Simulation of BB84 Quantum Key Distribution in depolarizing channel

Hui Qiao, Xiao-yu Chen*

College of Information and Electronic Engineering, Zhejiang Gongshang University, Hangzhou, 310018, China
xychen@mail.zjgsu.edu.cn

Abstract: In this paper, we employ the standard BB84 protocol as the basic model of quantum key distribution (QKD) in depolarizing channel. We also give the methods to express the preparation and measurement of quantum states on classical computer and realize the simulation of quantum key distribution. The simulation results are consistent with the theoretical results. It was shown that the simulation of QKD with Matlab is feasible. It provides a new method to demonstrate the QKD protocol.

Keywords: QKD; simulation; depolarizing channel; data reconciliation; privacy amplification

1. Introduction

The purpose of quantum key distribution (QKD) and classical key distribution is consistent, their difference are the realization methods. The classical key distribution is based on the mathematical theory of computational complexity, whereas the QKD based on the fundamental principle of quantum mechanics. The first QKD protocol is BB84 protocol, which was proposed by Bennett and Brassard in 1984 [1].The original BB84 protocol was an ideal model with noiseless channel. In practical QKD, various types of imperfections, for example, imperfect source and channel noise, will cause security loophole, such as PNS attack [2][3].

Bennett, Brassard, Salvail and Smolin firstly experimentally demonstrated the BB84 protocol in 1989[4]. In 1993, Muller, Breguet, and Gisin demonstrated the feasibility of polarization-coding fiber-based QKD over 1.1km telecom fiber[5] and Townsend, Rarity, and Tapster demonstrated the feasibility of phase-coding fiber-based QKD over 10km telecom fiber[6]. Up to now, the security transmission distance of QKD has been achieved over 120km[7].

At present, the study of QKD is limited to theoretical and experimental. The unconditionally secure protocol in theory needs further experimental verification. Because of the limit of technology and some imperfections, the study of QKD in the lab is difficulty and costly. The Gottesman-Knill theorem[8] provides the feasibility of efficiently simulating the QKD protocol on classical computers, thus we can design different algorithms to simulate the protocols.

Table 1: Procedure of BB84 protocol

Alice's photon polarization	↔ ⤢ ↕ ↔ ⤡ ⤢ ↕ ↕ ⤢ ↔ ⤡
Alice's bit sequence	0 0 1 0 1 0 1 1 0 0 1
Bob's basis	+ + × + × × × + × × +
Bob's measured polarization	↔ ↕ ⤡ ↔ ⤡ ⤢ ⤡ ↕ ⤢ ⤢ ↔
Bob's sifted measured polarization	↔ ? ? ↔ ⤡ ⤢ ? ↕ ⤢ ? ?
Alice and Bob's bit sequence	0 0 1 0 1 0
Final key	0 1 1 0

The goal of QKD is to allow distant participants, traditionally called Alice and Bob, to share a long random string of secret in the presence of an eavesdropper, traditionally called Eve[9]. The procedure of BB84 is shown in Table 1.

In this paper, we use Matlab to simulate the procedure of BB84 protocol. The BB84 protocol have been proven to be unconditionally secure [10][11], which based on the quantum complementary and used polarization-coding to realize the QKD. In our simulation algorithm, the source can produce four polarization

[*] Corresponding Author

978-1-935068-01-3 © 2009 SciRes.

photons with equal probability; after completing the preparation of qubits, the photons will through the noisy channel, here, we regard the channel as depolarizing channel[8](also called Pauli channel); then, the qubits with noise will firstly pass a BS(beam splitter), then pass a PBS(polarizing beam splitter), which can separate the mutual orthogonal quantum states; finally the photons will reach the SPD (Single Photon Detector), Bob get the raw key. Because of the bit error in raw key, Alice and Bob have to perform classical post-processing such as error correction and privacy amplification to get the final key.

