Journal of Computers Vol. 32 No. 3, 2021, pp. 119-134
doi:10.3966/199115992021063203009

Analysis of Quantum Key Randomness Based on Cold Region Practical QKD System

Jia-Nan Wu[1,2], Ying Zhang[1,2], Jian Zhao[1], De-Xin Zhu[1,2], Li-Jun Song[2,3*]

[1] Department of Computer Science and Technology, Changchun University, Changchun 130022, China

[2] Jilin quantum information technology Engineering Laboratory, Changchun 130000, China

[3] Jilin Normal University of Engineering Technology, Changchun 130000, China
ccdxslj@126.com

Received 9 September 2020; Revised 14 September 2020; Accepted 15 September 2020

Abstract. Quantum key distribution (QKD) systems have extremely strict requirements for random numbers. Random selection of basis vector is required when modulating the quantum state. The quality of randomness directly determines the security of final keys. The randomness of pseudorandom numbers based on mathematical algorithms depends on input seeds. As pseudorandom numbers may be cracked when used frequently, they cannot meet requirements of QKD protocols for random numbers. The output of the quantum random number generator is basis on the quantum mechanics intrinsic randomness, and is generally considered to have true randomness. In order to verify the randomness of quantum key generated by the cold region practical QKD system, BB84 protocol-based without post-processing, polarization-coded post-processing, phase-coded post-processing QKD systems were constructed, which generated three types of quantum keys as data sources to be analyzed. Meanwhile, pseudorandom keys generated by chaos algorithms and physical random keys generated by atmospheric noises were introduced for comparison. The experiment adopted national institute of standards and technology (NIST) to implement routine verification on stochastic performances of five keys. Additionally, we proposed a novel visualized randomness verification method based on statistical feature parameters. The results indicated that the quantum key generated by QKD systems with post-processing had superior stochastic performance.

Keywords: QKD, randomness, NIST, P-value, information entropy, correlation of adjacent pixels

1 Introduction

Random number, as a concept often mentioned in scientific research and daily life, is a basic resource in fields such as probability theory and quantum mechanics [1]. It plays an important role in cryptography, scientific simulation, gambling industry and basic science [2-3]. The current mainstream applications of random numbers are mostly based on pseudo random number generators which have many construction methods, including block cipher, stream cipher, chaos, number theory and other methods [4-9]. These methods are usually based on preset mathematical algorithms, using the available external information such as the system time as seeds. Computes use limited operating steps to generate subsequent random sequences by combining the previous random sequences with the seed information. This kind of method can meet the application requirements in terms of statistical sampling, etc [10]. Nevertheless, ingenious algorithm design can't get rid of the deterministic nature of generating pseudo random numbers.

With the recent rise of the Internet of things, cybersecurity has become a hot topic [11]. It is an urgent problem to encrypt important information by using secure key. The continuous development of quantum computing is seriously threatening the traditional encryption system. Although random sequences

* Corresponding Author

generated by physical random number generator (PRNG) based on atmospheric noise [12], electronic noise [13] and radiation decay [14] show good randomness, the output rate of random sequences is lower due to the physical bandwidth limitation or difficult use of the random source [15]. The quantum random number generator (QRNG) based on quantum physics generates random sequences fast, has high stochastic performance, and its intrinsic randomness can be guaranteed by the basic principles of quantum mechanics. In the past ten years, research institutions in the world have constructed different generation schemes of quantum true random numbers that typically include measuring photon path [16], photon arrival time [17-18], photon number distribution [19], phase noise [20], amplified spontaneous emission noise [21], and vacuum noise fluctuations [22].The scheme based on quantum random source is also called true random number generator (TRNG). However, the imperfection of the device and the intrinsic characteristics of the quantum random source will lead to the bias of the original output data, so the original data must be extracted by the corresponding post-processing program to get the quantum random number that meets the requirements [23].

Quantum Key Distribution (QKD) is the first quantum communication technology from laboratory to practical application, which is use the non-clonability of non-orthogonal single quantum state to complete the secured key distribution. Indeed, QKD systems are highly dependent on random numbers. In the QKD system, the security profile lies in the randomly sent quantum state, and the security of the randomly sent quantum state is guaranteed by the random number used. In other words, QKD systems need to generate numerous high-quality random sequences through TRNG to complete secure communication [11]. C. Z. Peng et al. provided the first decoy signal implementation scheme based on polarization state, completed one-way quantum communication of 75 km (single-phonon detector) and 102 km (dual-phonon detector), and obtained unconditionally secure final keys, and then combined a new data post-processing method with a decoy signal scheme, and obtained an unconditionally secure quantum key [24] with a communication distance increased from 142 km to 182 km. In 2015, Team of China University of science and technology proposed a quantum random number generation method based on measuring phase noise that can reach a generation rate of 68 Gbit/s [25]. In 2018, Pan et al. achieved a device-independent system and successfully obtained quantum keys [26]. In 2020, Xiongfeng Ma's group and the University of science and technology of China worked together for the first time to realize the experiment of quantum key distribution of non relay optical fiber over 500 km, which achieved the record of channel loss tolerance and created a new world record [27]. These research results have strongly promoted the development of quantum secret communication, and the standardization and application of QKD.

At present, there is no strict definition of whether a series of random sequences are truly random. It is generally considered that the random number sequences with redictability, eproducibility and iasedness are true random number sequences. Randomness is quantified by Min entropy, a special category of Renyi entropy [28]. At present, the most commonly used random test methods in the world are several standard test packages based on the statistical characteristics of test sequences, as well as other supplementary tests on statistical distribution, autocorrelation function and other test indicators. At present, the most commonly used random test methods in the world are several standard test packages NIST [29], DieHard and DieHarder [30-31], TESTU01f1 [32] based on the statistical characteristics of test sequences, and other supplementary tests on statistical distribution [33], autocorrelation function [34] and other test indicators. However, it should be noted that a sequence of random numbers can't be judged to be truly random even if it passes a series of tests of statistical indicators. In order to verify the randomness of quantum keys generated by practical QKD systems on the statistical index, point-to-point QKD systems based on BB84 protocol was constructed to obtain the quantum key without post-processing, and a polarization-coded QKD system with three nodes and a phase-coded 32 km remote QKD system were constructed to obtain post-processed quantum keys, and simultaneously pseudorandom keys generated by chaos algorithms and physical random keys generated by atmospheric noise were introduced for comparative analysis. The basic principles of generating random sequences by different mechanisms were explained, and detection results of randomness based on NIST packets were presented. Meanwhile, a novel visualized randomness verification method based on statistical feature parameters, including information entropy and correlation of adjacent pixels, is proposed.

