Simulation detection based on single photon quantum key distribution protocol

X N Liu\textsuperscript{1,3}, C C Hu\textsuperscript{1}, M J Yin\textsuperscript{3} and L Jin\textsuperscript{4}

\textsuperscript{1}School of Information Engineering, Zhengzhou University, Zhengzhou, China
\textsuperscript{2}State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, China
\textsuperscript{3}School of Cyberspace and Security, Information Engineering University, Zhengzhou, China

E-mail: 18437927318@163.com

Abstract. With the continuous development of quantum communication in recent years, quantum key distribution (QKD) has also become a key technology in the field of quantum communication. Due to the limitation of physical resources and experimental conditions, the effectiveness of different communication protocols cannot be accurately analyzed. To solve this problem, a protocol simulation method is proposed, BB84 and B92 protocols are simulated and analyzed on a classic computer by this method. On the Eclipse IDE Developers platform, the simulation program of the quantum communication protocol was written using Java language, the simulation process under the ideal environment and the eavesdropping environment was analyzed with emphasis. The simulation results show that the key distribution efficiency of BB84 is about 50% without eavesdroppers, which is much higher than 25% of B92, and the key distribution efficiency under eavesdropping conditions is about 25% and 18%. The experimental results are consistent with theoretical expectations, verifying the correctness of the protocol simulation, and also proving the feasibility of using computers for quantum communication protocol simulation.

1. Introduction

Information security issues have become more and more complicated with the rapid development of computer technology. The security of classic key distribution protocols mainly depends on solving discrete logarithms and decomposing prime factors of large numbers and other NP problems, such as RSA and El-Gamal, which can be achieved by solving complex mathematical convolution problems. Specifically, the security of the RSA cryptosystem depends on the difficulty of decomposition of large numbers [1], while the security of the El-Gamal cryptosystem depends on the calculation of discrete logarithms in a finite field [2]. In 1994, Peter Shor published a quantum algorithm that can solve factorization and discrete logarithm problems [3-4]. Shor's landmark paper means that if quantum computers appear, the key system under classical encryption algorithms will theoretically be no longer secure. However, with the rapid development of quantum computing and quantum cryptography, the proposed quantum key distribution protocol (QKD), which depends on quantum physical properties, pushes the security of key distribution to a new height.

There are two important aspects in cryptography, namely key distribution and data encryption. For the first aspect, many key agreements based on quantum properties have been proposed at this stage,
among which the more classic key distribution protocols are BB84 [5], B92 [6], and E91 [7] based on quantum entangled states. The BB84 protocol is based on two groups of non-orthogonal quantum states, and the Heisenberg uncertainty principle ensures the security of its key distribution; the B92 protocol can be regarded as a simplification of the BB84 protocol, which discards one in the process of key exchange Group non-orthogonal states, retaining the remaining set of non-orthogonal states of the two-state protocol; the implementation of the E91 protocol is a quantum key protocol based on EPR entangled pairs, and its security is mainly achieved by judging whether it violates the Bell inequality. Compared with the above two single-photon protocols, it is more complicated.

In 2007, Mohsen S. and hooshang an improved part of the execution process of BB84 protocol [8], and proved the validity and reliability of the theory without affecting the security of BB84, and gave the simulation results of the improved BB84. In 2009, Hui Q. and Xiao Ch. used the BB84 protocol as the basic model of QKD in the depolarization channel [9] and used MATLAB to simulate the QKD protocol. The simulation results are basically consistent with the theoretical calculation results. The analysis of the adequacy of the results obtained in this study is too weak. In 2019, Liliana, Z increased the direction of photon polarization in the BB84 protocol [10-11], thereby increasing the amount of information carried on a single photon, to achieve a higher level of security and improve the efficiency of key distribution, the author The correctness of the theory is verified by simulation, but its realization process is extremely complicated and the reliability is not high.

This paper uses Eclipse IDE Developers as the experimental platform on a classic computer, and use the socket network programming based on Java to establish the simulation channel, and simulate the quantum key distribution protocol based on single photon. The simulation results in ideal environment and eavesdropping environment are analyzed, and the efficiency of the two key distribution protocols is compared by QBER detection method.