2. Implementation of Simulation

The simulation model is shown in Fig.1[12], mainly including transmitter, quantum channel and receiver,

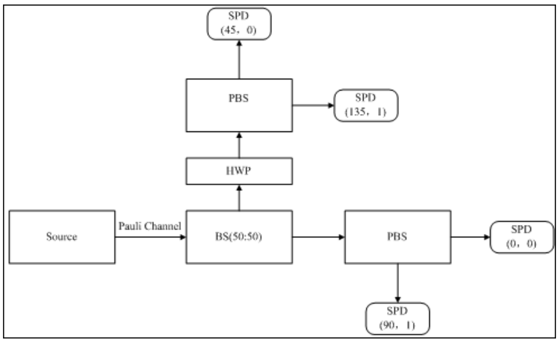

FIG.1: Polarization-coding QKD Communication model. BS: Beam Splitter; PBS: Polarizing Beam Splitter; HWP: Half Wave Plate; SPD: Single Photon Detector.

Compared to the ideal BB84 protocol, our simulation is closer to the actual. The procedure of the simulation of BB84 protocol is as follows:

(a) Alice sends Bob a sequence of photons $S=\{s_1,s_2,s_3,...,s_n\}$, each independently chosen from one of four polarizations—vertical, horizontal, 45-degrees and
135-degrees, where
$s_i \in \{|\leftrightarrow\rangle,|\updownarrow\rangle,|\square\ \rangle,|\square\ \rangle\}(i=1,2,3...,n)$

(b) For each photon, Bob randomly chooses one of two measurement bases{ + , × } to perform a measurement, then Bob broadcasts his bases of measurements.

(c) Alice and Bob discard all events where they use different bases for measurement.

(d) Alice and Bob compute the error rate ξ of the test events, if $\xi \le \xi_0$, they continue to next step, where ξ_0 is the threshold value, Otherwise, they abort.

(e) Alice and Bob convert the polarization data of all remaining data into binary string as follows: mapping a vertical or 45-degrees photon to “0” and a horizontal or 135-degrees photon to “1”.Then they get the raw key.

(f) Alice and Bob perform data reconciliation to correct the error, in this paper, we use the protocol binary.

(g) Alice and Bob perform privacy amplification to generate the final key.

2.1 Quantum source

The original BB84 protocol required a single photon source. However, due to the limitation of technology, perfect single photon source is still far from practical. In the actual experiment, we use the heavy attenuated laser sources as a substitute[13]. But simulation of QKD with Matlab on classical computer does not have this problem. Reference to classical information theory, quantum source can be defined as a quantum ensemble, which can output a particular set of qubits. In practical QKD, the source can not produce photon pulses with four polarization states at a time. In this paper, we construct a model of the source as follows: suppose that the source can randomly produce a set of quantum ensemble $\{|\leftrightarrow\rangle,|\updownarrow\rangle,|\square\ \rangle,|\square\ \rangle\}$ with equal probability. In our simulation algorithm, we use the density matrix to represent the polarization states.

$$\rho_0=\begin{pmatrix}1&0\\0&0\end{pmatrix},\rho_{90}=\begin{pmatrix}0&0\\0&1\end{pmatrix},$$

$$\rho_{45}=\frac{1}{2}\begin{pmatrix}1&1\\1&1\end{pmatrix}\text{and }\rho_{135}=\frac{1}{2}\begin{pmatrix}1&-1\\-1&1\end{pmatrix}$$

represents vertical, horizontal, 45-degrees and
135-degrees respectively.

2.2 Depolarizing channel

The depolarizing channel is one of an important quantum noise. Depolarizing channel can be described as follows[8]: a single-qubit can be depolarized with the probability p and maintain the original state with the probability $1-p$, where p is error probability. Supposed ρ is the original state which Alice produced, after passing the depolarizing channel, the output state is

$$\varepsilon(\rho)=(1-3p)\rho+p(X\rho X+Y\rho Y+Z\rho Z) \tag{1}$$

where

$$X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$

$Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ are Pauli matrix.