2 Theoretical Model Analysis of Random Numbers Source

2.1 Point-to-point QKD System Based on BB84 Protocol

In BB84 protocol, four pulse lasers are randomly emitted by the transmitting end Alice, correspondingly prepared as four polarization states (denoted as H, V, +, -), and sent to the receiving end Bob via the quantum beam splitter (QBS). Bob randomly selected a measurement basis for measurement. In the theory of quantum optics [35], when the average number of photons emitted by the transmitting end is μ, the weakly coherent pulse can be expressed as:

$$\rho_A = \sum_{n=0}^{\infty} \frac{\mu^n}{n!} e^{-\mu} |n><n|. \tag{1}$$

For QKD systems based on the BB84 protocol, the security bit rate can be expressed as:

$$r = 1 - H_2(\delta) - H_2(\delta_P). \tag{2}$$

where $H_2(\delta)$ is the amount of leaked information due to error correction, and $H_2(\delta_P)$ is the number of keys consumed by correcting errors in the ideal process.

On the receiving end, the loss of the optical system, detection efficiency, and count rate loss caused by the dead time of the detector are collectively attributed to Bob's detection efficiency, which is denoted as η_D:

$$\eta_D = \eta_{Bob} \times \eta_{QE} \times \eta_{DeadTime}. \tag{3}$$

where η_{Bob} is the transmission efficiency of Bob's optical system, η_{QE} is the detection efficiency, $\eta_{DeadTime}$ is the counting rate caused by the dead time of the detector, and photons generate random sequences through path selection. Single phonon must pass a 50:50 QBS to be received by a single-photon detector (SPD) after reaching the receiving end. Only the photons that can be detected can generate the original random data. When all single phonons pass QBS, there is a 1/2 probability for both paths that they can be selected. The quantum states detected by the detector after passing two paths are recorded as $|0>$ and $|1>$, respectively. Generally, the Error Rate of system is mainly caused by the imperfect optics and the dark count as well as noise of the system. QBER can be recorded as:

$$E_\mu Q_\mu = \sum_{i=0}^{\infty} e_i \frac{\mu^i}{i!} e^{-\mu} = e_0 + Y_0 + e_{opt}(1 - e^{-\eta\mu}). \tag{4}$$

Finally, Alice and Bob perform a base comparison on the open channel, only retaining the parts with the same base selection, which can be used as keys without post-processing, that is, the original random data generated based on the BB84 protocol.

2.2 Polarization-coded QKD Systems

For the polarization-coded decoy state QKD system [11], based on the BB84 protocol, Alice needs to prepare four polarization states (0 °, 45 °, 90 ° and 135 °) randomly. Herein, 0 ° and 90 ° polarization states correspond to the two basis vectors of Z base, while 45 ° and 135 ° polarization states correspond to the two basis vectors of X base. A strongly attenuated pulse laser was taken as the light source, and the average number of photons in the pulse is μ = 0.1. Additionally, Fresnel Multiple Prism (FMP) and Avalanched Photodiode-based Detector (APD) were used as a polarized splitter and the detection device [36], respectively. The photon state of a strongly attenuated pulse can be recorded as [1]:

$$|\varphi> = \cos\theta |H> + \sin\theta |V>. \tag{5}$$

where $|H>$ and $|V>$ are horizontal and vertical polarization states, respectively. After passing through the prism, the original photon state randomly collapses to the left-hand or right-hand polarization state. If

the photon state in the above formula is descripted by the left-hand and right-hand circular polarization state $|L>,$ and $|R>$, it can be expressed as:

$$|\varphi>=1/\sqrt{2}(\cos\theta-i\sin\theta)|R>+1/\sqrt{2}(\cos\theta+i\sin\theta)|L>. \quad \textbf{(6)}$$

Additionally, circular polarization state can be expressed by linear polarization state:

$$|R>=1/\sqrt{2}(|H>+i|V>). \quad \textbf{(7)}$$

$$|L>=1/\sqrt{2}(|H>+i|V>). \quad \textbf{(8)}$$

Regardless of the value of θ in the above formula, the probability of the two circular polarization states is always the same. In other words, after passing through the Fresnel prism, the QBS with a strong probability of 50:50 achieves the purpose of perfect balanced beam splitting. In contrast, the Bob end obtains random numbers sequences generated at a high rate.

In polarization-coded QKD systems, four lasers generate four polarization states through polarizers, respectively. Herein, lasers generate attenuated coherent states, four polarization states are transmitted to the receiving end Bob after splitter combining, and Bob uses wave plates, polarized splitter and four detectors for detection. The measurement base used by Bob is passively selected by using splitter. The two communication parties generate sequences after exchanging necessary information on the open channel according to the coding rules agreed by the protocol. Finally, the corresponding post-processing is performed to obtain the quantum key.

2.3 Phase-coded QKD Systems

Unlike polarization-coded ones, photon signals in phase-coded QKD systems are easier to maintain their phase information when transmitted in fiber. Hence, phase-coded decoy state QKD systems are usually employed in practical communications. According to the Weisskopf-Wigner (W-W) theory [37], considering the interaction of light and atoms and the laser structure, the phase noise of spontaneous radiation based on quantum mechanics is extracted. The variance of phase noise is proportional to the delay time. The quantum state of the entire system in spontaneous radiation can be recorded as [1]:

$$|\phi(t)>=a(t)e^{(-j\omega_0 t)}|e,0>+\Sigma_{k,s}b_{k,s}(t)e^{(-j\omega_0 t)}|g,1>. \quad \textbf{(9)}$$

where $a(t), b_{k,s}(t)$ represent the probability amplitudes of the upper and lower energy levels, respectively; $|0>,|1>$ are the vacuum state and the single-phonon state, respectively; $|e>,|g>$ are the excited state and the ground state, respectively; *k*, *s* are the wave vector and polarization, respectively. As can be seen from the above formula, when atoms spontaneously radiate from the excited state to the ground state, the emitted photons have different wave vectors and polarizations. Therefore, spontaneous radiation is the main source of phase noise [38].

W-W theory points out that the noise caused by spontaneous radiation is white noise and the phase change rate of spontaneous radiation can be regarded as having independent and identical distribution characteristics. Photons of spontaneous radiation perform Brownian motion in the cavity, and the conditional probability distribution of the phase difference caused by white noise relative to the initial moment follows the Gaussian distribution. Hence, the autocorrelation function can be obtained from the coherence time of phase noise [1]:

$$|E^*(t)E(t+\tau)>=<I(t)>e^{<[\Delta\phi(t)^2/2]>}=<I(t)>e^{<-|\tau|/\tau_{coh}>}. \quad \textbf{(10)}$$

where τ is the delay time, $\phi(t)$ represents white noise with uniform distribution at full angle $[0, 2\pi)$, and τ_{coh} is the coherence time of phase noise. When the autocorrelation function is smaller, the stochastic performance of random sequences is better.

