Simulating BB84 Protocol in Dephasing Qubit Channel

Xiao-yu Chen

Zhejiang Gongshang University, Hangzhou 310013, China
xychen@zjsu.edu.cn

Abstract. BB84 protocol of quantum key distribution had been proved to be absolutely secure. We simulate the rate of secure key distribution in dephasing channel on a classical computer with the method of event-by-event simulation. Theoretically, the private classical capacity of dephasing channel can be obtained in principle, since the channel is degradable. We give the formula of capacity with respect to the dephasing coefficient. The simulation meets the theory well.

Keywords: Dephasing channel, quantum capacity, BB84 protocol, degradable.

1 Introduction

Quantum communications on fiber or free space come into a reality today. The rate of transmitting quantum information faithfully down noisy channel is upper bounded by the quantum capacity of the channel. Quantum capacity is closely related to the private classical capacity in quantum cryptograph. For a given protocol such as BB84, non-ideal factors such as the control precision in communication process, noise in the transmission and dark counting at the receiving end can be modelled as the effects of a channel.

Unfortunately, quantum capacity exhibits a kind of nonadditivity that makes it extremely hard to deal with [1]. The quantum capacity of the most common quantum channel, the depolarizing channel, is not obtained yet. It requires a regulation process of the maximization of the coherent information that can hopelessly be solved with brute force. It has been proved that once the channel is degradable, single letter formula of the quantum capacity is available [2]. Thus for some special classes of channels, quantum capacity can be obtained analytically or numerically. Moreover, quantum capacity is equal to the private classical capacity for degradable channel [3]. The first example with calculable quantum capacity is quantum erasure channel[4]. Other examples are dephasing qubit channel[2], amplitude damping qubit channel[5], and continuous variable lossy channel[6], where the channels are either degradable or anti-degradable[7].

To provide a guideline for experimenters with the communication rate of faithfully transmitting of quantum information, one need the quantum capacity theory. One one side, quantum capacity usually can not be calculated exactly. One

A. Sergienko, S. Pascazio, and P. Villoresi (Eds.): QuantumCom 2009, LNICST 36, pp. 242–248, 2010.

the other hand, practical quantum optical communication systems are costly and systematical experimental data is not available. To fill the gap between the theory and the experiment, there is the method of classical computer simulation.

We in this paper will present event by event simulation of BB84 protocol in dephasing qubit channel. The reasons to simulate such a system are: (i) phase decoherence is one of the main obstacles in quantum information transmission, it is stronger than amplitude decay for many systems, the decay time of dephasing is 10-100 times shorter than the decay time of amplitude damping[8], (ii) protocols such as BB84 neglect the missing photons in the late treatment, so there is no need to treat amplitude damping separately, (iii) quantum capacity formula can be analytically worked out for dephasing qubit channel, providing a clear upper bound to the faithfully quantum information transmitting rate. (iv)BB84 protocol is well studied and widely used one. Its security has been proved [9]. Thus the properties of the simulation can be verified with theoretical and experimental results. The parameters such as length of the date package can be determined for the simulation.

2 Quanutm Capacity of Qubit Phase Damping Channel

Quantum capacity is one of the main issues in quantum information theory. It is concerned with the transmission ability of unknown quantum state on a given quantum channel. The critical quantity involved in the quantum capacity is the coherent information (CI) $I_c(\sigma, \mathcal{E}) = S(\mathcal{E}(\sigma)) - S(\sigma^{QR'})$ [10] [11]. Here $S(\varrho) = -\mathrm{Tr}\varrho \log_2 \varrho$ is the von Neumann entropy, σ is the input state, the application of the channel $\mathcal{E}$ results the output state $\mathcal{E}(\sigma)$; $\sigma^{QR'} = (\mathcal{E} \otimes \mathbf{I})(|\psi\rangle \langle\psi|)$, with R referred to the 'reference' system[10] (the system under process is Q system with annihilation and creation operators a and $a^\dagger$, we denote σ^Q as σ for simplicity), $|\psi\rangle$ is the purification of σ. The quantum channel capacity is[12][13][14]

$$Q = \lim_{n\to\infty} \sup_{\sigma_n} \frac{1}{n} I_c(\sigma_n, \mathcal{E}^{\otimes n}). \tag{1}$$

Since phase damping channel (or dephasing channel) is degradable, the quantum capacity can be expressed with single letter formula,

$$Q = \sup_{\sigma} I_c(\sigma, \mathcal{E}_p), \tag{2}$$

where $\mathcal{E}_p$ refers to the superoperator of phase damping channel.

