Stationary Randomness of Three Types of Six Random Sequences on Variant Maps

Jeffrey Zheng, Yamin Luo, Zhefei Li and Chris Zheng

Abstract Various random streams have different stationary properties. It is necessary to use statistical probability and time series to evaluate quality of stationary randomness. In this chapter, a testing model is used on three maps for a random sequence. Multiple segments are divided on the shifted sequence as three measuring sets. For a map, the maxima are extracted and three maximal values are identified. 2D maps represent stationary randomness. Conditions of station random/stationary sequences are investigated. Testing sets are collected from three types of six random resources: AES, DES, A5, RC4, Australian National University (ANU), and University of Science and Technology of China (USTC) (two block ciphers, two stream ciphers, and two quantum ciphers). Six random sequences are selected. Measurements of stationary randomness are compared. There are only 0.0034–4.27% differences that are recognized. Using variation ratios, six samples are composed of three variation categories on {AES, DES}, {A5, RC4}, and {ANU, USTC}, respectively. From a measuring viewpoint, all six samples are showing distinguished stationary randomness properties.

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

J. Zheng (✉) · Y. Luo · Z. Li · C. 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
e-mail: conjugatelogic@yahoo.com

Y. Luo
e-mail: 1047668416@qq.com

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

C. Zheng
e-mail: z@caudate.me

J. Zheng (ed.), *Variant Construction from Theoretical Foundation to Applications*,
https://doi.org/10.1007/978-981-13-2282-2_8

Keywords Stationary randomness · Segment · Shifted sequence · Maxima
Quantum sequence · Variation ratio

1 Introduction

In modern cyberspace environment [1], network communication technologies play the essential role to support advanced developments of science, technology, and social daily life in every aspect. From a security viewpoint of network communication, Communication Security (COMSEC) systems [2] are the most important part. Every COMSEC system depends on block cipher/stream cipher/hash technologies, and its core component is linked to a random number generator for any cryptographic applications.

Quantum satellite [3] using Quantum Key Distribution (QKD) systems [4] in cryptographic applications is the most advanced ICT development to establish ultra-secure quantum communications. For a QKD system, a truly random number generator [5], quantum random number generator, plays a key role.

From a reliable viewpoint, it is necessary to test stationary randomness degrees on shift operations in evaluations. In this section, a list of relevant schemes, pseudo-random/truly random sequences, P_value, statistical probability distribution, optical statistics, stationary/nonstationary properties, and variant maps, are discussed.

1.1 Pseudorandom Sequences from Linear Stream Ciphers

Traditional stream ciphers [6] on Linear Feedback Shift Register (LFSR) structure (in military cryptography) are used as pseudorandom number generators, due to the ease of implementation from simple hardware, long periods, and uniformly distributed streams. The LFSR stream ciphers are the core in classical stream ciphers through the mathematical theory of algebraic functions for system simulation and analysis.

However, an LFSR is a linear system leading to fairly easy cryptanalysis using the Berlekamp–Massey algorithm. Important LFSR-based stream ciphers A5/1 & A5/2 are used in GSM cell phones and E0 is used in Bluetooth protocol. But from cryptanalysis viewpoint, the A5/2 cipher has been broken and both A5/1 and E0 have serious weaknesses [7, 8].

1.2 Pseudorandom Sequences from Nonlinear Stream Ciphers

The new generation of stream ciphers [9, 10] is widely used in advanced cyber communications. Three general methods are applied to improve security weaknesses in LFSR-based stream ciphers:

1. **Nonlinear Functions**: Nonlinear combination of several bits from the LFSR state [11];

2. **Nonlinear Parts**: Nonlinear combination of the output bits of two or more LFSRs or using evolutionary algorithm for nonlinearity [12]; and
3. **Clock Control**: Irregular clocking of the LFSR, as in the alternating step generator [13].

With batch a series of nonlinear algorithms are emerged [14]: nonlinear equivalence [15], evolutionary methods [12], AES cipher [16], RC4 [17], ZUC [11], cellular automata [18], and nonlinear dynamic system [19].

The new generation of stream ciphers has being shifted from the traditional mode: LFSR [6] to various nonlinear modes: NLFSR [20, 21], clock control [13], nonlinear functions [11], etc.; it is essential for ciphers to be integrated and implemented [22] to satisfy security models. However, different from LFSR with well-established linear mathematical theories and simulation tools, it is extremely difficult to use advanced nonlinear mathematical theories, recursive models, descriptive tools, and implementing schemes [19] in nonlinear dynamic environments. How to evaluate cryptographic sequences generated from the nonlinear stream ciphers is an urgent problem for modern stream/block ciphers.

1.3 Truly Random Sequences from Hardware Devices

In addition to pseudorandom sequences generated by stream ciphers, high-quality stochastic oscillators of truly random sequences are generated from special hardware devices such as laser photonics [23], nonlinear optics [24], quantum optics [25], quantum noises [26], thermal noise [27], and chaos and fractal nonlinear dynamics [28].

Since various truly random sequences are created from specific physical models with special principles and uncertain methodologies, it is extremely difficult for cryptographic researchers to make proper measurements explore nonlinear dynamic properties.

1.4 P_value Schemes—Statistical Tests on Cryptographic Sequences

Randomness has being explored for many years [29] on a series of statistic testing theories and methods. From a testing viewpoint, it is feasible to apply statistic testing packages to measure randomness properties on a given cryptographic sequence. NIST 800-22 package is a typical representative to provide more than 15 testing schemes for evaluation. Using the testing package, it is essential to check whether P_value $>$0.01 for the sequence. Since such measuring scheme provides static property, it is difficult to use only P_value parameter to express complex dynamic behaviors intrinsically involved in cryptographic sequences.

Since comprehensive behaviors in nonlinear dynamics may increase computational complexities tragically to involve complicated dynamic properties in the multivariate environment, those dynamic behaviors are completely ignored in P_value schemes.

1.5 Multiple Statistical Probability Distributions

Measuring cryptographic 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 tool to test stochastic characteristics of a random data sequence [30] under the framework of probability, stochastic process, and statistics [31] for nonlinear problems. In this kind of measuring models, when a data sequence is sufficiently long, the high-dimensional probability distribution of the sequence [32] is converted into a continuous Gaussian distribution.

A typical projection model is shown in Fig. 1a; the central part shows a Gaussian surface with an unbalanced distribution in a 2D plane distributed as $P(X, Y)$ measures with pseudo-colors and two 1D projections shown in horizontal $P(X)$ and vertical $P(Y)$ planes, respectively. In Fig. 1b, a standard Gaussian surface with

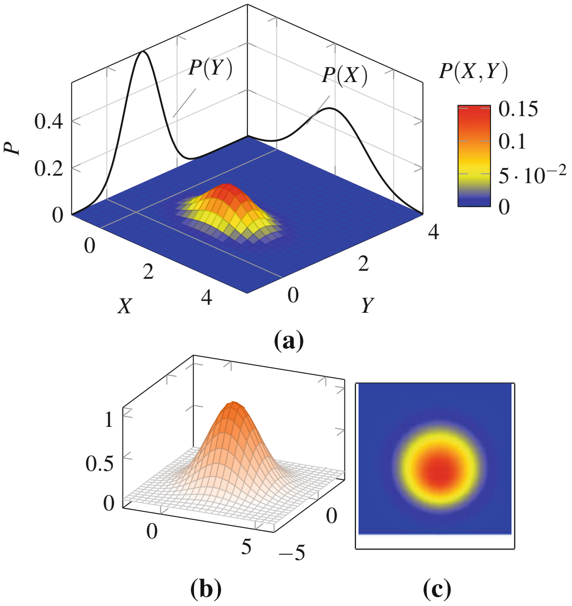


Fig. 1 Multivariate Gaussian Probability Distributions (**a**)–(**c**); **a** Bivariate normal distribution with two probability projections; **b** A symmetric bivariate normal surface with pseudo-colors; **c** A 2D pseudo-color map of the symmetric bivariate normal surface

symmetric shapes is illustrated and the 2D projection of its pseudo-color map is shown in Fig. 1c with continuous distribution of color on the map.