2. Protocol simulation process analysis

According to the description of single photon quantum key distribution protocol, the communication process mainly depends on two communication channels, namely quantum channel and classical channel. The quantum channel is mainly responsible for the distribution of quantum keys, the classical channel is responsible for key agreement and eavesdropping detection after measurement, and the eavesdropping mainly occurs in the key distribution stage of the quantum channel. The abstract model is shown in Figure 1:

![Quantum communication model](image)

**Figure 1.** Quantum communication model.

2.1. Analysis of coding scheme

The BB84 protocol uses the four polarization states of photons to encode. This protocol uses single photons with four polarization directions: horizontal \( |H\rangle \), vertical \( |V\rangle \), diagonal \( |+\rangle \), and anti-diagonal \( |-\rangle \) to prepare qubits. The 4 photon polarization states form two sets of orthogonal basis, of which \( |H\rangle \) and \( |V\rangle \) polarization states are orthogonal to each other, forming an orthogonal normalized basis vector \( Z \), which is represented by the symbol " + " in the simulation; \( |+\rangle \) and \( |-\rangle \) polarization states are orthogonal to each other, Form another orthogonal basis vector \( X \), which is represented by the symbol " x ". The polarization mode of the two orthogonal bases is shown in Figure 2.
The encoding rules of BB84 protocol quantum state information into classical information are shown in Table 1.

**Table 1. BB84 photon polarization coding scheme.**

| base | Polarization angle | Bit value |
|------|--------------------|-----------|
| +    | 0°                 | 0         |
|      | 90°                | 1         |
| ×    | 45°                | 0         |
|      | 135°               | 1         |

The B92 protocol is a simplification of BB84, which is based on a single-photon quantum key distribution protocol. The main difference from BB84 is that B92 only uses two non-orthogonal polarization states (level $|H\rangle$ and diagonal $|+\rangle$) for binary encoding. The coding scheme is shown in Table 2:

**Table 2. B92 photon polarization coding scheme.**

| base | Polarization angle | Bit value |
|------|--------------------|-----------|
| +    | 0°                 | 0         |
| ×    | 45°                | 1         |

2.2. Simulation process design

According to the execution process of the Alice and Bob protocol, the simulation process distributes the initial key through the following steps:

1. Preparation and distribution of qubits. Alice uses the "random bit generator" and "random sequence generator" in the "quantum preparation" module to generate a set of qubits $S = \{s_1, s_2, s_3, \ldots, s_n\}$ and a set of random measurement bases $S^b = \{s^b_1, s^b_2, s^b_3, \ldots, s^b_n\}$, $s^b_i \in \{+, \times\} i = \{1, 2, 3, \ldots, n\}$ to prepare polarized photons.

2. Bob uses a "random sequence generator" to randomly generate a set of measurement base sequence $M^b = \{m^b_1, m^b_2, m^b_3, \ldots, m^b_n\}$, $m^b_i \in \{+, \times\} i = \{1, 2, 3, \ldots, n\}$ and measure the received polarized photons.

3. Bob sends $M^b$ to Alice through the classic channel. After receiving the random measurement basis sent by Bob, Alice compares it with her random basis $S^b$, and then sends the same common measurement basis to Bob through the classic channel.
(4) After receiving the public measurement base sent by Alice, Bob finds the bits corresponding to the public measurement base, discards the remaining bit information, and sends the bit information corresponding to part of the public measurement base to Alice to detect whether the listener Eve exists. Since B92 is a two-state protocol during the simulation process, step (3) can be omitted from the protocol process. Bob only needs to find the effective photon with the vertical or 135° polarization in the measured photon polarization sequence, retain its bit information, and discard the bit information corresponding to the horizontal and 45° photons.

3. Protocol simulation structure design
The quantum key distribution protocol is a type of security protocol that uses the quantum state of microscopic particles as the carrier to send encryption keys based on the physical characteristics of quantum. This paper mainly uses computer simulation to realize the single-photon quantum key distribution protocol. The simulation structure design mainly includes three aspects: the establishment of the simulation simulation channel, the distribution of the initial key, and the negotiation and detection of the valid key.

3.1. Simulation channel construction
First, it is necessary to establish an analog communication channel between the sender (Alice) and the receiver (Bob). The two parties are based on the TCP protocol under Java Socket programming. In the simulation process, two communication channels are mainly established. The quantum channel is used for key distribution and the classical channel is used for key negotiation. The Socket server communication model based on TCP protocol is built as shown in Figure 3:

![Figure 3. Simulation channel construction based on TCP protocol.](image)

3.2. Simulation program structure design
The single-photon quantum key distribution protocol simulation is realized through the Java integrated environment on the Eclipse platform. The main simulation realizes the distribution process of quantum keys with and without eavesdropping. In the simulation process, the length of the initial key can be arbitrarily adjusted according to the input. A variety of random algorithms are considered in the simulation, which mainly completes the random generation of bits, measurement bases and photon polarization states. The simulation algorithm implementation process of the quantum key distribution protocol is shown in Figure 4.
3.3. Protocol simulation implementation

On the basis of the division and cooperation of various simulation modules, the verification of BB84 and B92 protocols is realized. After the communication is established, Alice can arbitrarily input a positive integer N, where N represents the initial key length generated. The "random sequence generator" will randomly create a sequence of N qubits and generate bases or photons of the corresponding length for Alice to use. Bob also uses N to create its own measurement base sequence, and then performs protocol measurement, verification, and detection operations.

