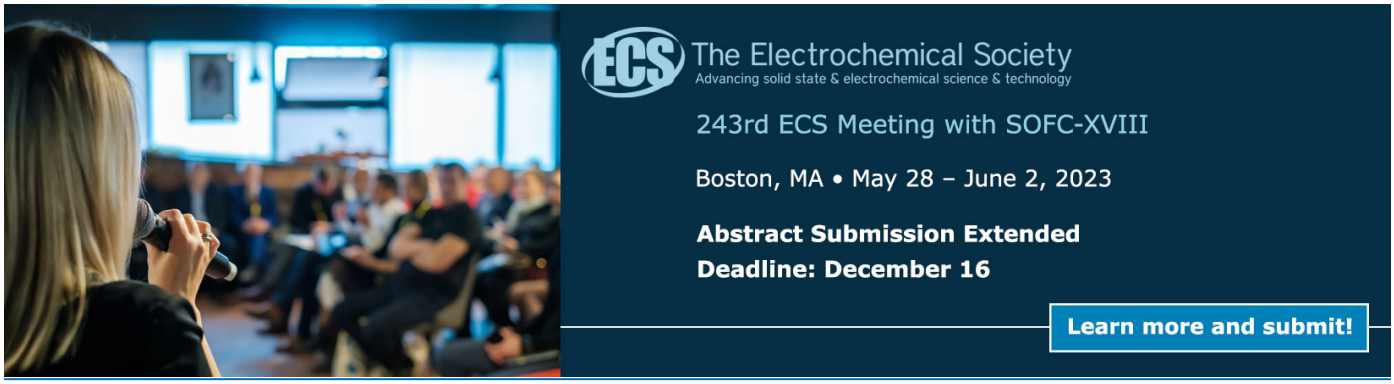
A quantum pseudo-random number generation scheme



A quantum pseudo-random number generation scheme

Yinghua Jiang[1], Biao Liu[1], Chenfei Guo[1] and Jiangbo Zhao[1,*]

[1] College of Information Engineering, Xizang Minzu University, Xianyang City, Shaanxi Province, 712000, China

*Corresponding author's e-mail: jbzhao@xzmu.edu.cn
*Corresponding author's ORCID: https://orcid.org/0000-0001-9831-2595

Abstract. Quantum random key distribution based on physical properties of quantum mechanics has high security and true randomness, but it has the disadvantages of low key generation efficiency and high cost. The classic pseudo-random number generator has the advantages of simple algorithm and high key generation efficiency, but it has extremely strict requirements on the security and randomness of the "seed". Based on the analysis of two unrelated technologies, this paper proposes a pseudo-random number generation scheme based on quantum key distribution. This scheme makes full use of quantum key distribution to share a short quantum random number-seed between the two communicating parties, then inputs the seed into a pseudo-random number generator. Finally, the two communicating parties share a long random number to encrypt the communication content. Research shows that compared with classic quantum key distribution and classic pseudo-random number generator, this scheme has stronger security, better randomness, and higher key generation efficiency.

1. Introduction

Quantum secure communication is a new discipline combining quantum mechanics, information theory and cryptography. It is a new communication method that uses the quantum characteristics of microscopic particles as an information carrier to convey secret information. Compared with classical communication methods, quantum secure communication has huge advantages in various aspects such as security, transmission efficiency, and channel capacity. This has made quantum secure communication as a new hot spot and direction in scientific research and technological development in the field of communication and information. Among the numerous applications of quantum communication, Quantum Key Distribution (QKD) which shares a random quantum key between two parties in communication, not only is the most in-depth research, it is also a significant direction which is closest to practicality. Scholars studying QKD have proposed a crowd of important quantum cryptographic protocols. In 1984, Bennett and Brassard jointly developed first QKD (BB84 protocol) in the world which depends on single-photon polarization states[1]; in 1992, Bennett Proposed QKD depends on non-orthogonal single photon bits (B92 protocol)[2]; in 1991, Ekert of the University of Oxford in UK first proposed QKD depends on Bell state entanglement[3]; Bennett, Brassard and Mermim had ameliorated the protocol of Ekert to make it more concise which implement QKD without utilizing Bell state[4]. In the current, Quantum Identity Authentication (QIA)[5-7], Quantum Secret Sharing (QSS)[8-13] and Quantum Private Comparison (QPC)[14-16] are rapidly developing towards practical aspects.