According to equation (1), the qubit through the depolarizing channel will become $\rho' = \varepsilon(\rho) = (1-4p)\rho + 2pI_2$, where I_2 is a two-dimensional unit matrix. Now, we can get the output polarization states, where $\tau = 1-4p$,

$$\rho_0' = \frac{1}{2}\begin{pmatrix} 1+\tau & 0 \\ 0 & 1-\tau \end{pmatrix}, \ \rho_{90}' = \frac{1}{2}\begin{pmatrix} 1-\tau & 0 \\ 0 & 1+\tau \end{pmatrix},$$

$$\rho_{45}' = \frac{1}{2}\begin{pmatrix} 1 & \tau \\ \tau & 1 \end{pmatrix}, \ \rho_{135}' = \frac{1}{2}\begin{pmatrix} 1 & -\tau \\ -\tau & 1 \end{pmatrix}.$$

2.3 Measurement

According to the Fig.1, after passing through the depolarizing channel, the polarization state will firstly pass a BS, where the photons can be divided into two-beams. One reached the HV PBS (0-degrees and 90-degrees) and the other reached the AD PBS (45-degrees and 135-degrees). In the process of simulation, we treat HWP and PBS as a whole to detect the photons of 45-degrees and 135-degrees. As shown in Fig.1, after passing the PBS, two mutually orthogonal states arrive at SPD respectively. In this paper, the SPD is Avalanche Photon Diode (APD), which can detect the polarization photons following the decoding rules.

In this paper, we use a pseudo-random sequence to simulate the BS, which determines reflection and transmission. Furthermore, in simulation algorithm, we treat PBS and SPD as a whole. Suppose after BS's reflection, the photons get into the PBS with HV basis, we measure it with vertical basis and calculate its trace. If $Tr[\rho'\rho_0] = 1/2$, the polarization direction of this photon is 45-degrees or 135-degrees, so abort; next, we will judge this photon is vertical or horizontal. According to our analysis, if $Tr[\rho'\rho_0] = \frac{1+\tau}{2} > 1/2$, the polarization direction of this photon is 0-degrees, in this case, the probability of the PBS wrongly judged it as 90-degrees is $\frac{1-\tau}{2}$, this part is bit error. In our simulation algorithm, the probability of the PBS treated it as 0-degrees photon is $\frac{1+\tau}{2}$; on the other hand, treated it as 90-degrees, and recorded the bit error.

We do a similar operation to deal with the photons of 45-degrees and 135-degrees, then, we get the raw key. The length of Bob's raw key is about half of Alice's, this bit sequence is obtained by Alice and Bob sifted the wrong measured basis they used. There are bit errors in the raw key, so we should perform data reconciliation and privacy amplification to generate a final key.

2.4 Data reconciliation

Alice converts the binary string into qubit and sends the polarization states to Bob through the quantum channel, Bob measures the received polarizations and converts them into binary string. They sift measured polarization by the classical channel and get the raw key, if the error bit rate is larger than the threshold, they abort. Even if the communication is effective, they also can not use the raw key directly, because that the error bit rate is still large. They have to perform error correction and privacy amplification[14].

The process which performs error correction in the public channel is known as data reconciliation[12]. The requirements of data reconciliation are as follows:

(a) Reduce the bit error rate to be appropriate for use, for example, less than 10^{-9} ;

(b) Reduce the information Eve obtained in this process as far as possible;

(c) Remain the useful data as many as possible;

(d) Faster and save resources as far as possible.

In this paper, we use protocol binary[12] to correct error. This method is simple and practical, but it can not correct the error with even numbers. We improved the protocol, increased error correction capacity. The detailed steps are as follows:

(a) Alice and Bob rearrange their sequence with the same random sequence. The purpose is to make the error uniformly distributed.

(b) Group the data into small packets, the length of each packet is 11;

(c) Alice and Bob detect the parity of each packet data respectively and compare the results through the public channel. If they have different results, it indicates that this packet has odd error bits, we divide this packet into two groups, detect the parity again, if they have different results, abort this group; on the contrary, abort the last bit of this group. Furthermore, calculate the bit error rate q_1 of the first round;

(d) After the first round error correction, bit errors may still exist, we rearrange the bit sequence with the same random sequence again and group the data into packets, the length of each packet in this step is k, where $k \approx 1/3q_1$. Repeat the step (c). If $q_1 > 0.00001$, repeat this step until the bit error rate is much lower, such as $q_1 < 0.00001$.