The transmitting end Alice generates a series of coherent light pulses after continuous light is intensity modulated. After strong attenuation, each light pulse is performed random phase modulation of 0 or π. At the Bob end, a single-bit delay loop is used for delay. Therefore, the coherent light pulse sent by Alice can detect the phase information of Alice modulation through the interference between two adjacent

single phonons probability amplitude pulses after passing through the single-bit delay loop. After the necessary classical information comparison, keys are obtained according to decoy state BB84 protocol.

2.4 Chaos Model

The deterministic chaotic dynamical system in the dissipative system was first discovered by an America meteorologist Lorenz in 1963 [39]. In 1975, Li and York proposed the concept of chaos and gave the mathematical definition [40]. Sensitivity to the initial state is the characteristic of chaotic system. If there are two identical systems with different initial states, the difference between the two systems will increase rapidly with time [41]. Logistic chaotic map has simple expression and good random performance. It is a kind of dynamic system which is widely used in various fields of chaotic secure communication. Its mathematical expression is as follows:

$$x_{n+1} = \mu x_n (1 - x_n). \tag{11}$$

When $\mu \in (0, 4)$, the state $x_n \in (0, 1)$. When $\mu \in (3.5699456, 4]$, the input and output of the logistics map are all distributed on (0, 1), and the working state of the logistics map is in chaos.

Chaotic sequences generated by multiple iterations using logistic sine mapping. If only the iterative value of the logistics map is used as the random number, when the probability density of the iterative value is:

$$\rho(x) = \frac{1}{\pi\sqrt{x(1-x)}}. \tag{12}$$

And $\rho(x)$ is distributed between (0, 1). It has singularity at both ends of the interval. In order to generate uniformly distributed random number sequence in the distribution interval (0, 1), its distribution function is:

$$y(x) = \int_0^x \frac{dx}{\pi\sqrt{x(1-x)}} = \frac{2}{\pi}\sin h^{-1}\sqrt{x}. \tag{13}$$

Where $y(x)$ is a uniformly distributed random sequence on interval (0, 1). The sequence is very sensitive to the initial conditions and chaotic parameters, and has the characteristics of aperiodicity and pseudo randomness.

2.5 Atmospheric Noise

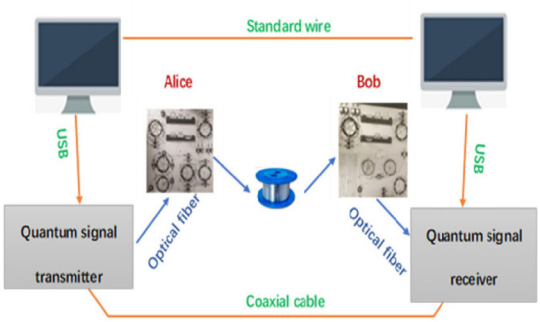
There are abundant random phenomena in nature, for example, we can make full use of the randomness of various noise signals to obtain true random numbers. At the beginning of 1997, it was first proposed by Antonio arauzo azofra, who wrote a random number generator for Solaris Operating System, and then developed it random.org Random number for users to download [11]. The random number is theoretically close to the atmospheric noise. The atmospheric noise is formed by the superposition of background Gaussian white noise and impulse noise, and the noise signal received by the receiver of VLF communication system is formed by the superposition of lightning discharge with global distribution. Although it is impossible to give the accurate mathematical expression of atmospheric noise with time domain and regional variation, the variation of noise signal field strength has statistical characteristics. The amplitude distribution characteristics can be obtained by measuring the noise statistical data at different times in different places, and it can be regarded as the sum of two independent random processes, which can be expressed as:

$$n(t) = w(t) + p(t). \tag{14}$$

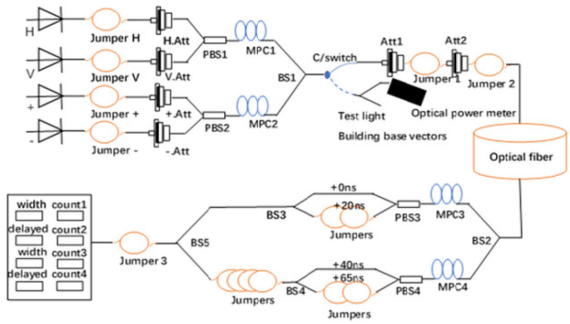
Where n(t) is the total atmospheric noise, w(t) is the background Gaussian white noise component in the atmospheric noise, and its mean value is 0. p(t) is a spike noise, which is the superposition of infinite narrow pulses generated by lightning near the receiver. The parameters of atmospheric noise at any time in any region of the world can be calculated by this formula, and the atmospheric noise produced approximately in this period in the laboratory can be calculated.

3 Data Preparation

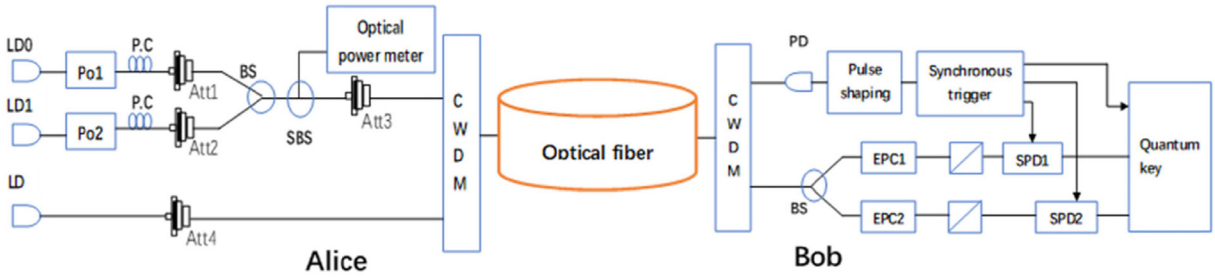
The point-to-point experiment platform device based on BB84 protocol is shown in Fig. 1(a). The transmitting end Alice randomly sends a series of single-phonon pulses (actually produced by weak laser source), the receiver Bob randomly selects the measurement basis to detect single phonon by SPD, and finally performs a basis vector comparison. Only the same part between the sender's preparation basis and the receiver's measurement basis is retained, which greatly limits the bit rate of keys. Therefore, post-processing needs to be introduced to increase the generating rate and bit rate of random sequences. Polarization-coded and phase-coded post-processing remote point-to-point QKD system devices are shown in Fig. 1(b) and Fig. 1(c), respectively.