From sample figures, the relationship between the projection curve and two 1D Gaussian distributions are observed in the multivariate normal probability environment. Multivariate Gaussian probability distributions support various schemes to analyze complex stochastic data set of measuring sequences in many applications in continuous conditions.

1.6 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 statistical distributions shown in Fig. 2 can be obtained by the light source [33]: 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.

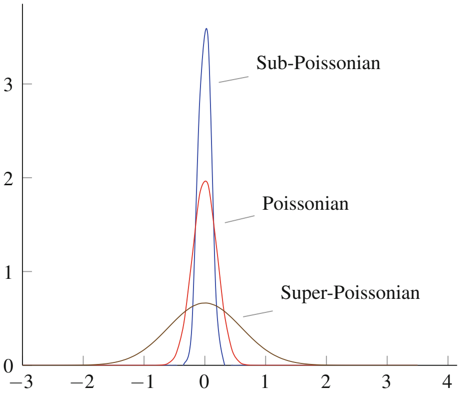


Fig. 2 Three-photon statistical distributions

1.7 Stationary and Non-stationary Properties

In mathematics and statistics, a stationary process is a stochastic process [34] 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 for many statistical procedures in time series analysis.

In 1938, Kolmogorov established the basic theorems for smoothing and predicting stationary stochastic processes [35, 36] that had major military applications during the Cold War.

In applied mathematics, the Wiener–Khinchin theorem [37–39] 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 identifying stationary times series is the ACF plot [40]. For a stationary time series, the ACF will drop to zero relatively quickly, while the ACF of nonstationary data decreases slowly [41].

1.8 Datastreams

1.8.1 Pseudorandom Number Resources

Four cryptographic sequences are selected: {AES,DES, A5, RC4}. For each cipher, a cryptographic sequence of 100MB data streams is collected.

{AES, DES} are block ciphers [16] on OFB mode to transfer block cipher output as a stream cipher stream.

A5/1 is a stream cipher [42] based around a combination of three LFSRs with irregular clocking.

RC4 is a stream cipher [43] designed by Ron Rivest in 1987. The design of RC4 avoids the use of LFSRs, its structure is ideal for software implementation, and it requires only byte manipulations.

1.8.2 Two Quantum Random Number Resources

Reliable and unbiased random numbers are important in cryptographic applications. Many algorithms can be used to generate pseudorandom numbers, but they can never be perfectly random or indeterministic.

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, it fluctuates about the mean. Those fluctuations can be converted into a source of random numbers [44–46] being a stationary Poisson distribution.

Two quantum cryptographic resources are selected: {ANU, USTC}. For each quantum cipher, a truly random sequence of 1GB data streams is collected.

USTC resource: In the Key Laboratory of Quantum Information, USTC, CAS, true random number sequences are generated [45]. This type of true random sequences supports advanced quantum communication devices of QKD systems [47, 48].

More than 20GB quantum random number sequences are provided by USTC for randomness testing.

ANU resource: The ANU Quantum Random Numbers Server is an open website [49] 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. Relevant data streams are downloaded.

1.9 Variant Framework

The conjugate classification [50] 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 [51] are visualized in 2D maps.

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 [52], image analysis, and processing for many years.

For n-tuple bit vectors, the variant logic framework [53] is proposed, and various applications are explored: 3D visual method on random number sequences [54], variant Pseudorandom Number Generator (PRNG) [55, 56], computational simulation on quantum interactions [57, 58], noncoding DNA analysis [59], and bat echolocation [60].

1.10 Proposed Scheme

For the convenience of testing stationary randomness on six cryptographic 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 is the number of 1 element and the number of 01 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.

1.11 Organization of the Chapter

This chapter describes a testing system for a stationary random sequence on diagrams of the system architecture and the core modules with input/output and processing functions in Sect. 2. In Sect. 3, the relationships among measuring sequences and the three statistical distribution maps are analyzed. In Sect. 4, four random sequences are generated from {AES, DES, A5, RC4} ciphers and two quantum cryptographic sequences collected from the Key Laboratory of Quantum Information, USTC, CAS, and ANU quantum number site. From the results of the visual maps in section IV, numeric analysis and brief comparison are carried out in Sect. 5. And finally in Sect. 6, the main results are summarized.

2 Testing System

To describe the testing system, diagrams are shown in Fig. 3.

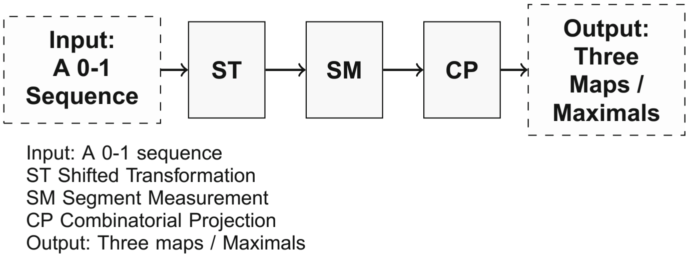


Fig. 3 The architecture of testing stationary random sequences

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.

2.2 Core Modules

The testing system consists of three modules: {ST, SM CP}.
Input: X $N = m * M$ bit sequence; m segment length; M total segments; r shift length;
Output: Three maps {1DP, 1DQ, 2DPQ}; Three maximals {1DP$_x$, 1DQ$_x$, 2DPQ$_x$}
Process: Shifting r position from X to be $Y = X(r)$ in ST. Making segment measuring sequences in SM and then projecting three measuring sequences as three maps and extracting three maximals in CP.

Let X, Y be 0–1 sequences with N elements, and the ST module takes the sequence X as input, then shift r position on the whole sequence to be the shifted sequence $Y = X(r)$ (i.e., a cyclic shift right + or shift left −).

$$\begin{gathered} Y = X(r), Y[I] = X[I \pm r], I \pm r(modN), \\ 0 \leq I < N; X[I], Y[I] \in \{0, 1\} \end{gathered} \tag{1}$$

In the SM module, the shifted vector is inputted and will be divided from a long sequence into M segments. For the i-th sub-vector, $0 \leq i < M$ on the j-th position $0 \leq j < m$, denoted as $Y_{i,j}$.

This sequence at the end of sub-vectors after the segmenting operation forms an $m * M$ matrix, m positions for the i-th complete row vector in the sequence correspond to a pair of 2-tuple measures: (p_i, q_i).

$$Y = \{Y_i\}_{i=0}^{M-1} \tag{2}$$

$$\begin{gathered} Y_i = \{Y_{i,0}, Y_{i,1}, \cdots, Y_{i,j}, \cdots, Y_{i,m-1}\} \\ 0 \leq i < M, 0 \leq j < m \end{gathered} \tag{3}$$

$$Y_i \to (p_i, q_i), 0 \leq i < M \tag{4}$$

$$\{Y_i\}_{i=0}^{M-1} \to \{(p_i, q_i)\}_{i=0}^{M-1} \tag{5}$$

The pair of 2-tuple measures (p_i, q_i) is determined by the following formula:

$$\begin{aligned} Y_{i,j} &= Y[J] \in \{0, 1\};\ J = i * m + j, \\ &\quad 0 \le i < M, 0 \le j < m, 0 \le J < m * M \qquad (6) \\ p_i &= \sum_{j=0}^{m-1} Y_{i,j}, Y_{i,j} \in \{0, 1\}, 0 \le p_i \le m; \qquad (7) \\ q_i &= \sum_{j=0}^{m-1} [(Y_{i,j-1}, Y_{i,j}) == (0, 1)], \\ &\quad j - 1(mod\ m), 0 \le q_i \le \lfloor m/2 \rfloor; \qquad (8) \end{aligned}$$

That is, $X = 0011010010, N = 10, M = 2, m = 5$; $(p_0 = 2, q_0 = 1)$; $(p_1 = 2, q_1 = 2)$.