Taking BB84 as an example, the simulations without eavesdropping are as shown in Figure 5:

4. Simulation detection and result analysis

Commonly used eavesdropping detection methods mainly include qubit error rate (QBER) [12] and qubit transmission time (QBTT) [13]. They completed the detection of eavesdroppers from two aspects: bit error rate and transmission delay. This article adopts QBER method to realize the detection of eavesdroppers. QBER is calculated by calculating the bit error rate of the final key obtained after the quantum transmission is completed and after the verification and detection stage.

The qubit error rate is defined as:
QBER = \frac{Q_e - Q_r}{Q_r} \times 100\%

Where \( Q_r \) is the number of all bits received by Bob, and \( Q_e \) is the number of effective bits obtained after check detection.

Since sequence generation and key verification are done randomly during the simulation process, the last valid bit will float up and down in an interval. In order to avoid misjudging this process as an eavesdropping, the key error rate threshold \( \epsilon_0 = 5\% \) is introduced according to the practicality of quantum key distribution during the analysis of the results [14]. If the error rate of the quantum key is \( \text{QBER} > \epsilon_0 \), it is determined that there is eavesdropping in the communication and the communication is abandoned; otherwise, it is considered that the QBER fluctuates in the normal range, and the bit information in the remaining positions will be retained as the initial key.

4.1. Experimental configuration
The experiment equipment in this article is a personal computer, the core processor is Intel(R) Core(TM)i7-9750H @ 2.50GHz, RAM 16GB, graphics processor is NVIDIA GeForce RTX 2060, Windows 10 operating system, development environment is Eclipse IDE for Java and DSL Developers-2020-06

4.2. Analysis of protocol simulation results
The simulation test is carried out in two modes with and without eavesdropping. Use \( N=(64, 128, 256, 512, 2048, 4096) \) to test respectively. In order to minimize the impact of the random function on the test results, each \( N \) value is simulated three times under the same conditions, and the results of the three simulations are calculated and averaged as the effective bits in the final key distribution process. In order to ensure the correct and secure key for subsequent information encryption, error correction and key enhancement are made for the bit information passing the security detection. The symbols and their meanings used in the simulation data analysis process are shown in Table 3:

| Parameter meaning | Initial key length | Public survey base | Valid key | Security key | Bit error rate |
|-------------------|--------------------|--------------------|-----------|--------------|----------------|
| Representation method | \( N \) | \( Q_b \) | \( Q_e \) | \( Q_f \) | \( \text{QBER}_e \) |

The simulation test data of BB84 and B92 under different conditions are as follows: Table 4 and Table 5:

| BB84Simulation | No eavesdroppers | Eavesdropper |
|----------------|-----------------|--------------|
| \( N \) | \( Q_r \) | \( Q_e \) | \( Q_f \) | \( \text{QBER}_e \) (%) | \( Q_r \) | \( Q_e \) | \( Q_f \) | \( \text{QBER}_e \) (%) |
| 64 | 31 | 31 | 29 | 51.7 | 31 | 17 | 73.4 |
| 128 | 65 | 65 | 60 | 49.1 | 63 | 30 | 76.6 |
| 256 | 129 | 129 | 117 | 49.6 | 118 | 56 | 74.6 |
| 512 | 252 | 252 | 234 | 50.8 | 249 | 135 | 73.6 |
| 1024 | 557 | 557 | 509 | 51.0 | 507 | 265 | 74.1 |
| 2048 | 1033 | 1033 | 936 | 49.6 | 990 | 568 | 72.3 |
| 4096 | 2029 | 2029 | 1831 | 50.5 | 2054 | 1044 | 74.5 |

According to the BB84 simulation test data table, when the eavesdropper Eve does not exist, the bit error rate \( \text{QBER}_e \) fluctuates up and down 50% of the theoretical value of BB84 protocol, and the
floating range is less than the bit error rate threshold $\varepsilon_0 = 5\%$. The security detection is passed, and the simulation results are the same as the theoretical expected value of the protocol. When the eavesdropper Eve exists, the bit error rate fluctuates around 75%, which is close to the protocol theoretical value.