(a) The point-to-point experiment platform device based on BB84 protocol



(b) Polarization-coded post-processing remote point-to-point QKD system



(c) Phase-coded post-processing remote point-to-point QKD system

Fig. 1. Cold region realistic QKD system

The following Table 1 shows the comparison results of different systems. The point-to-point experiment platform based on BB84 protocol consists of two PCs, quantum signal transmitter, quantum signal receiver, optical platform of transmitter, optical platform of receiver, 1km optical fiber, five optical fiber jumpers, standard network cable, USB cable, coaxial cable and power cable. Quantum random number generator is mainly composed of entropy source and algorithm post-processing. The entropy source is uncertain, and some analog or digital original random numbers need to be generated through uncertain physical phenomena. However, these original random numbers usually do not have good statistical characteristics, so it must be further processed through the algorithm post-processing to get a more satisfactory random number sequence. The QKD system based on phase coding is the first 32km practical remote point-to-point quantum secure communication network in Northeast China, which has been successfully implemented after debugging.

Table 1. Comparison of system characteristics for generating random sequences based on different methods

Produce / Characteristic	Quantum key sequence			Other key sequences	
	BB84	Polarization-coded	Phase-coded	Chaos	Atmospheric noise
Principle	Quantum physics	Quantum physics	Quantum physics	Deterministic algorithm	Atmospheric vibration
Distance	1km	5m	32km	No	No
Postprocessing	No	Yes	Yes	No	No
Periodicity	No	No	No	Yes	No
Certainty	No	No	No	Yes	No
Predictability	No	No	No	Yes	No
Repeatability	No	No	No	Yes	No

The following Table 1 shows the comparison results of different systems. The point-to-point experiment platform based on BB84 protocol consists of two PCs, quantum signal transmitter, quantum signal receiver, optical platform of transmitter, optical platform of receiver, 1km optical fiber, five optical fiber jumpers, standard network cable, USB cable, coaxial cable and power cable. Quantum random number generator is mainly composed of entropy source and algorithm post-processing. The entropy source is uncertain, and some analog or digital original random numbers need to be generated through uncertain physical phenomena. However, these original random numbers usually do not have good statistical characteristics, so it must be further processed through the algorithm post-processing to get a more satisfactory random number sequence. The QKD system based on phase coding is the first 32km practical remote point-to-point quantum secure communication network in Northeast China, which has been successfully implemented after debugging.

4 Theoretical Verification and Experimental Analysis

4.1 Verification of Randomness of Quantum Key Source

Among various optical signals, single phonon is the smallest energy unit and cannot be further divided. Hence, multiple dimensions of single-phonon signals can be used as sources of quantum randomness. However, ideal single phonon sources are barely possible. In practical application, the laser mainly reduces the average number of photons in the pulse to the level of single photon through attenuation, which is a quasisingle-photon source in the form of weak pulse laser. The pulse emitted by an ideal laser can be regarded as a coherent state, and expanded in Fock state:

$$|a>=e^{-|a|^2/2}\sum_{n=0}^{\infty}\frac{a^n}{n!}|n>. \tag{15}$$

where $|a>$ is coherent state, $|n>$ is Fock state, and the number of photons in coherent state conforms to the Poisson distribution:

$$P(n)=|n|a>|<a|n>=\frac{<n>^n e^{-(n)}}{n!}. \tag{16}$$

where $<n>^n=|a|^2$ is the average number of photons.

The effect of attenuator can be regarded as the photons passing with a certain probability. It is assumed that the average number of photons is β after the pulse passes through the attenuator, and the efficiency of the detector is η. Because the attenuation and detector effects are the same for all photons, the number of photons detected by the detector still conforms to the Poisson distribution:

$$P_\eta(n)=\frac{<\eta\beta>^n e^{-(\eta\beta)}}{n!}. \tag{17}$$

That is, the average number of photons is $\eta\beta$. The number of photons after passing the attenuator still

conforms to the Poisson distribution, indicating that the second-order correlation coefficient after passing the attenuator meets:

$$g^2(0) = 1. \tag{18}$$

According to the nature of the second-order correlation coefficient, it is known that pulses that conform to the above formula show neither bunching nor anti-bunching effects, and are independent of each other at any detection time. Therefore, in the above scheme for detecting single phonons, it is fully feasible to use a weak laser after strong attenuation instead of the single phonon source.

4.2 Analysis of NIST Packet Detection Results

The experimental environment was Intel (R) Core (TM) i5-2520M CPU @ 2.5GHz, 4G RAM, Win10 64-bit operating system. The simulation software used was Matlab R2016a. For the randomness detection of random numbers, there have been many general detection standards, including NIST detection, Diehard detection, and Three-Standard-Deviations detection [42-43]. The SP 800-22 test package provided by the National Institute of Standards and Technology is called NIST randomness test. NIST test is the national standard and technology research test. The basic idea of the test package is sub-tests based on numerous statistics, to determine whether to accept the original hypothesis usually using the P-Value method. An output sequence to be detected is divided into multiple fixed-length sub-sequences. According to the set confidence level α (the default value is 0.01), the probability where the sequence to be detected passes the sub-tests is given. When the test fails, sequences do not have confidence with sufficient randomness.

Table 2 shows the test results of random sequences obtained from five different generation methods. As observed, values of various random sequences were greater than α, indicating that they all successfully passed the test. Random sequences generated by polarization-coded and phase-coded QKD systems had P-values close to 1 at a single-bit frequency, which meets the requirements of uniform distribution of 0 and 1. As a whole, polarization-coded and phase-coded random numbers (P-VALUE) were generally higher than other values, especially in the frequency test, in-block frequency test, and run-length test. It proves that the Stochastic performances of polarization-coded sequences were better than those of other sequences. Stochastic performances of random sequences generated by chaos algorithms were worse than those of sequences generated by other methods, and in three sets of quantum key test results, Stochastic performances of post-processed random sequences were better than those of random sequences without post-processing.

Table 2. The test results of NIST-STS

Test \ Generate	BB84	Polarization-coded	Phase-coded	Chaos	Atmosphere noise
Monobit	0.298608	0.884565	0.882634	0.514356	0.096513
Block Frequency	0.764094	0.812248	0.790054	0.781222	0.322642
Runs	0.907452	0.914582	0.765659	0.723328	0.404926
Longest Run	0.437592	0.425815	0.423391	0.406910	0.413123
Binary matrix rank	0.164050	0.720546	0.622444	0.664683	0.601576
Dft	0.100348	0.11256	0.186864	0.17514	0.10005
NonOverlapping Template	1.000013	1.000002	0.998712	1.000020	1.013092
Overlapping Template	0.641599	0.854721	0.044196	0.647740	0.407883
Maurers universal*	0.999837	0.999958	0.999861	0.999645	0.999931
Iinear complexity	0.174272	0.254852	0.364865	0.38543	0.864439
Serial	0.433715	0.658411	0.813171	0.277872	0.291549
Approximate Entropy	0.754319	0.854712	0.973112	0.277692	0.291354
Cumulative sums	0.322354	0.766654	0.648273	0.727160	0.087374
Random excursion	0.282582	0.256844	0.191564	0.215553	0.013680
Random excursion variant	0.004437	0.051114	0.027875	0.453153	0.046413