The SM outputs the ordered M pairs of 2-tuple measures $\{p_i, q_i\}_{i=0}^{M-1}$.

The CP module consists of two units: Split and projection. The split adapts the SM's output as the input, and the 2-tuple measuring sequence $\{(p_i, q_i)\}_{i=0}^{M-1}$ will be splitted into two independent measuring sequences:$\{p_i\}_{i=0}^{M-1}$, $\{q_i\}_{i=0}^{M-1}$ to keep the original order invariant.

Three measure sequences are $\{p_i\}_{i=0}^{M-1}$, $\{q_i\}_{i=0}^{M-1}$, $\{(p_i, q_i)\}_{i=0}^{M-1}$.

The projection unit consists of three steps: Project Array (PA), Color Map (CM), and Get Maximal (GM). For three measuring sequences, two types of 1D and 2D measures will be processed separately.

The PA processes measuring sequences to transform them into integer arrays and the CM will organize them on either normalized histograms (1D measures) or color maps (2D measures), respectively.

The 1D measures involve two measuring sequences: $\{p_i\}_{i=0}^{M-1}$, $\{q_i\}_{i=0}^{M-1}$. Let $P[m + 1]$, $Q[\lfloor m/2 \rfloor + 1]$ and $NP[m + 1]$, $NQ[\lfloor m/2 \rfloor + 1]$ be two 1D (integer, float) arrays to represent the corresponding elements.

The 1DP statistic histogram is generated from a sequence $\{p_i\}_{i=0}^{M-1}$, NP, P two arrays (floating point, integer) with $(m + 1)$ elements. For the j-th element $NP[j]$, $P[j]$, $0 \le j \le m$, and 1DP$_x$ the maximal element, the output can be obtained by following procedure:

```
Initialization: $\forall NP[j] = 0.0,$
                $P[j] = 0, 0 \le j \le m;$
   Calculation: $for(i = 0; i < M; i + +)$
                $\{P[p_i] + +; \}$
 Normalization: $for(j = 0; j \le m; j + +)$
                $\{NP[j] = P[j]/M; \}$
   Get Maximal: $1DP_x = max\{NP[j] | 0 \le j \le m\}$
```

In the 1DP map, the PA corresponds to initialization and calculation; the MA handles normalization and the GM identifies the maximal element of the map.

The 1DQ statistic histogram is generated from a sequence $\{q_i\}_{i=0}^{M-1}$, NQ, Q two arrays (floating point, integer) with $(\lfloor m/2 \rfloor + 1)$ elements. For the j-th element $NQ[j]$, $Q[j], 0 \leq j \leq \lfloor m/2 \rfloor$, and 1DQ$_x$ the maximal element, the output can be obtained from following procedure:

```
 Initialization: $\forall NQ[j] = 0.0,$
                 $Q[j] = 0, 0 \leq j \leq \lfloor m/2 \rfloor;$
    Calculation: $for(i = 0; i < M; i++)$
                 $\{Q[q_i]++;\}$
  Normalization: $for(j = 0; j \leq \lfloor m/2 \rfloor; j++)$
                 $\{NQ[j] = Q[j]/M;\}$
    Get Maximal: 1DQ$_x = max\{NQ[j] | 0 \leq j \leq \lfloor m/2 \rfloor\}$
```

Using P, NP, Q, NQ arrays, it is possible to generate corresponding 1D statistical histograms as 1D maps.

In the 1DQ map, the PA corresponds to initialization and calculation; the MA handles normalization and the GM identifies the maximal element of the map.

The 2D measures specially processes one measuring sequence: $\{(p_i, q_i)\}_{i=0}^{M-1}$. Let $PQ[m + 1 : \lfloor m/2 \rfloor + 1]$ be a 2D integer array.

2DPQ statistic histogram is generated from a sequence$\{(p_i, q_i)\}_{i=0}^{M-1}$, PQ a 2D integer array with $(m + 1) * (\lfloor m/2 \rfloor + 1)$ elements; For the i, j-th element $PQ[i, j], 0 \leq i \leq m, 0 \leq j \leq \lfloor m/2 \rfloor$, and 1DPQ$_x$ the maximal element, their values can be obtained by following procedure:

```
Initialization: $\forall PQ[i, j] = 0,$
                $0 \leq i \leq m, 0 \leq j \leq \lfloor m/2 \rfloor;$
   Calculation: $for(i = 0; i < M; i++)$
                $\{PQ[p_i, q_i]++;\}$
  Pseudo-color: Matching proper color for
                $\forall PQ[i, j], 0 \leq i \leq m, 0 \leq j \leq \lfloor m/2 \rfloor$
   Get Maximal: 1DPQ$_x = max\{PQ[i, j] | 0 \leq i \leq m,$
                $0 \leq j \leq \lfloor m/2 \rfloor\}$
```

In the 2DPQ map, the PA corresponds to initialization and calculation; the MA handles pseudo-color and the GM identifies the maximal element of the map.

Through the CP module, three measuring sequences are transformed into two 1D arrays and one 2D array with $(m + 1)$, $(\lfloor m/2 \rfloor + 1)$ and $(m + 1) * (\lfloor m/2 \rfloor + 1)$ clusters.

The outputs of the testing system are three maps {1DP, 1DQ, 2DPQ} and three maximals {1DP$_x$, 1DQ$_x$, 2DPQ$_x$} as expected statistic distributions and representatives of the input 0–1 sequence, respectively.

3 Association Analysis

It is a counting scheme to sort the $\{p_i\}_{i=0}^{M-1}$ measuring sequence as a 1D histogram. When the measuring sequence meets ideal conditions, the 1D statistical distribution is a binomial distribution.

Lemma 1 *For an input 0–1 sequence, if the total number of segments is equal to $M = 2^m$, and each segment of m bits appears only once in the sequence, then the 1DP array satisfies the binomial distribution*

$$p[i] = \binom{m}{i}, 0 \leq i \leq m \tag{9}$$

Corollary 1 *If the input sequence meets the conditions of Lemma 1, then the total number of items in the 1DP array is equal to*

$$\sum_{i=0}^{m} p[i] = 2^m = M \tag{10}$$

Lemma 2 *If the input sequence meets the conditions of Lemma 1, then the 1DQ array satisfies following relation:*

$$Q[i] = 2\binom{m}{2i}, 0 \leq i \leq \lfloor m/2 \rfloor \tag{11}$$

Corollary 2 *If the input sequence meets the conditions of Lemma 1, then the total number of items in the 1DQ array is equal to*

$$\sum_{i=0}^{m/2} Q[i] = 2^m = M \tag{12}$$

Corollary 3 *For any 0–1 sequence with N elements, a 2DPQ projection in two directions is corresponding to either a 1DP array or a 1DQ array, respectively.*

Proof A 2DPQ array is generated from a measuring sequence $\{p_i, q_i\}_{i=0}^{M-1}$ and the 2DPQ array is sorted by $\{PQ[i, j]\}_{i=0}^{m}{}_{j=0}^{\lfloor m/2 \rfloor}$, from two directions $P[i] = \sum_{j=0}^{\lfloor m/2 \rfloor} PQ[i, j], 0 \leq i \leq m$; $Q[j] = \sum_{i=0}^{m} PQ[i, j], 0 \leq j \leq \lfloor m/2 \rfloor$. So two projections are corresponding to an either 1DP or 1DQ array.