In the computational basis $|0\rangle, |1\rangle$ of the Hilbert space $\mathcal{H}_Q$, the most general qubit state input can be parameterized as follows

$$\rho = \begin{bmatrix} 1-p, & \alpha^* \\ \alpha, & p \end{bmatrix}, \tag{3}$$

where $p \in [0,1]$ is the probability associated with the state $|1\rangle$ and $|\alpha| = \sqrt{p(1-p)}$ is a coherent term. The purification of ρ can be the state

$$|\Psi\rangle = \sqrt{1-p}\,|0\rangle \otimes |R_0\rangle + \sqrt{p}\,|1\rangle \otimes |R_1\rangle\,, \tag{4}$$

where the 'reference' qubit system $\mathcal{H}_R$ is introduced, and $|R_0\rangle, |R_1\rangle$ are the unit vectors of $\mathcal{H}_R$. Since $\rho = Tr_R |\Psi\rangle\langle\Psi| = \sqrt{1-p}\,|0\rangle\langle 0| + \sqrt{p(1-p)}(\langle R_1 | R_0\rangle |0\rangle\langle 1| + \langle R_0 | R_1\rangle |1\rangle\langle 0|) + \sqrt{p}\,|1\rangle\langle 1|$, we should put

$$\langle R_0 | R_1\rangle = \frac{\alpha}{\sqrt{p(1-p)}}. \tag{5}$$

The channel output state of a phase damping channel is

$$\mathcal{E}_p(\rho) = \begin{bmatrix} 1-p, & \gamma\alpha^* \\ \gamma\alpha, & p \end{bmatrix}, \tag{6}$$

where the coefficient $\gamma \in [0,1]$ characterizes the phase damping channel. The eigenvalues of the output state $\mathcal{E}_p(\rho)$ is

$$\lambda_{1,2} = \frac{1}{2}[1 \pm \sqrt{1 - 4(p(1-p) - |\alpha|^2\gamma^2)}], \tag{7}$$

The joint output state $\rho^{QR'} = \mathcal{E}_p \otimes I_R(|\Psi\rangle\langle\Psi|)$ can be expressed in the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ of $\mathcal{H}_Q \otimes \mathcal{H}_R$, with

$$|R_0\rangle = |0\rangle_R, \tag{8}$$

$$|R_1\rangle = \frac{\alpha}{\sqrt{p(1-p)}}|0\rangle_R + \sqrt{1 - \frac{|\alpha|^2}{p(1-p)}}\,|1\rangle_R. \tag{9}$$

Thus

$$\rho^{QR'} = \begin{bmatrix} 1-p, & 0, \gamma\alpha^*, & \gamma\sqrt{p(1-p)-|\alpha|^2} \\ 0, & 0, 0, & 0 \\ \gamma\alpha, & 0, \frac{|\alpha|^2}{(1-p)}, & \alpha\frac{\sqrt{p(1-p)-|\alpha|^2}}{1-p} \\ \gamma\sqrt{p(1-p)-|\alpha|^2}, & 0, \alpha^*\frac{\sqrt{p(1-p)-|\alpha|^2}}{1-p}, & p - \frac{|\alpha|^2}{(1-p)} \end{bmatrix}. \tag{10}$$

Although $\rho^{QR'}$ is a matrix function of the coherent term $|\alpha|$, the eigenvalues of $\rho^{QR'}$ do not rely on $|\alpha|$. Two of the eigenvalues are

$$\Lambda_{1,2} = \frac{1}{2}[1 \pm \sqrt{1 - 4p(1-p)(1-\gamma^2)}],$$

the other two eigenvalues $\Lambda_{1,2}$ are 0. The von Neumann entropy of the output state is

$$S(\mathcal{E}_p(\rho)) = H_2(\lambda_1), \tag{11}$$

where $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function. The maximum of $H_2(\lambda_1)$ should be achieved when $\lambda_1 = \frac{1}{2}$, that is, $|\alpha| = 0$, $p = \frac{1}{2}$. Thus, the maximization conditions of entropy of the output state $S(\mathcal{E}_p(\rho))$ are $|\alpha| = 0, p = \frac{1}{2}$. Meanwhile, the entropy of the joint output state is