In 1917, G.S.Vernam proposed a one-time pad (OTP) encryption method[17], and G. Shannon proved the unconditional security of this encryption method in 1949[18]. OTP refers to a symmetric

cryptographic algorithm in which the communicating parties use a random key equal to the plaintext to encrypt and decrypt the plaintext, and the key is discarded after being used once. Although OTP is extremely secure, it is difficult to share a sufficiently long random key between the two parties in the communication. Quantum key distribution can achieve high-strength security key distribution between the two communicating parties, but it faces an adverse situation in lower generation efficiency of key and higher cost. If the amount of data between the two parties in the communication is copious, this problem of QKD will be more critical.

Pseudo Random Number Generator (PRNG) is an algorithm that inputs "seed" into a preset mathematical algorithm and outputs a stable pseudo-random sequence at an extremely fast rate, and the statistical characteristics of sequence are guaranteed by the algorithm. The method of PRNG is characterized by simple devices, mature algorithms, and high generation efficiency. Therefore, it is widely used in gaming activities, statistical sampling, and numerical simulation. Due to the algorithm of the classic PRNG is public, the security of the PRNG entirely depends on the confidentiality of the "seed", and the randomness of sequence is extremely correlating with the randomness of the "seed".

In order to realize the sharing of high-efficiency random numbers between two communication parties, this paper proposes a quantum pseudo-random number generation scheme, to alleviate the problem of low key generation rate and high cost in QKD technology, and the problem that the PRNG requires a high level of confidentiality and randomness of the "seed". This scheme uses a method which QKD will share a "seed" key with the same binary bits between the two parties in communication, and the“seed”will be inputted into a pseudo-random number generator of the same algorithm. In the result, both parties share a same Binary bit of pseudo-random number used as a one-time pad secret key. Compared with the classic QKD protocol, this scheme makes full use of the security and randomness of QKD, and alleviates the problems of slow generation rate and high cost in the QKD. Compared with the classic PRNG scheme, in this scheme, the “seeds” with unconditional security and true randomness ensure the security and randomness of pseudo-random numbers. Therefore, the random number shared by this scheme makes grate contributions to strong security, good randomness and high rate of key generation.

2. Basic knowledge of relevant issues

Pseudo-random number generation algorithms generally include square method, Fibonacci method, shift method, linear congruence method, nonlinear and inverse congruence method, and taking the minimum number method.

The advantages of the square method are simple calculation, easy implementation on a computer, and low memory consumption. While there are some existing disadvantages such as the phenomenon of a bias against a small number, the poor nature of uniformity, the difficulty in uncertain length and periodicity, the serious dependence on initial data and a problem that the randomness of the sequence of numbers is prone to degradation. The advantages of the Fibonacci method are simple calculations, fast speeds of calculation, and long periods. The disadvantages are that the numbers in the random sequence are easy to repeat, the independence is poor, there is a phenomenon of non-uniform and they have significant sequence correlation. The advantage of the shift method is the fast operation speed; the disadvantage is that it depends heavily on the initial value. If the initial value is too small, the length of the pseudo-random number sequence is short and the independence is poor. And the period of the random sequence is related to the computer word length. The calculation speed of the linear congruence method is acceptable, but the disadvantage is that there are sparse grids at high latitudes and long-period correlation. The non-linear and inverse congruence methods are complicated to calculate and have a large amount of calculation. So, its disadvantages are that the random sequence has low generation efficiency, there is a long period phenomenon, and the period depends on the computer word length. The advantage of taking the minimum number method is that it is simple to calculate and easy to implement; the disadvantage is that the "seed" is a pure decimal number with a long digit.

Analysis of six PRNG algorithms in five dimensions: "computation complexity", "Degree of dependence on seed", "random sequence uniformity", "random sequence periodicity" and "random sequence generation efficiency". The results are shown in Table I.

Table 1. Table of analysis results of six pseudo-random generation algorithms.

