikipedia.org/wiki/Random_number_generation
3. S. Golomb, *Shift-Register Sequences*, Revised edn. (Aegean Park Press, Laguna Hills, California, 1982)
4. de A. Queiroz, J. Schechtman, Elimination of nonlinear clock feedthrough in component-simulation switched-current circuits. in *Proceedings of the 1998 IEEE International Symposium on Circuits and Systems, 1998. ISCAS '98* (II378-II381, 1998)
5. D. Meschede, in *Optics, Light and Lasers*, 2nd edn. (Wiley-VCH, 2007)
6. M. Nakazawa et al., QAM quantum stream cipher using digital coherent optical transmission. Opt. Expr. **22**(4), 4098–4107 (2014)
7. S. Lian et al., A chaotic stream cipher and the usage in video protection. Chaos Solitons Fractals **34**(3), 851–859 (2007)
8. NIST, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications (NIST, Special Publication, 2010)
9. K. Ito, Gaussian filter for nonlinear filtering problems, in *Conference on decision and control*, pp. 1218–1223 (2000)
10. F. Orieux, O. Feron, J. Giovannelli, Sampling high-dimensional Gaussian distributions for general linear inverse problems. IEEE Signal Process. Lett. **19**(5), 251–254 (2012)
11. M. Fox, *Quantum Optics: An Introduction* (Oxford University Press, New York, 2006)
12. M.B. Priestley, in *Non-linear and Non-stationary Time Series Analysis* (Academic Press, 1988)
13. N. Wiener, *Time Series* (Cambridge, M.I.T Press, 1964)
14. Stationary process, https://en.wikipedia.org/wiki/Stationary_process
15. A.E. Ivanova, Using optical splitters in quantum random number generators based on fluctuations of vacuum. J. Phys., Conf. Ser. **735**, 012077 (2016)
16. X.T. Song, Phase-coding self-testing Quantum random number generator. Chin. Phys. Lett. **32**(8), 080302–080310 (2015)
17. T. Symul, S.M. Assad, P.K. Lam, Real time demonstration of high bitrate quantum random number generation with coherent laser light. Appl. Phys. Lett. **98**, 231103 (2011)
18. Quantum random number generator, http://photonics.anu.edu.au/qoptics/Research/qrng.php
19. W. Chen, Active phase compensation of quantum key distribution system. Chin. Sci. Bull. **53**(9), 1310–1314 (2008)
20. D.E. Knuth. *The Art of Computer Programming*, vol 4A: Combinatorial Algorithms Part 1 (Addison-Wesley, 2011)
21. Z.J. Zheng, *Conjugate Transformation of Regular Plan Lattices for Binary Images*, Ph.D. Thesis (Monash University, 1994)
22. J. Zheng, C. Zheng, A framework to express variant and invariant functional spaces for binary logic. Front. Electr. Electron. Eng. China **5**(2), 163–172 (2010) Higher Educational Press and Springer, https://doi.org/10.10072Fs11460-010-0011-4
23. H. Wang, J. Zheng, 3D visual method of variant logic construction for random sequence, in *Australian Information Warfare and Security*, pp. 16–27 (2013)
24. J. Zheng, Novel Pseudo-Random number generation using variant logic framework, in *2nd International Cyber Resilience Conference*, 10bit04 (2011). http://igneous.scis.ecu.edu.au/proceedings/2011/icr/zheng.pdf

25. J. Zheng, C. Zheng, T.L. Kunii, Interactive maps on variant phase space, in *Emerging Application of Cellular Automata*, (InTech Press, 2013) pp. 113–196
26. D.M. Heim, O. Heim, P.A. Zeng, J. Zheng, Successful creation of regular patterns in variant maps from bat echolocation calls. Biol. Syst.: Open Access **5**, 2 (2016). https://doi.org/10.4172/2329-6577.1000166
27. J. Zheng, C. Zheng, Stationary randomness of quantum cryptographic sequences on variant maps, in *Proceedings on ASONAM '17*, (ACM, 2017). ISBN 987-1-4503-4993-2/17/07, https://doi.org/10.1145/3110025.3110151