4.3 Visual Random Verification Based on Statistical Characteristic Parameters

Experiment preparation. According to the preliminary judgment, the random performance of quantum key is better than that based on Chaos Theory and atmospheric noise. The randomness of the sequence can be detected by data packets, and the accuracy of the results needs to be further verified by local randomness test. In the aspect of image selection, Fig. 2 shows the synthesis of four carefully selected images, including classic Lena image, cameraman image, lifting body image, rice image, almost containing all kinds of attributes of the image, and there is no smooth transition at the junction of the four images, which is not available for general natural images, increasing the difficulty of image scrambling. Arnold scrambling uses the image matrix of order dimension to transform the pixel points (x, y) in the target image to (x', y'), and the transformation matrix is as follows [44]:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix} \bmod 1,\ x,\ y \in (0,1). \tag{19}$$

The above formula is the scrambling on the unit square. When the image size is N × N, the transformation matrix is expressed as follows:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix} \bmod N,\ x,\ y \in (0,1,...,N-1). \tag{20}$$

In Arnold scrambling, after a certain number of iterations, the target image pixels can be randomly and uniformly distributed in the scrambled image.

Fig. 2. Original graph

Visual analysis of experimental results. (Information entropy.) Shannon Entropy is a description index of statistical characteristics of random sequence [45]. Information entropy is used to measure the distribution of gray values in an image. The more uniform (random) the gray distribution is, the greater the information entropy is. That is to say, in the sequence satisfying the distribution, all information is effective information, and the stronger the image's ability to resist statistical attacks. Taking n-bit as a basic unit, the probability density distribution of the subsequence with n-bit length as the basic unit is investigated. The effective information in random sequence is described from the perspective of statistical distribution. Therefore, information entropy can also represent the statistical distribution and correlation between bits to a certain extent, and is widely used as a measure of randomness. The information entropy $H(I)$ can be defined as:

$$H(I) = \sum_{i=0}^{L-1} p(I_i) lg(p(I_i)). \tag{21}$$

where L = 256 represents the gray level, I_i represents the pixel value belonging to the ith gray level, and $p(I_i)$ represents the probability that the pixel value I_i appears in the image I.

In the experiment, the parameter verification results of encrypting the original image with different keys are shown in Table 3:

Table 3. Parameter verification results of encrypting images with different keys

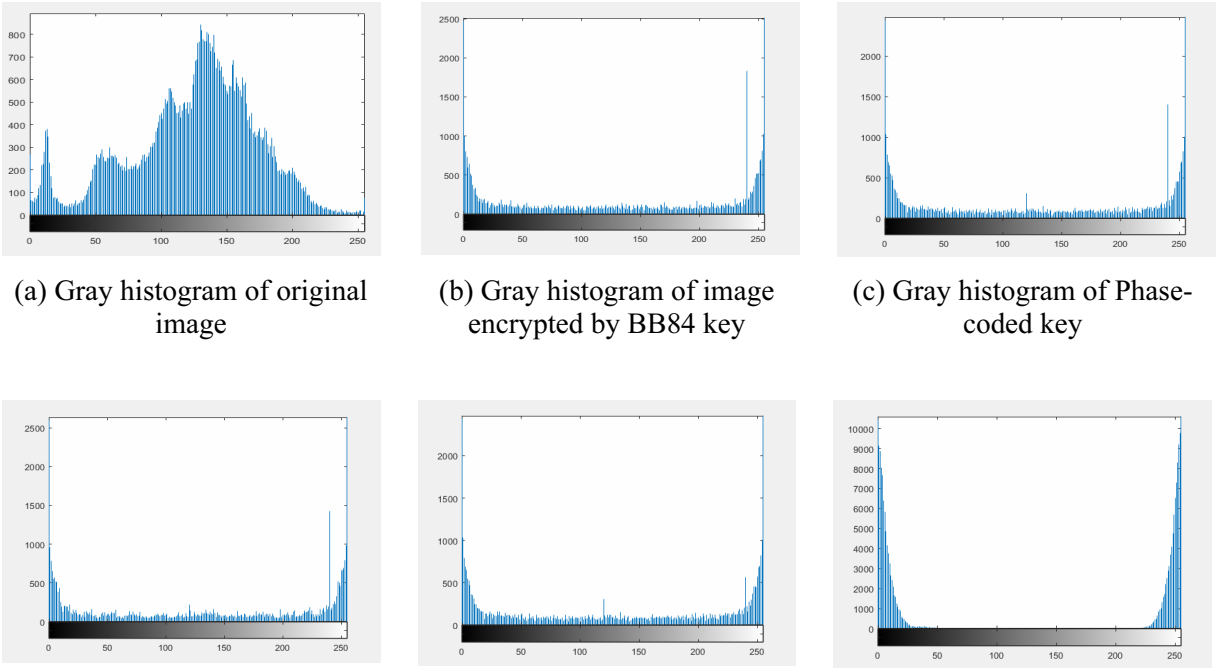
	Original graph	BB84	Phase-coded	Polarization-coded	Chaos	Atmosphere noise
mean value	124.1269	54.4436	61.7625	61.6581	69.7248	69.4614
variance	2.3793e+03	1.9861e+03	1.1005e+04	1.0985e+04	1.1983e+04	1.1955e+04
Information entropy	7.5145	7.8145	7.9743	7.9763	7.7375	7.7286

As observed, the entropy value of the images encrypted with the above random sequences were relatively close to the ideal value 8, which indicated that the five random sequences tested made the gray distribution of the original image more uniform and meet the uniform distribution, and all information was valid Information and had the greatest non-determinism. However, the information entropy value of the image encrypted using the quantum key generated by the QKD system changed more significantly, and the information entropy value was also the largest. The results indicated that the quantum key sequences had a uniformly distributed statistical feature. Hence, quantum key sequences have maximum information entropy and maximum uncertainty, and showed better Stochastic performance.

(Histogram and space histogram.) Digital image has both spatial distribution and statistical characteristics. How many pixels each image contains is a simple statistical feature. Gray histogram is widely used to find the binary threshold of gray image. The calculation formula is as follows:

$$p(r_k) = \frac{n_k}{MN}. \tag{22}$$

where r_k is the gray level of the pixel, n_k is the number of pixels with gray r_k, and MN is the total number of pixels in the image. The statistical results are shown in Fig. 3 and Fig. 4.