Corollary 4 *For an arbitrary 0–1 input sequence, the total number of items in the 2DPQ array is equal to*

$$\sum_{i=0}^{m} \sum_{j=0}^{\lfloor m/2 \rfloor} PQ[i, j] = \sum_{i=0}^{m} P[i] = \sum_{j=0}^{\lfloor m/2 \rfloor} Q[j] = M \tag{13}$$

In Corollaries 3 and 4, the total number of each component on three statistic arrays is equal to the total number of segments M, and the 2DPQ array occupies a central position in the projection to other two arrays.

Let $\{1\mathrm{DP}_x(r), 1\mathrm{DQ}_x(r), 2\mathrm{DPQ}_x(r)\}$ denote three maximals on the selected sequence for $0 \le r \le m$; three maximal sequences are $\{1\mathrm{DP}_x(r)\}_{r=0}^m$, $\{1\mathrm{DQ}_x(r)\}_{r=0}^m$, $\{2\mathrm{DPQ}_x(r)\}_{r=0}^m$.

For a 0–1 sequence with M segments, if each segment of m bits is composed of a state and only one state is involved, then the sequence is a circular sequence.

Lemma 3 *For a sequence $0 \le r \le m$, the sequence is a circular sequence, iff $1DP_x(r) = 1DQ_x(r) = 1$ and $2DPQ_x(r) = M$.*

Proof For a circular sequence, shift operations do not change the pair of measures, only a single (p, q) value is possible.

Theorem 1 *For a sequence with stationary random properties, it has*
$1DP_x(0) \simeq \cdots \simeq 1DP_x(r) \simeq \cdots \simeq 1DP_x(m) \ll 1$,
$1DQ_x(0) \simeq \cdots \simeq 1DQ_x(r) \simeq \cdots \simeq 1DQ_x(m) \ll 1$, or
$2DPQ_x(0) \simeq \cdots \simeq 2DPQ_x(r) \simeq \cdots \simeq 2DPQ_x(m) \ll 1$.

Proof In any random condition, it is necessary for pairs of $\{(p, q)\}$ to have certain states significantly different from a circular sequence in either $\ll 1$ or $\ll M$ condition. Under the stationary random condition, all maximals satisfy only $\simeq$ relations under shift operations.

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.

Theorem 2 *For two $\{i, j\}$-th G maps G^i and G^j on $G_x^i \simeq G_x^j$ with variation ratios $G_x^{i,R}$ and $G_x^{j,R}$, if a variation ratio has a minimal value, then the relevant map has a better stationary random property than the maximal one.*

Proof Since $G_x^R = \Delta G_x / G_x$ and $G_x^i \simeq G_x^j$, it is a relative measure on $\forall r(max\{G_x(r)\} - min\{G_x(r)\})/G_x \ge 0$. So $min\{\Delta G_x^i, \Delta G_x^j\} \le max\{\Delta G_x^i, \Delta G_x^j\}$, the minimal variation ratio indicates the better stationary random property.

Corollary 5 *For different maps, it is better to compare various variation ratios relevant to the same type of distributions.*

Proof For various maps in the same type of distributions, relevant $\{G_x\}$ should satisfy the similar–equal condition.

4 Testing Results

Four pseudorandom sequences are generated by $\{$A5,RC4,DES, AES$\}$ ciphers, and two quantum cryptographic sequences are selected from both ANU and USTC resources.