	Computation complexity	Degree of dependence on seed	Random sequence uniformity	Random sequence periodicity	Random sequence generation efficiency
Square method	simple	high	poor	short	high
Fibonacci method	simple	general	poor	long	high
Shift method	simple	high	poor	short	high
Linear congruence method	**general**	**low**	**good**	**long**	**general**
Nonlinear and inverse congruence method	complex	low	good	long	low
Taking the minimum number method	simple	high	poor	short	high

The analysis shows that the linear congruence method has low dependence on "seeds", good random sequence quality, and acceptable computational complexity and generation efficiency. Therefore, it is a suitable quantum pseudo-random number generation scheme combining the linear congruence method with QKD. The linear congruence method is a pseudo-random number generation algorithm which is widely used at present. The basic idea is to perform a linear operation on the previous number and take a modulus to obtain the next number. The recursive formula is:

$$x_{n+1} = (ax_n + c) \bmod m \tag{1}$$

In the formula: a is a multiplier, $0<a<m$; c is an increment, $0\leq c<m$; m is a modulus, $m>0$; x_0 is an initial value, $0\leq x_0<M$; x_{n+1} is a random number, $0\leq x_{n+1}<M$.

The quantum key distribution used in this scheme involves two kinds of measurement bases, X-base and Z-base, $\{|+\rangle, |-\rangle\}$ is a set of standard orthogonal bases, X-basis; $\{|+\rangle, |-\rangle\}$ is another set of standard orthogonal bases, Z-basis. X-basis and Z-basis are non-orthogonal basis, and they satisfy the following relationship:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad , \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad ,$$
$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \quad , \quad |1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) \quad . \tag{2}$$

The results of the four different states measured by the two measurement bases are shown in Table II.

Table 2. Measurement results of different states.

	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
Z-basis	$\|0\rangle$	$\|1\rangle$	50%$\|0\rangle$ or 50%$\|1\rangle$	50%$\|0\rangle$ or 50%$\|1\rangle$

X-basis	50%$\|+\rangle$ or 50%$\|-\rangle$	50%$\|+\rangle$ or 50%$\|-\rangle$	$\|+\rangle$	$\|-\rangle$

3. Quantum pseudo-random number generation scheme

Step 1: Alice and Bob share a linear congruent random number generation algorithm in the open channel.

Step 2: Alice randomly prepares a quantum sequence S_1 containing 4n single photons whose polarization state is one of ($|0\rangle, |1\rangle, |+\rangle, |-\rangle$). Alice sends S_1 to Bob via a quantum channel.

Step 3: After Bob receives S_1, he uses the X-basis or Z-basis to measure S_1 randomly, and publishes the sequence of the bases which is used through the common channel.

Step 4: Alice compares the base sequence used by Bob with the base sequence of S_1 prepared by himself. In order to form the quantum sequence S2, the single photon state corresponding to the same base should be retained, while the single photon state corresponding to the different base should be discarded.

Step 5: Alice randomly selects a part of the single photon in S_2 and publicly announces its preparation status. Bob compares the preparation status and measurement status of this part of the single photon for eavesdropping inspection.

Step 6: If Bob finds that the bit error rate of the temptation particle exceeds the threshold, there is an eavesdropping in the communication and the protocol is terminated; otherwise, there is no eavesdropping in the communication and the protocol continues.

Step 7: Alice and Bob round off the photons for eavesdropping inspection at the same time, and the remaining particles form a quantum sequence S_3. Since ($|0\rangle, |-\rangle$) is encoded as 0 and ($|1\rangle, |+\rangle$) is encoded as 1 in S_3, Alice and Bob obtain the binary bit sequence k1 according to S_3.

Step 8: Alice and Bob use k_1 as a "seed" to input a linear congruence algorithm and they obtain a pseudo-random sequence binary bit sequence k_2.

The scheme flow is shown in Figure 1.