2.5 Privacy amplification

The concept of privacy amplification was first proposed by Bennett, Brassard and Robert[15]. Privacy amplification is a method of extracting a secret key from a string which is partially-known to an eavesdropper. This method is at the cost of reducing the information which legitimate users obtained to improve the security of the data in public channel. The concept of privacy amplification is proposed with the need of quantum cryptography, now, it has become an important research topic in the classical secure communication.

We will discuss the privacy amplification in our simulation algorithm. We suppose that Alice and Bob have l bits after error correction, they estimate Eve knows t bits, choose s as security parameters. We use Hash function F,

$f \in F$, $F:\{0,1\}^l \to \{0,1\}^r, r = l - t - s$. After data reconciliation, the mutual information $I(A,B)$ will reduce from l to r, the mutual information $I(E,A)$ will reduce from t to less than $2^{-s}/\ln 2 \approx 1.443 \times 2^{-s}$ [12], where r is the length of final key, in this paper, the value of t is chosen in a reasonable range, e.g., from 0 to 5. Furthermore, we set $s = 30$ [16].

In the algorithm of our simulation, the Hash function we used is a $l \times r$ matrix only containing 0 and 1. We apply the mod-2 operation to the l bits sequence and the $l \times r$ matrix. Finally, we can get the final key with unconditional security.

3. Simulation results and Discussions

Simulation results are crucial for verifying the simulation experiment. Here we explain the principle of our simulation and give the results.

In this paper, we performed the simulation based on the BB84 protocol. The noise channel is such that its private classical capacity is equal to the maximal achievable key rate in BB84 with quantum bit error rate q. The coherent information of the channel provides an upper bound on the bit rate of BB84 protocol.

The coherent information of BB84 channel can be evaluated, giving the following upper bound [17],

$$C_p(N_q^{BB84}) \le H(\frac{1}{2} - 2q(1-q)) - H(2q(1-q)) \quad (2)$$

Smith calculated the upper bound of the bit rate according to lemma (2). When $q = 0.15$, the channel capacity is 0, that is, the bit rate has reduced to 0 when $q \le 0.15$. The bit rate we obtained is less than the upper bound.

Mayers has proved that a secure bit rate is $1 - H(2q) - H(q)$, then, Mayers, Shor and Preskill pointed the possibility of the secure bit rate $1 - 2H(q)$ [18]. We also calculate it.

In the above formulas, $H(x)$ is the binary entropy $-x\log_2 x - (1-x)\log_2(1-x)$ .The bit rate is $R = r/m$, where r is the length of final key, m is the length of raw key.

In this paper, our goal is to calculate the bit rate of BB84 protocol with our simulation experiment. In principle, whatever possible results can be obtained in the simulation process.

We have done a number of experiments to simulate the communication between Alice and Bob with Matlab. In our simulation, Alice sends 10000 photons to Bob each time, error probability p between 0 and 0.15. We calculated the bit error rate and bit rate, and compared

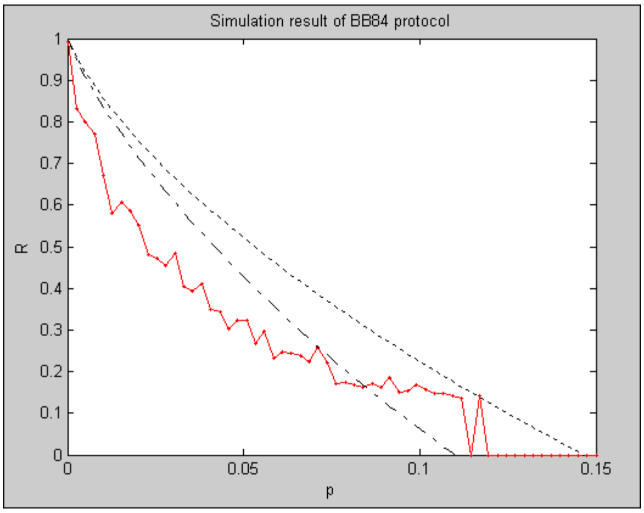

Figure.2: Simulation result of BB84 protocol.
The horizontal axis is the error probability, and the vertical axis is the bit rate. The dashed line is the upper bound of the bit rate. The dot-dashed line is the result of Hayashi. The red line is our result.

them with the previous theoretical results, the simulation results we obtained are correct. The simulation result is shown in Figure.2:

As shown in Figure.2, there are statistical fluctuations. The main reason is that we use random numbers in simulation process. In an ideal QKD, the BS can split a photon with equal probability. Nevertheless, we use a pseudo-random number in simulating the BS. Moreover, we also use pseudo-random numbers in simulating the source and SPD. All of these imperfect factors will cause the fluctuations. However, the perfect random number is unnecessary for secure QKD [19].