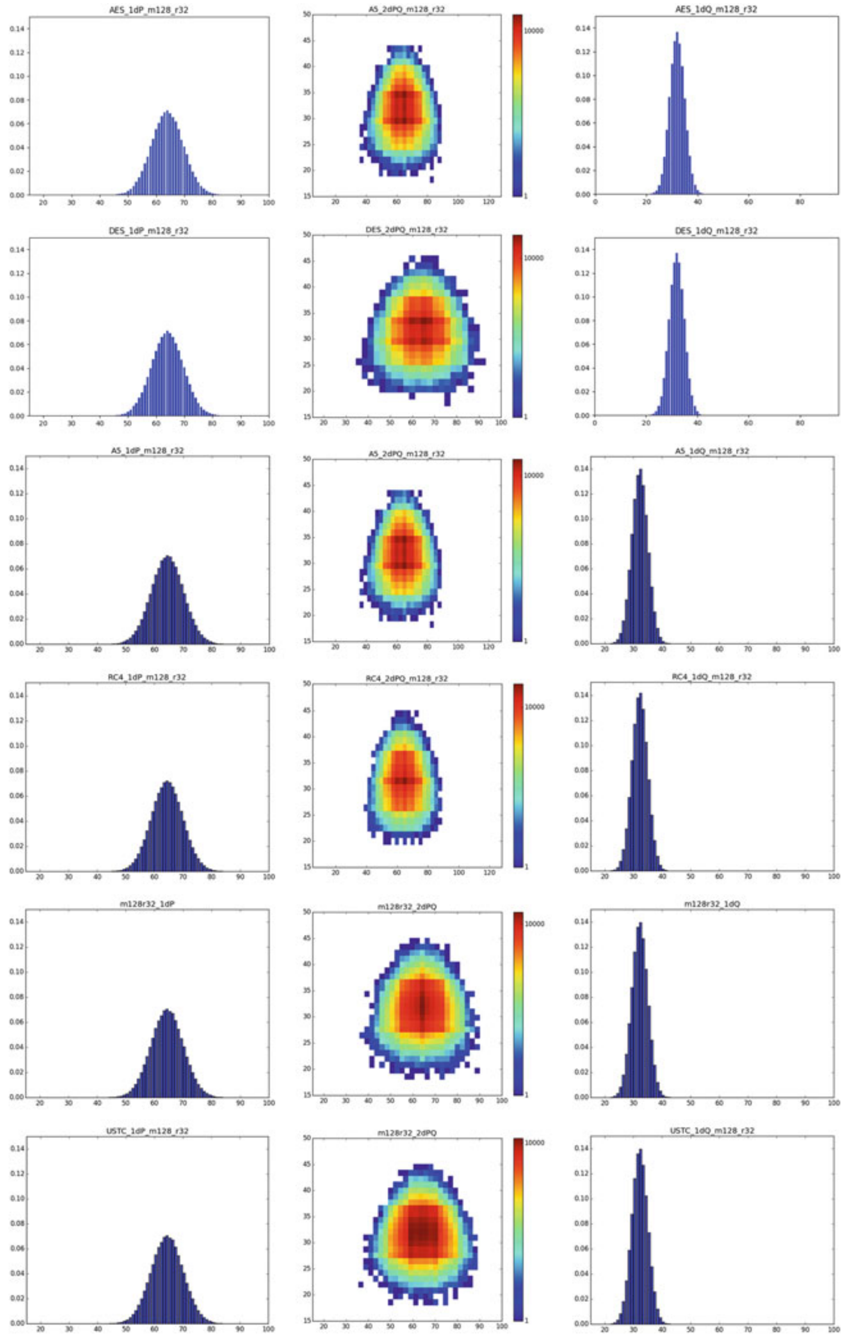


Fig. 4 Six cryptographic sequences on $r = 32$ 1DP, 2DPQ, and 1DQ maps

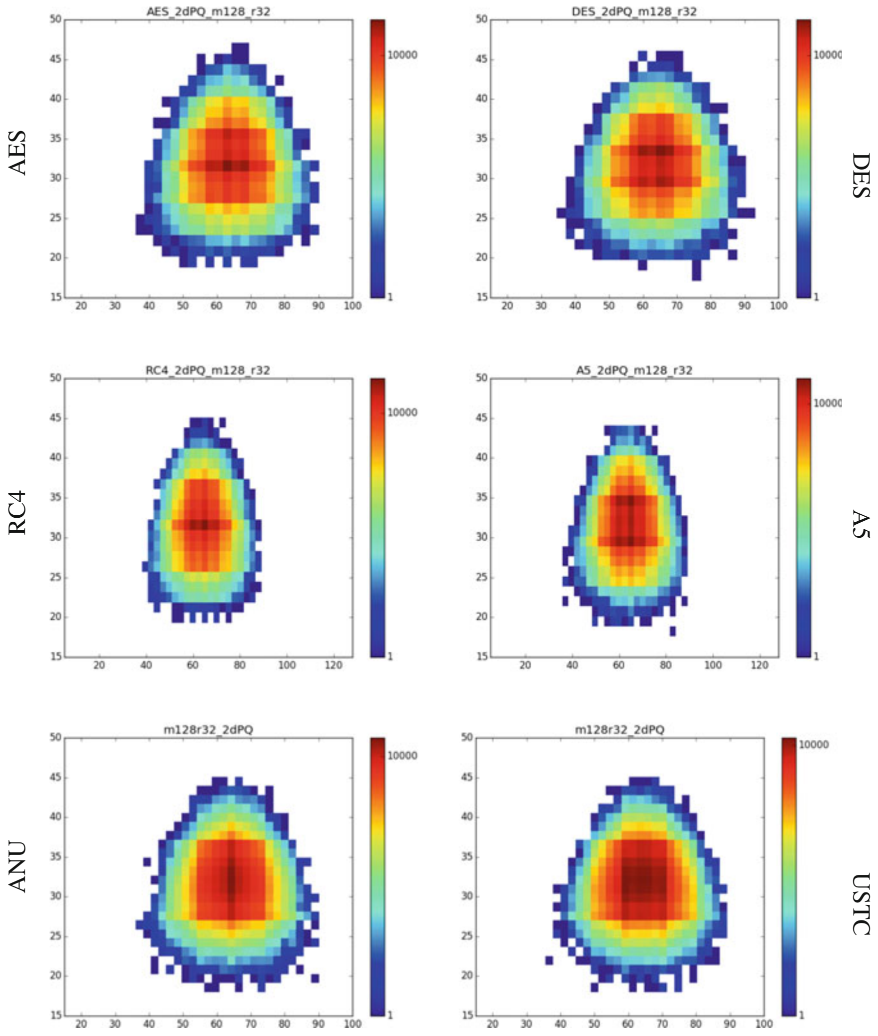


Fig. 5 Six cryptographic sequences on $r = 32$ 2DPQ maps

Typical results of testing stationary properties for six sequences on 18 maps of {1DP, 2DPQ, 1DQ} are shown in Fig. 4. Each position contains nine shift values of $r = 32$ selected. A total number of 18 maps are included. Six 2DPQ maps are shown in Fig. 5 as enlarged maps. Each map has shift values of $r = 32$, respectively.

Three variation measures $\{G_x, \Delta G_x, G_x^R\}$ for maps {1DP, 2DPQ, 1DQ } of six sequences are shown in Table 1, and their sorted orders are listed in Table 2. Twenty-four 2D maps of maximal curves for $r = 0 - 128$ are shown in Table 3. Three left columns contain 18 enlarged variation maps of {1DQ, 1DP, 2DPQ} and the last column contains six variation regions of 1DQ + 1DP + 2DPQ in six 2D maps. Six enlarged 2D maps are shown in Table 4 and six larger 2D maps are shown in Table 5.

In Table 6, 49 pairs of differences for variation ratios are listed in three 7 × 7 tables to illustrate refined quantity measures on three levels. There are seven entries on diagonals with seven trivial 0 values. For other 42 nontrivial values, let $dG_x^R\%$ denote differences of $G_x^R\%$ based on the basic variation ratios in Table 1, and various differences of variation ratios among six samples are listed. Differences of three variation ratios $\{dQ_x^R\%, dP_x^R\%, dPQ_x^R\%, \}$ on seven items {∅, AES, DES, A5, RC4, ANU, USTC} are illustrated.

5 Result Analysis

Eighteen maps in Fig. 4 are composed of three groups. Six 1DP maps have similar distributions in bell shapes to illustrate Poissonian distributions. Six 2DPQ maps are

Table 1 Comparisons on three variation measures for six samples

1DQ:	$Q_x\%$	$\Delta Q_x\%$	$Q_x^R\%$
AES:	14.05	0.42	3.0
DES:	14.05	0.36	2.55
A5:	13.953	0.19725	1.4136
RC4:	14.210	0.21985	1.5471
ANU:	13.961	0.17761	1.2722
USTC:	13.944	0.19664	1.4102
1DP:	$P_x\%$	$\Delta P_x\%$	$P_x^R\%$
AES:	7.07	0.42	3.96
DES:	7.05	0.25	3.5
A5:	7.02650	0.17665	2.51409
RC4:	7.19459	0.16223	2.25498
ANU:	7.0352	0.15472	2.1992
USTC:	7.0289	0.13542	1.9265
2DPQ:	$PQ_x\%$	$\Delta PQ_x\%$	$PQ_x^R\%$
AES:	1.0	0.09	9.02
DES:	1.0	0.08	8.21
A5:	0.98690	0.05508	5.5818
RC4:	1.02754	0.05106	4.96913
ANU:	0.99245	0.04791	4.8276
USTC:	0.98675	0.04691	4.7544

Table 2 Possible sorted orders of three types of variation measures; (a) $G_x\%$, (b) $\Delta G_x\%$, (c) $G_x^R\%$

$G_x\%$	min	max	min - max sorted	min-max range
1DQ:	USTC	RC4	USTC-A5-ANU-AES-DES-RC4	$13.944 \leq Q_x\% \leq 14.21$
1DP:	A5	RC4	A5-USTC-ANU-DES-AES-RC4	$7.0289 \leq P_x\% \leq 7.19459$
2DPQ:	USTC	RC4	USTC-A5-ANU-DES-AES-RC4	$0.98675 \leq PQ_x\% \leq 1.02754$

(a)

$\Delta G_x\%$	min	max	min - max sorted	min-max range
1DQ:	ANU	AES	ANU-USTC-A5-RC4-DES-AES	$0.17761 \leq \Delta Q_x\% \leq 0.42$
1DP:	USTC	AES	USTC-ANU-RC4-A5-DES-AES	$0.13542 \leq \Delta P_x\% \leq 0.42$
2DPQ:	USTC	AES	USTC-ANU-RC4-A5-DES-AES	$0.04691 \leq \Delta PQ_x\% \leq 0.09$

(b)

$G_x^R\%$	min	max	min - max sorted	min-max range
1DQ:	ANU	AES	ANU-USTC-A5-RC4-DES-AES	$1.2722 \leq Q_x^R\% \leq 3.0$
1DP:	USTC	AES	USTC-ANU-RC4-A5-DES-AES	$1.9265 \leq P_x^R\% \leq 3.96$
2DPQ:	USTC	AES	USTC-ANU-RC4-A5-DES-AES	$4.7544 \leq PQ_x^R\% \leq 9.02$

(c)