(a) Gray histogram of original image

(b) Gray histogram of image encrypted by BB84 key

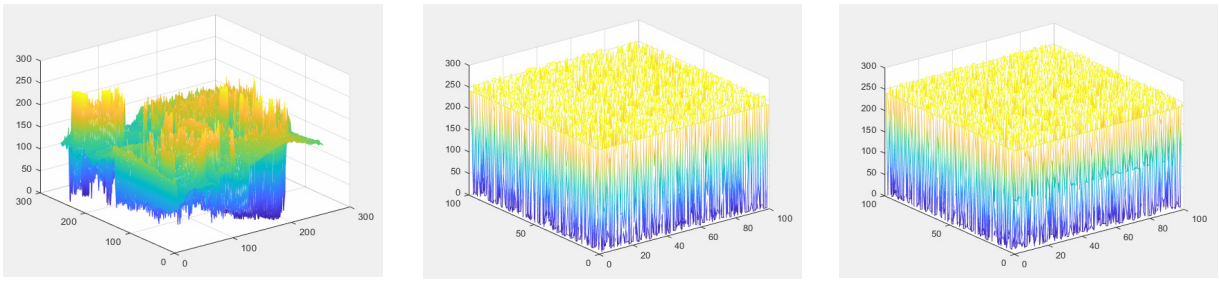
(c) Gray histogram of Phase-coded key

(d) Gray histogram of Polarization-coded key

(e) Gray histogram of Chaos key

(f) Gray histogram of Atmosphere noise key

Fig. 3.



(a) Gray space histogram of original image

(b) Gray space histogram of image encrypted by BB84 key

(c) Gray space histogram of Phase-coded key

(d) Gray space histogram of Polarization-coded key

(e) Gray space histogram of Chaos key

(f) Gray space histogram of Atmosphere noise key

Fig. 4.

As observed, the horizontal ordinate is the gray level, and the vertical ordinate is the sum of the number of pixels in each gray level in the picture. The grayscale histogram corresponding to each sequence had a certain change rule. Generally, the grayscale histogram appeared two crests, and there must be a gray value between the two crests to determine the range of the binarization threshold. From the histogram and three-dimensional visual effects, it can be seen that the gray level of the original histogram was obvious, and there were multiple troughs and crests. The grayscale histogram distributions of images scrambled with different sequences were all uniform, indicating that statistics information was better hidden. However, images scrambled with a quantum key had better diffusion and encryption performance.

(Correlation of adjacent pixels.)1800 pairs of adjacent pixels were taken from the original image and the scrambled image arbitrarily. The adjacent pixels in the horizontal, vertical, and diagonal lines were taken to calculate the correlation index of the adjacent pixels value according to the following formula [46]:

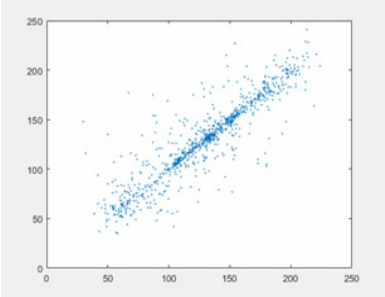
$$r_{pq} = \frac{\operatorname{cov}(p,q)}{\sqrt{D(p)D(q)}}. \tag{23}$$

$$\operatorname{cov}(p,q) = \frac{1}{N}\sum_{i=1}^{N}(p_i - E(p))(q_i - E(q)). \tag{24}$$

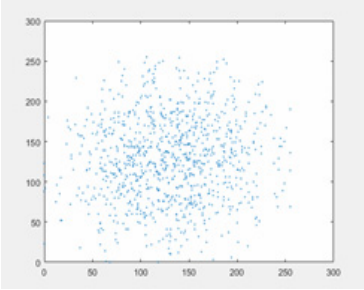
$$E(p) = \frac{1}{N}\sum_{i=1}^{N} p_i. \tag{25}$$

$$D(p) = \frac{1}{N}\sum_{i=1}^{N}(p_i - E(p))^2. \tag{26}$$

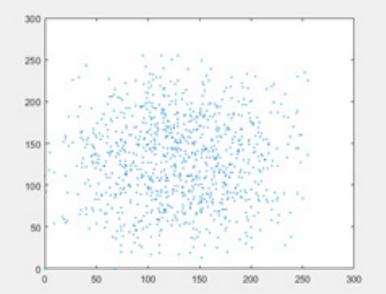
where p and q represent gray values of two adjacent pixels of the color QR code, N represents the number of pixels of the color QR code, and $E(p)$ and $E(q)$ represent the mean of p_i and q_i, respectively. The statistical results are shown in Fig. 5, Fig. 6 and Fig. 7.