$$S(\rho^{QR'}) = H_2(\Lambda_1), \tag{12}$$

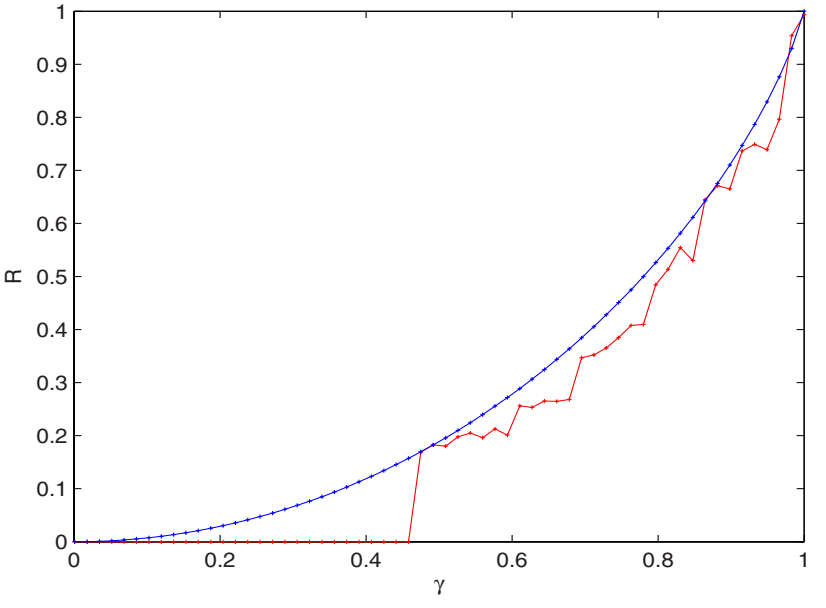

Fig. 1. The comparison of simulation result with quantum capacity, γ is the dephasing coefficient, R is the secure key transmission rate

it is an decreasing function of Λ_1 for $\Lambda_1 \geq \frac{1}{2}$. The minimum should be achieved with maximal Λ_1, which is only possible when $p = \frac{1}{2}$,regardless of the off-diagonal element α of the input state. Hence the coherent information $I_c(\rho, \mathcal{E}_p) = S(\mathcal{E}_p(\rho)) - S(\rho^{QR'})$ achieves its maximum at $|\alpha| = 0$, $p = \frac{1}{2}$. The maximum of I_c is just the quantum capacity since the channel is degradable. We have the quantum capacity

$$Q = 1 - H_2(\frac{1}{2}(1+\gamma)). \tag{13}$$

For a degradable channel, it has been proved that private classical capacity is equal to quantum capacity[3]. The depasing channel is degradable, thus the private classical capacity of the dephasing channel is

$$C_p = Q = 1 - H_2(\frac{1}{2}(1+\gamma)). \tag{14}$$

the achievable private information transmission rate R is upper bounded by private classical capacity C_p. The theoretical private classical capacity formula (14) is shown in Figure 1 as the smooth curve.

3 Simulation with Classical Computer

The standard BB84 protocol use polarized quantum state ensemble $\{|-\rangle, ||\rangle, |\diagup\rangle, |\diagdown\rangle\}$ as the source. The polarizations are horizontal (0°), vertical (90°), diag-

onal up (45°), diagonal down (135°), respectively. Denote $|\psi_0\rangle = |-\rangle, |\psi_1\rangle = ||\rangle, |\psi_2\rangle = |/\rangle, |\psi_3\rangle = |\backslash\rangle$, we have $|\psi_{2,3}\rangle = \frac{1}{\sqrt{2}}(|\psi_0\rangle \pm |\psi_1\rangle$. In the basis of $\{|\psi_0\rangle, |\psi_1\rangle\}$, the density matrices of the four states are

$$\rho_0 = \begin{bmatrix} 1\,0 \\ 0\,0 \end{bmatrix}, \rho_1 = \begin{bmatrix} 0\,0 \\ 0\,1 \end{bmatrix}, \rho_2 = \frac{1}{2}\begin{bmatrix} 1\,1 \\ 1\,1 \end{bmatrix}, \rho_3 = \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1\,1 \end{bmatrix}. \tag{15}$$

The output density matrices are

$$\rho_0' = \begin{bmatrix} 1\,0 \\ 0\,0 \end{bmatrix}, \rho_1' = \begin{bmatrix} 0\,0 \\ 0\,1 \end{bmatrix}, \rho_2' = \frac{1}{2}\begin{bmatrix} 1\,\gamma \\ \gamma\,1 \end{bmatrix}, \rho_3' = \frac{1}{2}\begin{bmatrix} 1 & -\gamma \\ -\gamma\,1 \end{bmatrix}. \tag{16}$$

Thus if horizontal and vertical basis is chosen to convey classical bit in BB84 protocol, the dephasing channel takes no effect to the bit, and if diagonal (up and down) basis is chosen, the dephasing channel does affect the bit transmitted. At the sending end, Alice randomly chooses the horizontal and vertical basis or diagonal basis. Alice converts the binary string into qubit and sends the polarization states to Bob through the quantum channel. At the receiving end, Bob measures the received polarizations and converts them into binary string. They sift measured polarization by declaring the basis chosen with public classical channel and get the raw key, if the error bit rate is larger than a threshold, they abort. Even if the communication is effective, they can not use the raw key directly, the bit error rate is still very large. They have to perform error correction and privacy amplification.