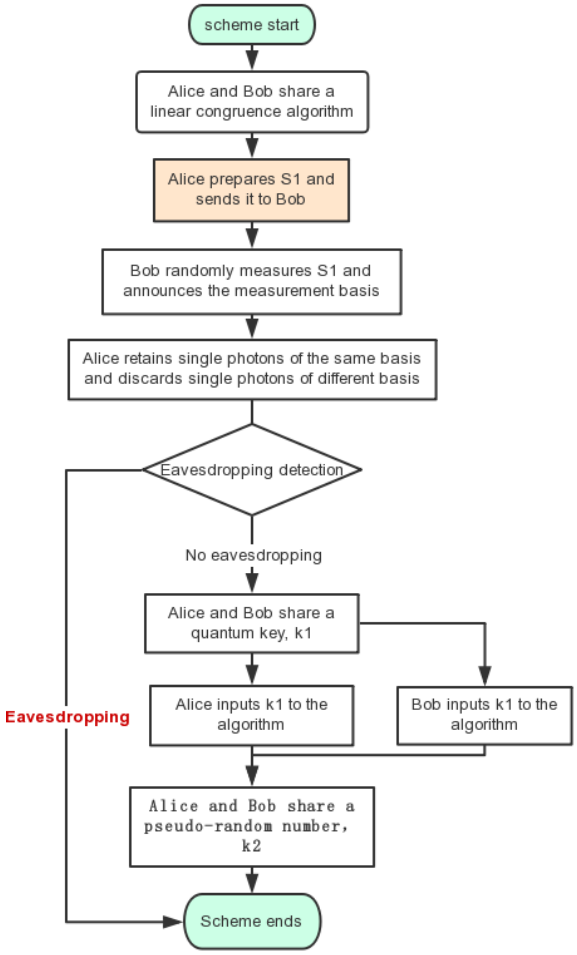


Figure 1. Flow chart of quantum pseudo-random number generation scheme.

4. Experimental results

Through the quantum key distribution equipment, as shown in Figure 2, a "seed" key--k_1 is shared between users Alice and Bob. The quantum key distribution device obtains k_1 by steps such as stabilizing the transmission voltage, finding synchronization light and automatically synchronizing the delay, as shown in Figure 3.

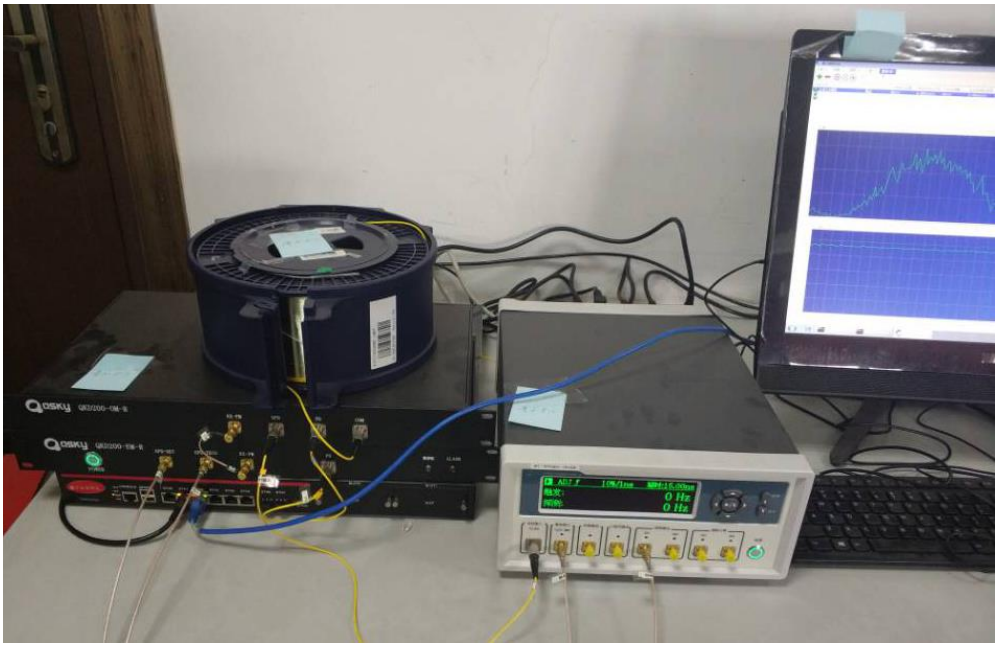


Figure 2. Quantum key distribution equipment.