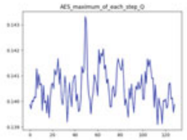
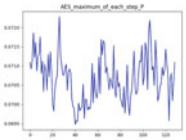
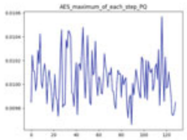
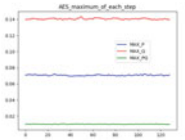
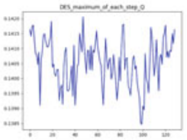
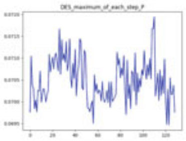
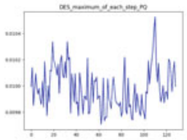
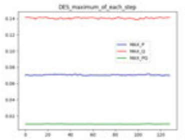
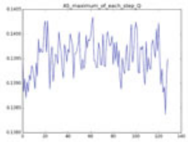
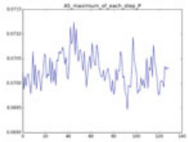
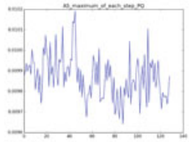
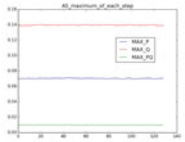
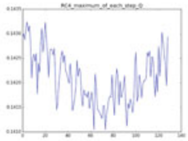
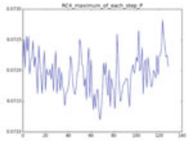
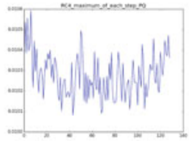
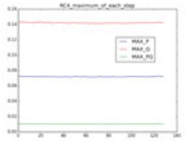
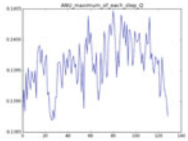
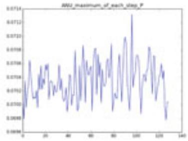
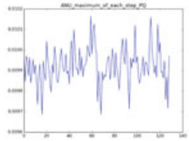
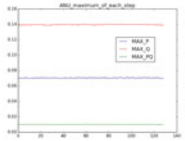
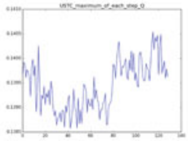
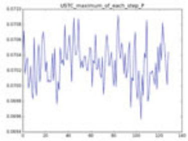
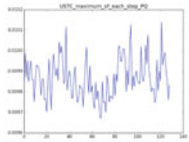
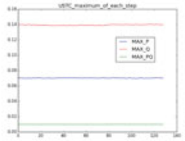
2D distributions. They have a symmetry on left/right directions and have a broken symmetry on up/down directions. Pseudo-color pixels on six maps indicate relevant 3D shapes. Compared with six 1DP maps, six 1DQ maps have similar distributions and more narrow bell shapes to illustrate sub-Poissonian distributions. It is possible to illustrate different maps on shift $r = 32$ for each map.

In Table 1, three pairs of maximal and minimal variation ratios are identified and three full orders are sorted in Table 2. Compared with G_x sorted orders, both $\{\Delta G_x, G_x^R\}$ variation ratios, six samples keep the same sorted orders as two groups: 1DQ and {1DP, 2DPQ} for their min-max variation ratios. Six enlarged 2DPQ maps on shift $r = 32$ are shown in Fig. 5 to form three pairs {AES:DES, RC4:A5, ANU:USTC}. Three pairs of six maps have similar visual distributions.

Twenty-four variation maps are shown in Table 3 as four groups. Each group contains six 2D maps. For three groups of {1DQ, 1DP, 2DPQ}variation distributions, eighteen enlarged 2D maps are shown in significant waveforms. For the group of 1DQ + 1DP + 2DPQ distributions, six maps are shown in three average variations satisfying $1DQ_x > 1DP_x > 2DPQ_x$, respectively. The fourth group of variation measures combines three variations of 1DQ + 1DP + 2DPQ in one unified 2D maps. From the six 2D maps, their stationary randomness of global variations are clearly illustrated.

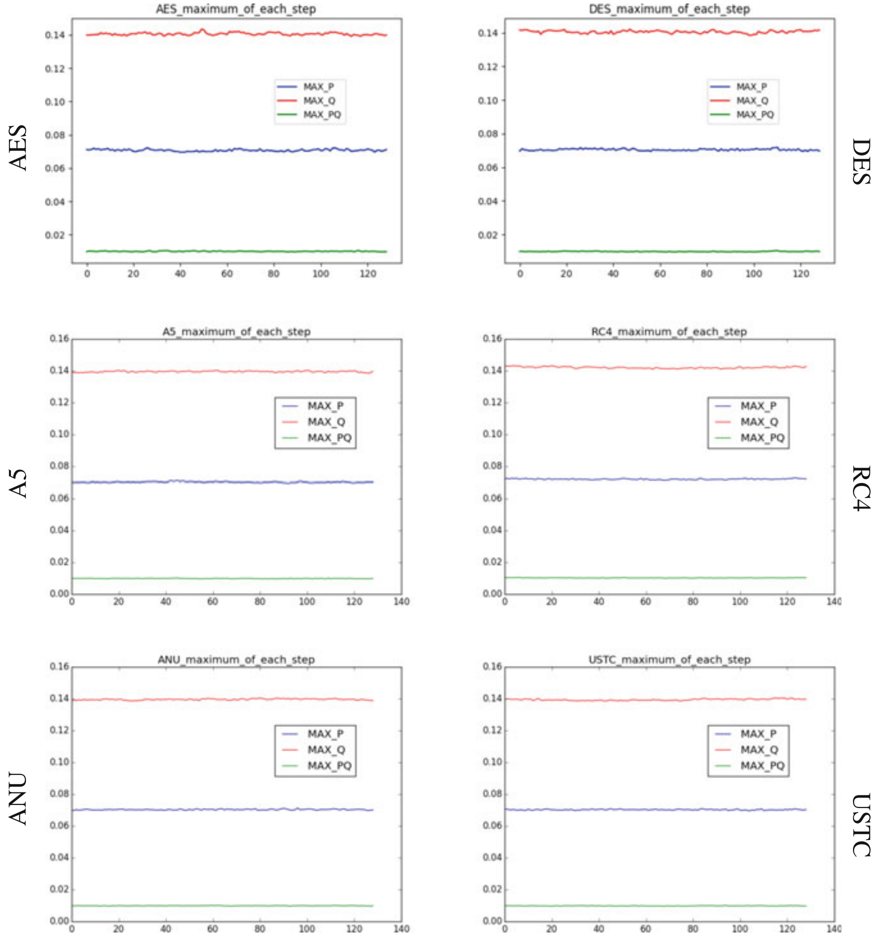
In Table 4, AES and DES map may have high frequent waves, and other enlarged 2D maps have stationary properties. In Table 5, larger waves appear and more details could be identified. Although significant variations are appeared in different 2D maps, it is difficult to make classification depending on their variation behaviors.

Table 3 Variation distributions of six samples

	1DQ	1DP	2DPQ	1DQ+1DP+2DPQ
AES				
DES				
A5				
RC4				
ANU				
USTC				

In Table 6, three variation ratios of differences are bounded in $0.0034 \leq |dQ_x^R\%| \leq 1.73$, $0.056 \leq |dP_x^R\%| \leq 3.96$, and $0.073 \leq |dPQ_x^R\%| \leq 4.27$, respectively. In general, three groups of variation ranges on differences meet $\{dQ_x^R\%\} \subset \{dP_x^R\%\} \subset \{dPQ_x^R\%\}$. From a stationary testing viewpoint, 2DPQ shows the strongest distinct property, 1DQ has the weakest numeric property, and 1DP provides the middle identifying property.

Table 4 Six variations on 2D maps



Since three groups can be identified by {AES, DES} block ciphers, {A5, RC4} stream ciphers, and {ANU, USTC} quantum ciphers, stationary randomness quantities can be classified as three {AES, DES}-highest, {A5, RC4}-middle, and {ANU, USTC}-lowest categories to provide distinct variation measures in the testing. Three quantity categories may correspond to distinguish artificial, semi-artificial, and natural designs for various generating mechanisms of cryptographic resources.