4. Conclusion

We have designed the simulation algorithm of polarization-coding QKD on classical computer and realized the classical simulation of BB84 protocol with Matlab. In this paper, we construct the channel as depolarizing channel and simulate the optical components, such as source, BS, PBS and SPD. Finally, we calculate bit rate and draw its curve, the simulation results we obtained are proved to be correct. Simulation of QKD on classical computer is an important method to verify the QKD protocol. Moreover, it also provides a new direction to research the quantum cryptography. It has been shown that simulation of QKD with Matlab can work even with the fluctuations.

References

[1] C.H.Bennett and G.Brassard, ”*Quantum cryptography:Public key distribution and coin tossing*,” [C] Proceedings of IEEE International Conference on Computers,Systems and Signal Processing,Bangalore,India,pp.175-179,1984.

[2] B.Huttner, N.Imoto, N.Gisin and T.Mor, [J] Phys. Rev A51,1863(1995);

[3] G.Brassard, N.Lütkenhaus, T.Mor, and B.C.Sanders, [J] Phys.Rev.Lett.85,1330(2000).

[4] C.H.Bennett, F.Bessette, G.Brassard, L.Salvail ,and J.Smolin,J.of Cryptography **5**,3 (1992).

[5] A.Muller, J.Breguet, and N.Gisin, Europhys.Lett.**23**,383 (1993).

[6] P.D.Townsend, J.G.Rarity, and P.R.Tapster, [J] Electron. Lett.**29**,634 (1993).

[7] C.Gobby, Z.L. Yuan, A.J. Shields, [J] *Appl. Phys*.Lett.**84** 3762(2004).

[8] Michael A.Nielsen, Isaac L.Chuang *Quantum Computation and Quantum Information*,[M] Cambridge University Press 2000.

[9] Hoi-Kwong Lo and Yi Zhao *Quantum Cryptography*, ArXiv: quant-ph/0803.2507v4

[10] D.Mayer, J.Assoc. Comput . Mach. **48,**351 (2001). Its preliminary version appeared in “Advances in Aryptology-Proc. Crypto” 96, Vol.1109 of Lecture Notes in Computer Science, Ed. N. Koblitz, Springer-verlag, New York,1996,p.343.

[11] P.W.Shor and J.Preskill, [J] Phys Rev.Lett.85,441(2000)

[12] Rui-lin Ma *Quantum Cryptography Communication* (in Chinese) [M]. Science Press.2006

[13] Q.D. Xuan, R. ALLéaume, L.Xiao, F.Treussart, B. Journet, and J.-F. Roch. *Intensity noise measurement of strongly attenuated laser diode pulses in the time domain*. [J] Eur. Phys. J. Appl. Phys., 35:117,2006.

[14] A. R. Calderbank and P. W. Shor. *Good quantum error-correcting codes exist*. [J] Phys. Rev. A, 54:1098-1105, 1996

[15] C.H.Bennett, G.Brassard, C.Crepeau and U.M.Maurer *Generalized privacy amplification* IEEE Trans Information Theory,1995,**41(6)**;1915-1923

[16] G.Gilbert, M.Hamrick and F.J.Thayer *Privacy Amplification in Quantum Key Distribution:Pointwise Bound versus Average Bound*, ArXiv :quant-ph/0108013v1

[17] G.Smith and J.A.Smolin *Additive extensions of a quantum channel*, ArXiv:quant-ph/0712.2417v1

[18] M.Hayashi *Practical Evaluation of Security for Quantum Key Distribution* [J] Phys. Rev. A, **74**,022307 (2006)

[19] Xiangbin Wang *Perfect random number generator is unnecessary for secure quantum key distribution*, ArXiv:quantum-ph/0405182v2

978-1-935068-01-3 © 2009 SciRes.