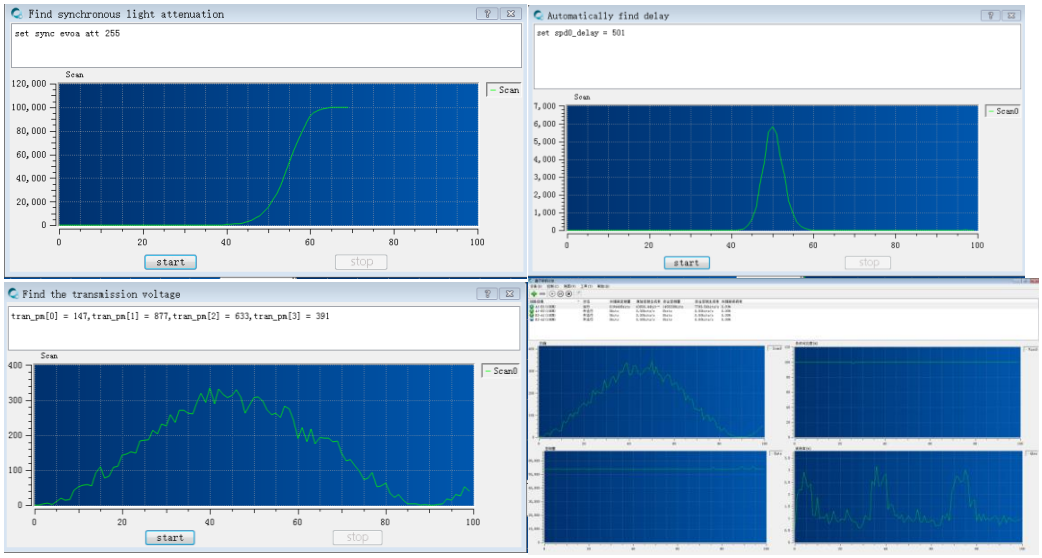


Figure 3. Generation of quantum random keys.

The 20-bit binary bit key k_1 generated by the quantum key distribution equipment is used as a "seed" in the linear congruence algorithm to obtain a 200-bit binary bit pseudo-random number k_2. The code and running result of the linear congruence algorithm are shown in Figure 4.

```
In [2]: from time import time
#defin the m,a,c
m = 2 ** 32
a = 1103515245
c = 12345
# the LCG algorithm
def LCG(seed):
    seed = (a * seed + c) % m
    return seed / float(m-a)
#the QKD binary nums to decimal
def bin2dec(binaryString):
    # the length of binaryString must be even,such as 100
    # the the measurement result as 00 11 01 10
    # eg:the MR is :|0> |0> |+> |1>,the binaryString is: 00000111, we do binary to decimal to 00000111 -->7
    return int(binaryString,2)
#main
def main():
    #br = input("please enter the range (separated by ,)with which the random number is generated:")
    #mi = eval(br.split(',')[0])
    #ma = eval(br.split(',')[1])
    #print("The range of random number generation is pow(10,200-1) to pow(10,201)-1")
    mylen = 200
    mi = pow(10,mylen-1)
    ma = pow(10,mylen)-1
    # seed = time()
    originalSeq = '00010011101100011100'
    seed = bin2dec(originalSeq)
    rd = LCG(seed)
    #print("seedRd is :{}".format(rd))
    print ("The seed sequence produced by QKD is : \n{}".format(originalSeq))
    ourd = int ((ma-mi)*rd) + mi
    print("The 200-bit pseudorandom sequence generated by the linear congruence algorithm is: \n{}".format(ourd))
# main
begin_time = time()
main()
end_time = time()
run_time = end_time-begin_time
print("Time used:",run_time)

The seed sequence produced by QKD is :
00010011101100011100
The 200-bit pseudorandom sequence generated by the linear congruence algorithm is:
34692747548974533546918867053900262616751216906752918424656822496402858795320855624347222012560229731624874481043777506558452
87719085661779650587728450704152650286320700983465869162388380750322860032
Time used: 0.0009641647338867188

In [3]: len('34692747548974533546918867053900262616751216906752918424656822496402858795320855624347222012560229731624874481043777506584

Out[3]: 200
```

Figure 4. The code and running result.

5. Security analysis of the scheme

5.1. Intercept/resend attack.

If there is an eavesdropper Eve over the course of the communication between Alice and Bob, most of the information of this scheme is disclosed through the public channel, so the eavesdropping behavior can only occur on the quantum channel. If Eve intercepts and eavesdrops on the qubits in S_1, then sends the quantum sequence to Bob. Because the quantum states used in this scheme are non-orthogonal to each other, Eve does not know the specific quantum states and cannot obtain information. According to the quantum unclonable theorem (it is impossible to clone the quantum without destroying the unknown quantum), it can be known that Eve's eavesdropping behavior will inevitably bring disturbance to S1. Furthermore, this eavesdropping behavior will be discovered by Alice and Bob through the bit error rate, so the intercept/resend attack cannot be successful.