Considering all differences of variation ratios on six samples listed in Table 6, there are only 0.0034–4.27% differences (thirty-four in one million to four percent) are recognized. From a measuring viewpoint, all six samples are showing distinct stationary randomness properties.

Table 5 Larger six variations on 2D maps

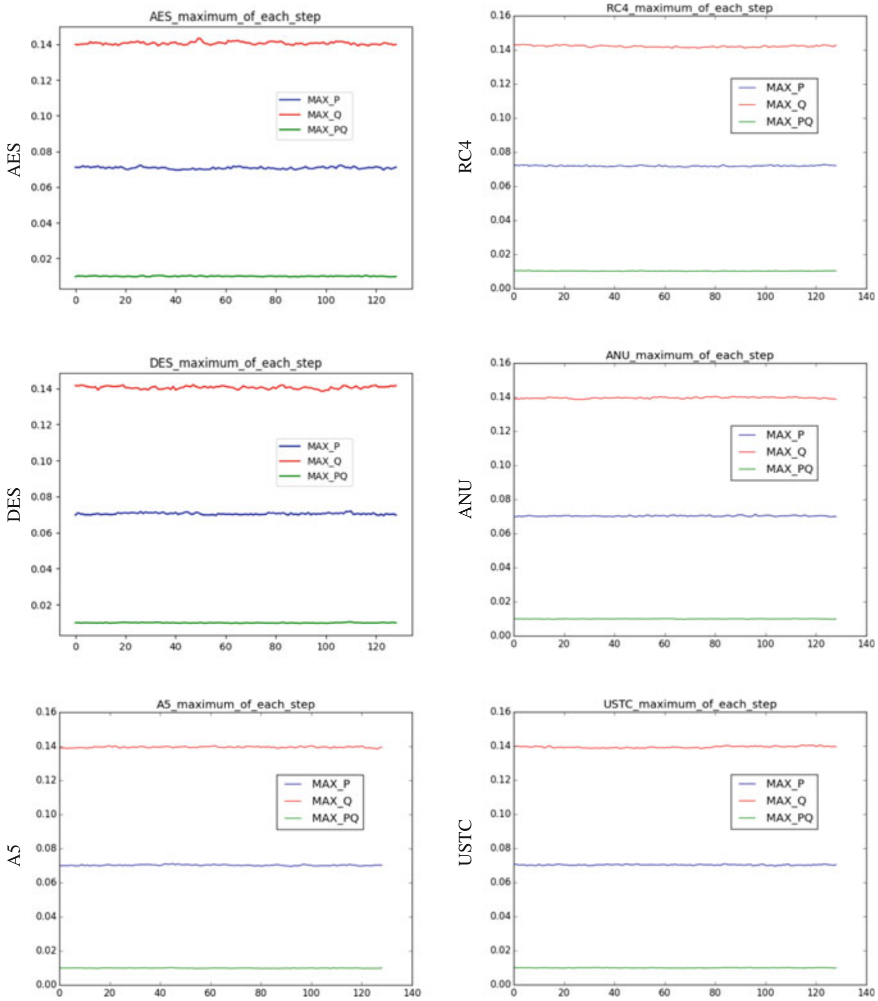


Table 6 Differences of variation ratios among three maximals of six samples

$dQ_x^R\%$	∅	AES	DES	A5	RC4	ANU	USTC
∅	0	-3.0	-2.55	-1.4136	-1.5471	-1.2722	-1.4102
AES	3.0	0	0.45	1.5864	1.4529	1.7278	1.5808
DES	2.55	-0.45	0	1.1364	1.0029	1.2778	1.1398
A5	1.4136	-1.5864	-1.1364	0	-0.1335	0.1414	-0.0034
RC4	1.5471	-1.4529	-1.0029	0.1335	0	0.2749	0.1369
ANU:	1.2722	-1.7278	-2.2778	-0.1414	-0.2749	0	-0.138
USTC:	1.4102	-1.5898	-1.1398	-0.0034	-0.1369	0.138	0

$dP_x^R\%$	∅	AES	LFSR	A5	RC4	ANU	USTC
∅	0	-3.96	-3.5	-2.51409	-2.25498	-2.1992	-1.9265
AES	3.96	0	0.46	1.44591	-0.54996	1.7608	2.0335
DES	3.5	-0.46	0	0.98591	1.24502	1.3008	1.5735
A5	2.51409	-1.44591	-0.98591	0	0.25911	0.31489	0.58759
RC4	2.25498	0.54996	-1.24502	-0.25911	0	0.05578	0.32848
ANU:	2.1992	-1.7608	-1.3008	-0.31498	-0.05578	0	0.2727
USTC:	1.9265	-2.0335	-1.5735	-0.58759	-0.32848	-0.2727	0

$dPQ_x^R\%$	∅	AES	DES	A5	RC4	ANU	USTC
∅	0	-9.02	-8.21	-5.5818	-4.96913	-4.8276	-4.7544
AES	9.02	0	0.81	3.4382	4.05087	4.1924	4.2656
DES	8.21	-0.81	0	2.6282	3.24087	3.3824	3.4556
A5	5.5818	-3.4382	-2.6282	0	0.61267	0.7542	0.8274
RC4	4.96913	-4.05087	-3.24087	-0.61267	0	0.14153	0.21473
ANU:	4.8276	-4.1924	-3.3824	-0.7542	-0.14153	0	0.0732
USTC:	4.7544	-4.2656	-3.4556	-0.8274	-0.21473	-0.0732	0

6 Conclusion

It is feasible to evaluate stationary properties for a random sequence using the testing system. Using three maps {1DP, 1DQ, 2DPQ}, a series of variation measures and their ratios are illustrated. Extracting maximal measures is identified for shift $r : 0 - m$. For each sample, three 2D maps of variation curves provide refined characteristics to evaluate stationary randomness properties in global. Sample variation maps are shown in exactly similar–equal relationships among the same group of average variations. Further explorations and applications are required to check the testing system on other applications of cryptographic streams. Three quantity categories of artificial, semi-artificial, and natural designs may be explored to get intrinsic stationary randomness information from refined testing and future explorations.

Acknowledgements Thanks to 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 Random Numbers Server for quantum cryptographic sequences.