According to the B92 simulation test data table, when the eavesdropper Eve does not exist, $QBER$ converges to 75%, and the floating range is less than the bit error rate threshold $\varepsilon_0 = 5\%$, the simulation data is valid, and the simulation result is the same as the theoretical expected value of the protocol. When the eavesdropper Eve exists, the bit error rate converges to 82%, and the floating range is much greater than the $\varepsilon_0$ theoretical bit error rate threshold.

4.3. Results comparative analysis

According to the simulation test data of BB84 and B92, the two protocols are compared vertically, and the efficiency of the two key distribution protocols and the relationship between the initial key length and the final effective key are compared more intuitively. The test data comparison chart is as shown in Figure 6 and Figure 7:

**Figure 6. BB84/B92 effective key length comparison**

**Figure 7. BB84/B92 bit error rate comparison**

It can be seen from the quantization curve in Figure 7 that the effective key length is proportional to the initial key length $N$. Under the condition of the same initial key length and no eavesdropping, the effective key of B92 is much smaller than the BB84 protocol. It can be seen from the convergence curve of Fig. 8 that the bit error rate curves of BB84/B92 all start to converge around 256 initial key lengths. The bit error rates of BB84 and B92 converge to 50% and 75% respectively without eavesdropping, so the key transmission efficiency is 50% and 25% respectively, and the fluctuation is less than threshold $\varepsilon_0 = 5\%$. In the presence of eavesdropping, the error rates of BB84 and B92 converge to 75% and 82%, respectively, and the error rate fluctuations are significantly greater than
the error rate threshold $\varepsilon_0$. Under the same conditions, the key transmission efficiency of BB84 is twice that of B92. Therefore, from the perspective of effective key transmission efficiency, the BB84 protocol is better than the B92 protocol.

5. Conclusion and future works

This paper designs a method of simulating single-photon key distribution on a classic computer. It implements the protocol using two different modes, with/without attack influences, based on a holistic simulation (experimental and real simulator).

Through the simulation data, it is concluded that the key distribution efficiency of the BB84 protocol is twice that of the B92 without eavesdropping, and the relationship curve of Alice/Bob with/without eavesdropper Eve interference in the communication process is given. According to the basic consistency between the quantified curve and theoretical analysis, the correctness of the simulation algorithm design and the effectiveness of simulation are verified. How to design a Domain Specified Language (DSL) through the existing simulation process to describe the quantum key distribution protocol will be the focus of the next step.

6. References

[1] Denning, D. E. (1984). Digital signatures with RSA and other public-key cryptosystems. Communications of the ACM, 27(4), 388-392.
[2] ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory, 31(4), 469-472.
[3] Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review, 41(2), 303-332.
[4] Shor, P. W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science (pp. 124-134). Ieee.
[5] BENNETT, C. (1984). 14, BRASSARD G. Quantum cryptography: Public-key distribution and tossing. In Proceeding of IEEE International Conference on Computers, Systems and Signal Processing: December (pp. 10-12).
[6] Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. Physical review letters, 68(21), 3121.
[7] Ekert, A. K. (1991). Quantum cryptography based on Bell’s theorem. Physical review letters, 67(6), 661.
[8] Sharifi, M., & Azizi, H. (2007). A simulative comparison of bb84 protocol with its improved version. Journal of Computer Science & Technology, 7.
[9] Qiao, H., & Chen, X. Y. (2009). Simulation of BB84 Quantum Key Distribution in depolarizing channel. In Proceedings of 14th Youth Conference on Communication.
[10] Liliana, Z. (2019, July). Two, Three and Four Dimensional BB84: A Comparative Analysis Based on C# Simulation. In 2019 International Conference on Emerging Security Technologies (EST) (pp. 1-5). IEEE.
[11] Zisu, L. (2019). A method to improve the BB84 protocol. Scientific Bulletin" Mirea cel Batran" Naval Academy, 22(1), 1-7.
[12] Treiber, A. (2009). A fully automated quantum cryptography system based on entanglement for optical fibre networks (Doctoral dissertation, uniwien).
[13] Anghel, C. (2011). New Eavesdropper Detection Method in Quantum Cryptograph. The Annals of “Dunarea de Jos “University of Galati. Fascicle III, Electrotechnics, Electronics, Automatic Control, Informatics, 34(1), 1-8.
[14] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. Reviews of modern physics, 81(3), 1301.