5.2. Entanglement attack.

If the eavesdropper Eve intercepts the qubit sequence S_1, and performs a normal operation on the particles in S_1 to make it form a larger Hilbert space.

$$E \otimes |0e\rangle = a|0e_{00}\rangle + b|1e_{01}\rangle$$

$$E \otimes |1e\rangle = b'|0e_{10}\rangle + a'|1e_{11}\rangle$$

$$E \otimes |+e\rangle = \frac{1}{\sqrt{2}}\left(a|0e_{00}\rangle + b|1e_{01}\rangle + b'|0e_{10}\rangle + a'|0e_{11}\rangle\right)$$

$$= \frac{1}{2}\left[|+\rangle\left(a|0e_{00}\rangle + b|1e_{01}\rangle + b'|0e_{10}\rangle + a'|0e_{11}\rangle\right) + |-\rangle\left(a|0e_{00}\rangle - b|1e_{01}\rangle + b'|0e_{10}\rangle - a'|0e_{11}\rangle\right)\right]$$

$$E \otimes |-e\rangle = \frac{1}{\sqrt{2}}\left(a|0e_{00}\rangle + b|1e_{01}\rangle - b'|0e_{10}\rangle - a'|0e_{11}\rangle\right)$$
$$= \frac{1}{2}\left[|+\rangle\left(a|0e_{00}\rangle + b|1e_{01}\rangle - b'|0e_{10}\rangle - a'|0e_{11}\rangle\right) + |-\rangle\left(a|0e_{00}\rangle - b|1e_{01}\rangle - b'|0e_{10}\rangle + a'|0e_{11}\rangle\right)\right] \quad (3)$$

The four pure states $\{e_{00}, e_{01}, e_{10}, e_{11}\}$ determined by the operator E satisfy the normalization conditions:

$$\sum_{\alpha,\beta\in\{0,1\}} \langle e_{\alpha,\beta}|e_{\alpha,\beta}\rangle = 1 \quad (4)$$

The matrix of Eve's unitary operation E is expressed as

$$E = \begin{pmatrix} a & b' \\ b & a' \end{pmatrix} \quad (5)$$

Since EE*=1 , a, b, a ', b' satisfy the following relationship

$$|a|^2 + |b|^2 = 1$$
$$|a'|^2 + |b'|^2 = 1$$
$$ab^* = (a')^* b' \quad (6)$$

Then, we get the result

$$|a|^2 = |a'|^2, |b|^2 = |b'|^2 \quad (7)$$

If Eve attacks particles in an entangled state, the eavesdropper's interference will inevitably introduce errors, so that the presence of the eavesdropper can be detected with a probability of P:

$$P = |b|^2 = 1 - |a|^2 = |b'|^2 = 1 - |a'|^2 \quad (8)$$

When Eve does not want to introduce error, the total particles must be related to Eve's direct state of the auxiliary quantum states. However, the stochastic state indicates that there is no correlation between the auxiliary particle and the particle of S_1, so the eavesdropper does not get any useful information, thus proving that the entanglement attack will not be successful.

6. Random analysis of the scheme

The quantum random number obtained by experiments is k_1 which is used as the "seed" to input the linear congruence algorithm to obtain the pseudo-random sequence decimal bit sequence k_2. The value of k_1 and k_2 are shown in Table III.

Table 3. The value of k_1 and k_2.

	The value
k_1	00010011101100011100
k_2	28348386471240871623729309818022537734895730878522876471662289203101808468184608257706587530381224342174921422916505856310581267548082226439880216309280330330589508989884390920249812478106312562966528

Use the ENT (Pseudo-random Number Sequence Test Program) test program to test the random characteristics of k_2. The test results are as follows

The arithmetic mean of k2 is α, α = 4.41;

The variance of k_2 is β, β = 8.6619;

The first-order autocorrelation function of k_2 is γ, γ = 0.07.

Therefore, the pseudo-random number k_2 satisfies a random number characteristic.

7. Effectiveness analysis of the scheme

The generation time of k_1 is t_1, and $t_1 = 0.00256$s. The generation time of k_2 is t_2, and $t_2 = 0.00047$s.

The quantum random key generation efficiency is η_1, $\eta_1 = 7799.54$b / s, and the pseudo-random number generation efficiency obtained by the linear congruence algorithm is η_2,

$$\eta_2 = 600\text{bit} / (t_1 + t_2) = 600\text{bit}/(0.00256\text{s}+0.00047\text{s}) = 198216.06\text{b} / \text{s} \quad (9)$$

In the experiment, the ratio of quantum pseudo-random number generation efficiency to quantum random key efficiency is p,

$$p=\eta 2/\eta 1=198216.06/7799.54=25.42 \quad (10)$$

As the length of the random number key further increases, the generation efficiency of the quantum pseudo-random number will further improve, and the ratio to the quantum random key will be higher than 25.42. Therefore, quantum pseudo-random numbers are more efficient in key generation than quantum random keys.