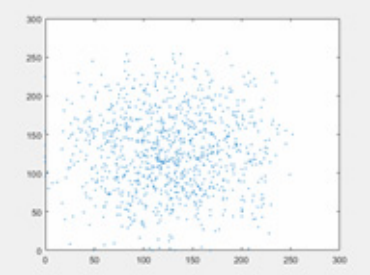
(a) Original image



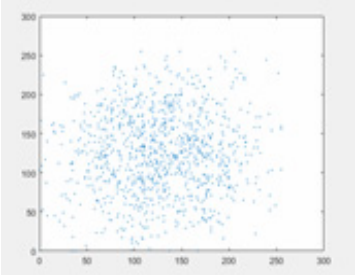
(b) Image encrypted by BB84 key



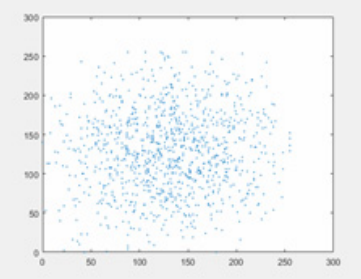
(c) Image encrypted by Phase-coded key



(d) Image encrypted by Polarization-coded key

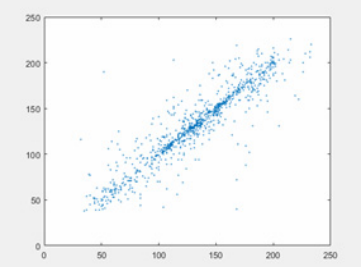


(e) Image encrypted by Chaos key

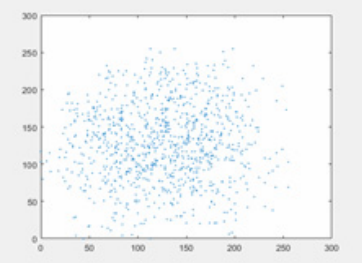


(f) Image encrypted by Atmosphere noise key

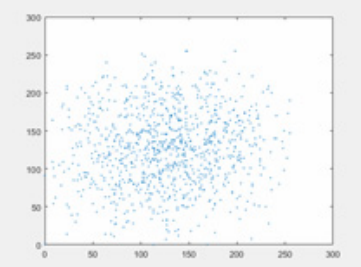
Fig. 5. Horizontal distribution



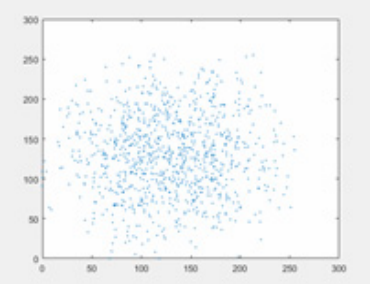
(a) Original image



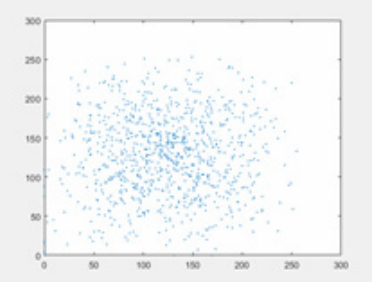
(b) Image encrypted by BB84 key



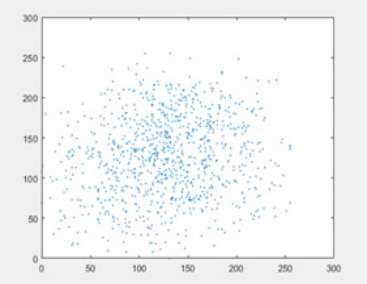
(c) Image encrypted by Phase-coded key



(d) Image encrypted by Polarization-coded key

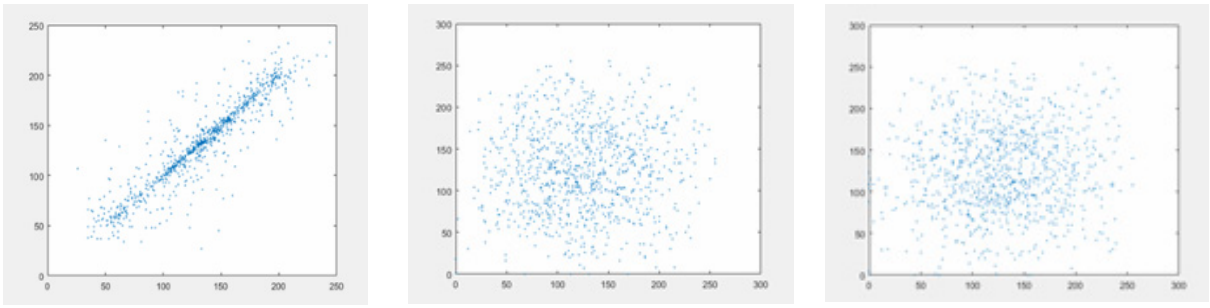


(e) Image encrypted by Chaos key



(f) Image encrypted by Atmosphere noise key

Fig. 6. Vertical distribution



(a) Original image (b) Image encrypted by BB84 key (c) Image encrypted by Phase-coded key

(d) Image encrypted by Polarization-coded key (e) Image encrypted by Chaos key (f) Image encrypted by Atmosphere noise key

Fig. 7. Diagonal distribution

The Arnold scrambling transform matrix was used to scramble the matrix. The measured experimental results are shown in Fig. 5, Fig. 6 and Fig. 7. Any adjacent pixel points in each component matrix are randomly distributed in the entire image space. The distributions of points on the horizontal, vertical and diagonal lines of the image represent the random distribution of each sequence, and the return values are shown in Table 4. As can be seen from the figure and the data in the table, the correlation coefficients of horizontal, vertical, and diagonal lines in the original picture were all larger than 0.2, and the image correlation coefficients encrypted using the above random sequences were reduced to a lower level, which indicated that the encrypted images had a certain autocorrelation. More importantly, the autocorrelation coefficients of encrypted images using quantum keys were significantly lower than those of images encrypted with random sequences generated by chaos and atmospheric noise, demonstrating improved Stochastic performances and attack resistance of quantum keys.

Table 4. Correlation of adjacent pixels

coefficient	Original image	BB84	Phase-coded	Polarization-coded	Chaos	Atmosphere noise
Horizontal	0.2794	-0.0732	-0.0742	-0.0516	-0.0887	-0.1042
Vertical	0.2596	-0.0680	-0.0569	-0.0397	-0.0680	-0.0758
Diagonal	0.2457	0.0491	0.0184	0.0162	0.0491	0.0494

5 Conclusions

QKD systems are highly dependent on random numbers and require TRNG to generate numerous high-quality random sequences to achieve secure communication. In this paper, NIST tests are performed with keys from different sources and the randomness is verified by visual analysis based on statistical parameters. Experimental results indicate that post-processed quantum random sequences have higher randomness and security than quantum random sequences without post-processing, pseudorandom

sequences and physical random sequences. The research results are helpful for the practicality and industrialization of quantum confidential communication technology.

Acknowledgements

The research was supported by the financial support from the National Science Fund Project of China No. (61772227), Jilin development and reform commission construction fund (2020C020-2), Science Technology Development Foundation of Jilin Province under grant No. (20180201045GX), Education Department of Jilin Province (No. JJKH20191201KJ, JJKH20190902KJ).

References

[1] H. Guo, Z. Li, X. Peng, Quantum Cryptography, Modern laser technology and Application, National Defense Industry Press, 2016, ISBN：9787118111729.

[2] B. Wang, G. Hu, H. Zhang, C. Wang, From Evolutionary Cryptography to Quantum Artificial Intelligent Cryptography, Journal of Computer Research and Development 56(10)(2019) 2112-2134.

[3] B. Ge, Design and application of a new pseudo-random number generator [doctoral dissertation], University of Chinese Academy of Sciences, 2016.

[4] S.W. Golomb, Shift register sequences, San Francisco: Holde-Day Inc, 1967 (21-24).

[5] G.S. Fishman, L.R. Moore, An exhaustive analysis of multiplicative congruential random number generators with modulus 231-1*, SIAM Journal on Scientific and Statistical Computing 7(1)(1986) 24-45.

[6] Y. Guo, S. Sun, An image encryption algorithm based on true random number and pseudo random number, Journal of Shaanxi Normal University (Natural Science Edition) 48(2)(2020) 52-57.

[7] X. Ma, J. Yu, F. Yang, J. Mou, Pseudo-random sequence generator based on high-dimensional chaotic system, Journal of Dalian Polytechnic University 39(2)(2020) 143-149.

[8] Q. Ding, J. Pang, J.Q. Fang, X.Y. Peng, Designing of chaotic system output sequence circuit based on FPGA and its applications in network encryption card, International Journal of Innovative Computing, Information and Control 3(2)(2007) 449-456.

[9] M. Drutarovsky, P. Galajda, Chaos-based true random number generator embedded in a mixed-signal reconfigurable hardware, Journal of Electrical Engineering 57(4)(2006) 218-225.

[10] L.Y. Sheng, L.L. Cao, K.H. Sun, J. Wen, Pseudo-random number generator based on TD-ERCS chaos system and its statistic characteristics analysis, Acta Physica Sinica-Chinese Edition 54(9)(2005) 4031-4037.

[11] F.H. Xu, X.F. Ma, Q. Zhang, H.K. Lo, J.W. Pan, Secure quantum key distribution with realistic devices, Reviews of Modern Physics 92(2)(2020) 025002.

[12] http://www.random.org/.