References

1. Cyberspace: https://en.wikipedia.org/wiki/Cyberspace
2. Communications Security:https://en.wikipedia.org/wiki/Communications_security
3. Quantum satellite: https://qz.com/760804
4. Quantum key distribution:https://en.wikipedia.org/wiki/Quantum_key_distribution
5. Random number generation:https://en.wikipedia.org/wiki/Random_number_generation
6. S. Golomb, *Shift-Register Sequences*, Revised edn. (Aegean Park Press, Laguna Hills, California, 1982)
7. E. Barkam, E. Biham, N. Keller, Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication. Journal of Cryptology **21**(3), 392429 (2008)
8. Y. Lu; W. Meier; S. Vaudenay. The Conditional Correlation Attack: A Practical Attack on Bluetooth Encryption. *Crypto 2005*. 3621: 97117 (2005)
9. eSream:https://en.wikipedia.org/wiki/ESTREAM
10. P. Junod & A. Canteaut (2011). *Advanced Linear Cryptanalysis of Block and Stream Ciphers*. IOS Press. p. 2. ISBN 9781607508441
11. ZUC. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 and 128-EIA3: Document 2: ZUC Specification
12. A. Poorghanad, A. Sadr, A. Kashanipour, generating high quality pseudo random number using evolutionary methods. IEEE Congress on Comput. Intell. Security **9**, 331–335 (2008)
13. A. de Queiroz, J. Schechtman, Elimination of nonlinear clock feedthrough in component-simulation switched-current circuits in *Circuits and Systems, 1998. ISCAS '98. Proceedings of the 1998 IEEE International Symposium on*, pp. II378–II381 (1998)
14. A. Fuster-Sabater and F.Vitini. Classes of Nonlinear Filters for Stream Ciphers, Chapter *Geometry, Algebra and Applications: From Mechanics to Cryptography*,
15. S. Ronjom, C. Cid, Nonlinear Equivalence of Stream Ciphers. in *Proceeding of Fast Software Encryption, 17th International Workshop*, FSE 2010, Seoul, Korea, Lecture Notes in Computer Science, vol. 6147, Springer, pp. 40–54 (2010)
16. J. Nechvatal, E. Barker, L. Bassham, et al., Report on the development of the advanced encryption standard (AES), in *National Institute of Standards and Technology (NIST)* (2000). http://csrc.nist.gov/archive/aes/round2/r2report.pdf
17. G. Paul, S. Maitra. *RC4 Stream cipher and Its Variants*. (CRC Press, 2012)
18. S.D. Cardell, A. Fuster-Sabater, Linear models for the self-shrinking generator based on CA. Journal of Cellular Automata **11**(23), 195211 (2016)
19. N. Nagaraj, One-time pad as a nonlinear dynamical system. Commun. Nonlinear Sci. Numer. Simul. **17**, 4029–4036 (2012)
20. E. Dubrova, M. Teslenko and H. Tenhunen. On analysis and synthesis of (n,k)-non-linear feedback shift registers, *Proceedings of the conference on Design, automation and test in Europe*, 1286-1291, 2008

21. E. Dubrova, A List of Maximum Period NLFSRs. Cryptology ePrint Archive, Report 2012/166, 2012
22. Y. Zhao, Y. Hu, S. Li, A new analysis method for nonlinear component of stream ciphers. J. Inf. Comput. Sci **10**(16), 5313–5321 (2013)
23. Meschede, D. *Optics, Light and Lasers*, 2 ed. (Wiley-VCH, 2007)
24. R. Boyd. *Nonlinear Optics* (3rd ed.). Academic Press (2008)
25. M. Nakazawa et al., QAM quantum stream cipher using digital coherent optical transmission. Opt. Express **22**(4), 4098–4107 (2014)
26. M. Yoshida et al., Single-channel 40 Gbit/s digital coherent QAM quantum noise stream cipher transmission over 480 km. Opt. Express **24**(1), 652–661 (2016)
27. J. Barry, E. Lee, *David G* (Messerschmitt. Digital Communications, Sprinter, 2004)
28. S. Lian et al., A chaotic stream cipher and the usage in video protection. Chaos Solitons and Fractals **34**(3), 851–859 (2007)
29. D. E. Knuth, *The Art of Computer Programming*, vol. 2: *Seminumberical Algorithms* (Addison-Wesley, 1969)
30. D. Makovoz, Noise variance estimation in signal processing, in *International Symposium on Signal Processing and Information Technology*, pp. 364–369 (2006)
31. Ito, Kazufumi. Gaussian filter for nonlinear filtering problems. *Conference on decision and control* (2000): 1218-1223
32. 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)
33. M. Fox, *Quantum Optics: An Introduction* (Oxford University Press, New York, 2006)
34. M.B. Priestley. *Non-linear and Non-stationary Time Series Analysis* (Academic Press, 1988))
35. A. Kolmogorov, https://en.wikipedia.org/wiki/Andrey_Kolmogorov
36. A.N. Kolmogorov (1903–1987). *Royal Netherlands Academy of Arts and Sciences*. Retrieved 22 July 2015
37. D.C. Champeney, *Power spectra and Wiener's theorems* (Cambridge University Press, A Handbook of Fourier Theorems, 1987)
38. N. Wiener, Generalized harmonic analysis. Acta Math. **55**, 117258 (1930). https://doi.org/10.1007/bf02546511
39. N. Wiener, *Time Series Press* (M.I.T Press, Cambridge, 1964)
40. Stationary process: https://en.wikipedia.org/wiki/Stationary_process
41. Stationary: https://www.otexts.org/fpp/8/1
42. A5/1 stream cipher:https://en.wikipedia.org/wiki/A5/1
43. R. Rivest, J. Schuldt, Spritz a spongy RC4-like stream cipher and hash function. Retrieved 26 October 2014
44. A.E. Ivanova et al., Using optical splitters in quantum random number generators based on fluctuations of vacuum. J. Phys.: Conf. Ser. **735**, 012077 (2016)
45. X.T. Song et al., Phase-Coding Self-Testing Quantum Random Number Generator. Chin. Phys. Lett. **32**(8), 080302–080310 (2015)
46. 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)
47. W. Chen et al., Active phase compensation of quantum key distribution system. Chinese Science Bulletin **53**(9), 1310–1314 (2008)
48. M. Sasaki et al., Field test of quantum key distribution in the Tokyo QKD network. Opt. Express **19**(11), 10387–10409 (2011)
49. Quantum random number generator of ANU: http://photonics.anu.edu.au/qoptics/Research/qrng.php
50. Z.J. Zheng. *Conjugate transformation of regular plan lattices for binary images*, Ph.D. Thesis, Monash University (1994)
51. Z.J. Zheng, C.H.C. Leung, Visualising global behaviour of 1D cellular automata image sequences in 2D Map. Phys. A **3–4**, 785–800 (1996)
52. D.E. Knuth. *The Art of Computer Programming*, vol. 4A: *Combinatorial Algorithms Part 1* (Addison-Wesley, 2011)

53. J. Zheng, C. Zheng, A framework to express variant and invariant functional spaces for binary logic. Frontiers of Electr. Electron. Eng. China, **5**(2), 163–172. Higher Educational Press and Springer-Verlag (2010). 10.1007/s11460-010-0011-4 http://link.springer.com/article/10.10072Fs11460-010-0011-4
54. H. Wang, J. Zheng, 3D Visual Method of Variant Logic Construction for Random Sequence. Aust. Inf. Warfare Security 16–27 (2013)
55. W.Z. Yang, J. Zheng, Variant pseudo-random number generator, Hakin9 Extra. Timing Attack **06**(13), 28–31 (2012)
56. 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
57. J. Zheng, C. Zheng, Variant simulation system using quaternion structure. J. Modern Opt. **59**(5), 484–492 (2012) Taylor & Francis Press
58. J. Zheng, C. Zheng, T.L. Kunii, Interactive maps on variant phase space, in *Emerging Application of Cellular Automata*, pp. 113–196 (InTech Press, 2013)
59. J. Zheng, W. Zhang, J. Luo, W. Zhou, R. Shen, Variant map system to simulate complex properties of DNA interactions using binary sequences. Adv. Pure Mathe. **3**(7A), 5–24 (2013)
60. D.M. Heim, O. Heim, P.A. Zeng, J. Zheng, Successful creation of regular patterns in variant maps from bat echolocation calls. Biological Systems: Open Access **5**, 2 (2016). https://doi.org/10.4172/2329-6577.1000166
61. Daemen, Joan; Rijmen, Vincent (March 9, 2003). *AES Proposal: Rijndael*. National Institute of Standards and Technology. p. 1. Retrieved 21 February 2013
62. LFSR scheme:https://en.wikipedia.org/wiki/Linear-feedback_shift_register
63. NIST. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* (NIST, Special Publication, 2010)
64. M. Soltanalian, P. Stoica, Computational design of sequences with good correlation properties. IEEE Trans. Signal Process. **60**(5), 2180–2193 (2012)