In the simulation, random numbers are needed at the sending process and at the measurement in order to choose the horizontal and vertical basis or diagonal basis.

3.1 Data Reconciliation

The process which performs error correction in the public channel is known as data reconciliation. The requirements of data reconciliation are as follows: (a) to reduce the bit error rate to an appropriate value for use. (b) to reduce the information Eve obtained in this process as far as possible; (c) to maintain the useful data as many as possible; (d) to be fast and to save resources as far as possible.

In this paper, we will use bipartition protocol to correct errors. The method is simple and practical, although it can not correct errors with even number bit flips. We improved the original protocol, increased the error correction capability. The detailed steps are as follows: (a) Alice and Bob rearrange their sequence according to the same random sequence. The purpose is to make the errors uniformly distributed. (b) The data is divided into small packets, with the length of each packet being 11 bits (according to our empirical data); (c) Alice and Bob detect the parity of each packet data respectively and compare the results through some public channel. If they have different results, it is to say that the packet has odd error bits. We divide this packet into two further groups, detect the parity once more. If Alice and Bob have different results, they abort this

group; On the contrary, they abort the last bit of this group. Furthermore, they 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 some other random sequence which is the same to Alice and Bob and divide the data into packets, the length of each packet in this step is $k \approx 1/(3q_1)$. Repeat the step (c). If $q_1 > 10^{-5}$, repeat this step until the bit error rate is much lower, such that $.q_1 < 10^{-5}$.

3.2 Privacy Amplification

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.

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 $2^{-s}/\ln 2 \approx 1.443 \times 2^{-s}$, where r is the length of the final key. In this paper, the value of t is chosen in a reasonable range, e.g., from 0 to 5. Furthermore, we set $s = 30$.

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 Hash matrix. Finally, we can get the final key with unconditional security.

4 Conclusions

We simulate BB84 protocol of quantum key distribution in dephasing channel with classical computer. With properly chosen of the length of the first round package in the data reconciliation and the precision of leaked information to the environment, we calculation the yield of the protocol. The transmission rate with respect to the dephasing coefficient is given. Theoretically, the private classical capacity of the channel is also deduced and shown in the figure as a comparison. We can see that the simulation are quite in agreement with theory except in the severe depasing end.

References

1. DiVincenzo, D.P., Shor, P.W., Smolin, J.A.: Phys.Rev. A 57, 830 (1998)
2. Devetak, I., Shor, P.W.: Comm. Math. Phys. 256, 287 (2005)
3. Simth, G.: Phys. Rev. A 78, 022306 (2008)
4. Bennett, C.H., Divincenzo, D.P., Smolin, J.A.: Phys. Rev. Lett. 78, 3217 (1997)
5. Giovannetti, V., Fazio, R.: Phys. Rev. A 71, 032314 (2005)
6. Wolf, M.M., Perez-Garcia, D., Giedke, G.: Phys. Rev. Lett. 98, 130501 (2007)

7. Caruso, F., Giovannetti, V.: Phys. Rev. A 74, 062307 (2006)
8. Ioffe, L., Marc Mzard, M.: Phys. Rev. A 75, 032345 (2007)
9. Shor, P.W., Preskill, J.: Phys. Rev. Lett. 85, 441 (2000); PRL85 (2000)
10. Schumacher, B.: Phys. Rev. A 54, 2614 (1996); Schumacher, B., Nielsen, M.A.: Phys. Rev. A 54, 2629 (1996)
11. Lloyd, S.: Phys. Rev. A 55, 1613 (1997)
12. Devetak, I.: IEEE Trans. inf. Theory 51, 44 (2005); Devetak, I., Winter, A.: Proc. R. Soc. Lond. A 461, 207 (2005)
13. Barnum, H., Knill, M., Nielsen, M.A.: IEEE Trans. Inf. Theory 46, 1317 (2000)
14. Horodecki, M., Horodecki, P., Horodecki, R.: Phys. Rev. Lett. 85, 433 (2000)