[13] R.P. Liu, C. Chen, M.C. Wu, P. Li, X.M. Guo, Y.Q. Guo, High-speed Quantum Random Number Generation based on Continu-ous Variable Vacuum Noise, Study on Optical Communications (5)(2019) 22-27,70.

[14] H. Schmidt, Quantum-mechanical random-number generator, Journal of Applied Physics 41(2)(1970) 462.

[15] R. Yang, E. Hou, H. Liu, L. Gong, Y. Wang, J. Zhang, Low-power physical random number generator using Boolean networks, Journal of Shenzhen University Science and Engineering 37(1)(2020) 51-56.

[16] Q. Yan, B. Zhao, Q. Liao, N. Zhou, Multi-bit Quantum Random Number Generation by Measuring Positions of Arrival Photons, Review of Scientific Instruments 85(10)(2014) 103116.

[17] Y. Ji, M. Zhuang, G. Zhang, A. Chen, L. Wang, W. Li, High speed measurement device independent quantum key distribution with finite detector dead time, Infrared and Laser Engineering 47(z1)(2018) 55-59.

[18] Y.Q. Nie, H.F. Zhang, Z. Zhang, J. Wang, X.F. Ma, J. Zhang, J.W. Pan, Practical and Fast Quantum Random Number Generation based on Photon Arrival Time Relative to External Reference, Applied Physics Letters 104(5)(2014) 051110.

[19] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, H. Zeng, Quantum Random-Number Generator based on Photon- Number-Resolving Detector, Physical Review A 83(2)(2011) 023820.

[20] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, H. Lo, Ultrafast Quantum Random Number Generation based on Quantum Phase Fluctuations, Optics Express 20(11)(2012) 12366-12377.

[21] Y. Liu, M. Zhu, B. Luo, J. Zhang, H. Guo, Implementation of 1.6 Tb s-1 Truly Random Number Generation Based on a Super-Luminescent Emitting Diode, Laser Physics Letters 10(4)(2013) 045001.

[22] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U.L. Andersen, C. Marquardt, G. Leuchs, A Generator for Unique Quantum Random Numbers based on Vacuum States, Nature Photonics 4(10)(2010) 711-715.

[23] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, H.K. Lo, Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction, Physical Review A 87(6)(2013) 062327.

[24] C.Z. Peng, J. Zhang, D. Yang, W.B. Gao, H.X. Ma, H. Yin, H.P. Zeng, T. Yang, X.B. Wang, J.W. Pan, Experimental Long-Distance Decoy-State Quantum Key Distribution Based On Polarization Encoding, Physical review letters 98(1)(2007) 010505.1-010505.4.

[25] H.Y. Zhou, X. Yuan, X.F. Ma, Randomness generation based on spontaneous emissions of lasers, Physical Review A 91(6)(2015) 062316.

[26] Y. Liu, Q. Zhao, M.H. Li, J.Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.Z. Liu, C. Wu, X. Yuan, H. Li, W.J. Munro, Z. Wang, L. You, J. Zhang, Z. Ma, J. Fan, Q. Zhang, J.W. Pan, Device-independent quantum random-number generation, Nature 562(7728)(2018) 548-551.

[27] X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.L. Tang, Y.J. Sheng, Y. Xiang, W. Zhang, H. Li, Z. Wang, L. You, M.J. Li, H. Chen, Y.A. Chen, Q. Zhang, C.Z. Peng, X. Ma, T.Y. Chen, J.W. Pan, Implementation of quantum key distribution surpassing the linear rate-transmittance bound, Nature Photonics 14(2020) 422-425.

[28] A. Renyi, On measures of entropy and information, in: Proceedings of the fourth Berkeley symposium on mathematical statistics and probability, 1961.

[29] L.E. Bassham, A.L. Rukhin, J. Soto, J.R. Nechvatal, M.E. Smid, S.D. Leigh, M. Levenson, M. Vangel, N.A. Heckert, D.L. Banks, A Statistical test suite for random and pseudorandom number generators for cryptographic applications, Special Publication (NIST SP)- 800-22 Rev 1a, 2010.

[30] G. Marsaglia, DIEHARD: a battery of tests of randomness, 1996.

[31] R.G. Brown, D. Eddelbuettel, D. Bauer, Dieharder: A random number test suite, Open Source software library, under development, 2013.

[32] P. L'Ecuyer, R. Simard, TestU01: A C library for empirical testing of random number generators, ACM Transactions on Mathematical Software (TOMS) 33(4)(2007) 22.

[33] X. Ma, X. Yuan, Z. Cao, B. Qi, Z. Zhang, Quantum random number generation, Quantum Information 2(2016) 16021.

[34] M. Herrero-Collantes, J.C. Garcia-Escartin, Quantum random number generators, Reviews of Modern Physics 89(1)(2017) 015004.

[35] L.Y. Sheng, L.L. Cao, K.H. Sun, J. Wen, Pseudo-random number generator based on TD-ERCS chaos and its statistic characteristics analysis, Acta Physica Sinica 54(9)(2005) 4031-4037 (in Chinese).

[36] X.J. Yao, X. Tang, Z.M. Wu, G.Q. Xia, Multi-channel physical random number generation based on two orthogonally mutually coupled 1550 nm vertical-cavity surface-emitting lasers, Acta Physica Sinica 67(2)(2018) 024204.

[37] C.H. Henry, Theory of the linewidth of semiconductor lasers, IEEE Journal of Quantum Electronics 18(2)(1982) 259-264.

[38] B. Qi, Y.M. Chi, H.K. Lo, L. Qian, High-speed quantum random number generation by measuring phase noise of a single-mode laser, Optics Letters 35(3)(2010) 312-314.

[39] E. N. Lorenz, Deterministic Nonperiodic Flow, Journal of the Atmospheric Sciences 20(2)(1963) 130-141.

[40] T.Y. Li, J.A. Yorke, Period Three Implies Chaos, The American Mathematical Monthly 82(10)(1975) 985-992.

[41] E. Ott, Chaos in dynamical systems, Cambridge: Cambridge University Press, 1993.

[42] J. Liu, Q. Qu, Randomness tests of several chaotic sequences, Computer Engineering and Applications 47(5)(2011) 46-49.

[43] G. Shi, F. Kang, H. Gu, Research and implementation of randomness tests, Computer Engineering 35(20)(2009) 145-147.

[44] Y. Guo, Y.Y. Zhou, S.W. Jing, Multiple-image Encryption Based on Image Recombination and Bit Scrambling, Acta Photonica Sinica 49(4)(2020) 174-186.

[45] C.E. Shannon, A mathematical theory of communication, The Bell System Technical Journal 27(4)(1948) 623−656.

[46] G. Xie, B. Yang, Quantum chaos image encryption algorithm based on bit scrambling, Computer Engineering 43(7)(2017) 182-186, 192.