8. Conclusion

The algorithm used in this solution is simple and easy to implement. The key generation speed is fast. The security of the key is based on the Heisenberg uncertainty principle in quantum mechanics, the quantum non-clonable theorem, the relevance and non-locality of entangled particles. Therefore, random numbers have unconditional security and true randomness. By combining quantum key distribution with classical pseudo-random number generation algorithms, the quantum pseudo-random number generation scheme combines the advantages of both and overcomes the shortcomings of the two technologies. This scheme improves the security, randomness, and key generation efficiency of shared random numbers, and reduces the cost of key generation, thereby making the one-time pad encryption method easier to implement in real life.

References

[1] Bennett C H. (1984) Quantum cryptography: Public key distribution and coin tossing[C] Proc. IEEE International Conference on Computers Systems and Signal Processing. 175-179.
[2] Bennett C H. (1992) Quantum cryptography using any two nonorthogonal states.[J]. Physical Review Letters, **68**(68): 3121-3124.
[3] Ekert A K. (1991) Quantum cryptography based on Bell's theorem[J]. Physical Review Letters, **67**(6): 661-663.
[4] Bennett C H, Brassard G, Mermin N D. (1992) Quantum cryptography without Bell's theorem.[J]. Physical Review Letters, **68**(5): 557-559.
[5] Zhang XingLan. (2009) One-way quantum identity authentication based on public key[J]. Chinese Science Bulletin, **12**: 2018-2021.
[6] YuGuang Yang, Qiaoyan Wen, Xing Zhang. (2008) Multiparty simultaneous quantum identity authentication with secret sharing[J]. Science in China, **03**: 99-105.
[7] Zhang XingLan. (2009) One-way quantum identity authentication based on public key[J]. Chinese Science Bulletin, **54**(12): 2018-2021.
[8] Shi J H, Zhang S L, Zhang H L, et al. (2014) One-insider attack of quantum secret sharing protocol with collective eavesdropping check[J]. Quantum Information Processing, **13**(1): 33-42.
[9] Chen R K, Zhang Y Y, Shi J H, et al. (2014) A multiparty error-correcting method for quantum secret sharing[J]. Quantum Information Processing, **13**(1): 21-31.
[10] Shi W M, Zhang J B, Zhou Y H, et al. (2016) A non-interactive quantum deniable authentication protocol based on asymmetric quantum cryptography[J]. Optik - International Journal for Light and Electron Optics, **127**(20): 8693-8697.

[11] Tsai C W, Hwang T. (2012) Multi-party quantum secret sharing based on two special entangled states[J]. Science China Physics, Mechanics & Astronomy, **55**(3): 460-464.
[12] Yu Wang, Caixing Tian, Qi Su. (2019) Measurement-device-independent quantum secret sharing and quantum conference based on Gaussian cluster state[J]. Science China Information Sciences, **62**(7): 72501.
[13] Jiang Y H, Zhang S B, Dai J Q, et al. (2018) Quantum secret information equal exchange protocol based on dense coding[J]. Modern Physics Letters B, **32**: 1850125-.
[14] Liu W J, Liu C, Liu Z H, et al. (2014) Erratum to: Same Initial States Attack in Yang et al. Quantum Private Comparison Protocol and the Improvement[J]. International Journal of Theoretical Physics, **53(3)** 271-276.
[15] Chen Y T, Hwang T. (2014) Comment on the "Quantum Private Comparison Protocol Based on Bell Entangled States" [J]. International Journal of Theoretical Physics, **53**(3): 837-840.
[16] Wang Y K, Zhang J, Huang W, et al. (2015) A Quantum Private Comparison Protocol with Splitting Information Carriers[J]. International Journal of Theoretical Physics, **54**(1): 281-291.
[17] G. S. Vernam. (1926) Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications[J]. Transactions of the American Institute of Electrical Engineers, **XLV**(2): 295-301.
[18] Claude E. Shannon. (1984) Communication Theory of Secrecy Systems[J]. Bell System Technical Journal, **28**(4): 656-715.