International Journal of Quantum Information
Vol. 6, No. 6 (2008) 1195–1202

World Scientific
www.worldscientific.com

QUANTUM KEY DISTRIBUTION WITH CLASSICAL ALICE

HUA LU*,†,‡,§ and QING-YU CAI†

*Department of Mathematics and Physics,
Hubei University of Technology, Wuhan 430068, China

†State Key Laboratory of Magnetic Resonance and
Atomic and Molecular Physics,
Wuhan Institute of Physics and Mathematics,
The Chinese Academy of Science, Wuhan 430071, China

‡Graduate School of the Chinese Academy of Sciences,
Beijing 100049, China
§luhua@wipm.ac.cn

Received 15 September 2008

It seems that quantum key distribution (QKD) may be completely insecure when the message sender Alice always encodes her key bits in a fixed basis. In this paper, we present a QKD protocol with classical Alice, i.e. Alice always encodes her key bit in the $\{|0\rangle, |1\rangle\}$ basis (we call it classical {0,1} basis) and the eavesdropper Eve knows this fact. We prove that our protocol is completely robust against any eavesdropping attack and present the amount of tolerable noise against Eve's individual attack. Next, we present a QKD protocol to demonstrate that secure key bits can be distributed even if neither Alice nor Bob has quantum capacities, and extend this idea to a QKD network protocol with numerous parties who have only classical capacities. Finally, we discuss that quantum is necessary in QKD for security reasons, but both Alice and Bob may be classical.

Keywords: Quantum communication; classical Alice.

PACS Number(s): 03.67.Hk, 03.67.-a

1. Introduction

Quantum cryptography, or more precisely called quantum key distribution (QKD), provides perfect security based on the principles of physics. In QKD, two remote parties, Alice and Bob, can distribute secret key bits with a quantum channel and a reliable classical channel. In the well-known BB84 as well as some other suggested protocols, both Alice and Bob perform quantum operations on their qubits to encode and decode secret key bits. In the traditional QKD protocols, both Alice and Bob are quantum since their operations are noncommutative, so that the quantum uncertainty principle will protect their communication against Eve's eavesdropping. Recently, Boyer *et al.* presented a novel QKD protocol with

classical Bob,[1] in short BKM07, in which Bob has only classical capacities. They proved that their protocol is completely robust against any eavesdropping attack: Eve's any eavesdropping attack will result in a nonzero probability of being caught. So, it is interesting to know whether QKD is secure when Alice is classical, i.e. Alice always encodes her key bits in a fixed basis? Furthermore, we may ask whether QKD is still secure when neither Alice nor Bob has quantum capacities? At first glance, the answer may be negative since Eve knows that Alice only encodes her key bits in a fixed basis.

In this paper, we present a novel QKD protocol with classical Alice. In our protocol, Alice has only classical capacities and always encodes her key bits in the $Z = \{|0\rangle, |1\rangle\}$ basis and Eve knows this fact. We prove our protocol is robust and calculate the secure information of Alice and Bob's INFO key bits to generate the final key against Eve's individual attack. Our calculation shows that the security of the final key bits is determined by two independent parameters which can be verified experimentally by Alice and Bob. We then present a QKD protocol in which neither Alice nor Bob has quantum capacity and prove its security. Next, we extend this idea to a QKD network with numerous classical parties.

This paper is organized as follow: we first present our QKD protocol with classical Alice and prove its security. We calculate the secure information of Alice and Bob's INFO key bits against Eve's individual attack. We then present a QKD protocol in which both Alice and Bob are classical and extend it to a QKD network protocol with numerous parties. Finally, we discuss whether quantum and quantum capacities are necessary or not in QKD.

2. QKD with Classical Alice

Let us assume that Bob holds a round-trip quantum channel which leads from Bob's lab to the outside world and back to Bob's lab. Bob always prepares his qubit in $X = \{|+\rangle, |-\rangle\}$ basis and sends it out through his quantum channel, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Alice can access a segment of Bob's quantum channel. When a qubit passes through that segment, Alice can either let it go undisturbed or measure it in classical {0,1} basis and prepare a fresh one in classical {0,1} basis and send it. When Bob received the travel back qubit, he measures it in Z basis or X basis randomly. Bob announces which basis he used and Alice announces whether she measured the travel qubit or not. In the case that Alice refreshed the travel qubit and Bob also measured it in Z basis, they share a common bit as SIFT bits. In the case that Alice refreshed the travel qubit but Bob measured it in X basis, they discard their results this time. When Alice let the qubit go directly but Bob measured it in Z basis, Alice and Bob discard their results, too. If Alice did not disturb the travel qubit and Bob measured it in X basis, Bob keeps the measurement results as CTRL bits. After all of Bob's qubits distributed, Bob publishes some of his measurement results to verify QBER in SIFT. If both the QBER in SIFT and QBER in CTRL are tolerable, Alice and Bob will use the rest

bits in SIFT as INFO bits to generate final key bits. In our protocol, it is clear that all of Alice's operations are performed in the fixed classical {0,1} basis so that we define Alice to be classical.[1]

Let n be the desired key bit string. Our protocol can be explicitly described with a program below:

(a0) $N = 8n(1 + \delta)$, where the positive δ is some fixed parameters.
(a1) Bob generates qubits in X basis and records its state. Then he sends it out through his quantum channel.
(a2) Alice accesses Bob's qubit.
(a3) With probability c, Alice lets it go without any disturbance. With probability $1 - c$, Alice refreshes the travel qubit and sends it back to Bob.
(a4) Bob measures the travel back qubit in Z basis or X basis randomly, and he then publishes which basis he used.
(a5) If Bob measured the travel qubit in Z basis and Alice refreshed it, then goto (b0). If Bob measured the qubit in X basis and Alice let it go undisturbed, then goto (b1). If Bob measured the qubit in Z basis and Alice did not disturb it, then goto (b2). If Bob measured the qubit in X basis and Alice refreshed it, then goto (b2).
  (b0) Alice and Bob use their results as SIFT bits. goto (c0)
  (b1) Bob uses his measurement results as CTRL bits. goto (c0)
  (b2) Alice and Bob discard their results this time. Continue.
  (c0) $N = N - 1$. If $N > 0$, then goto (a1). Or else, continue.
  (c1) Bob publishes some of his measurement results in (b0) to verify QBER in SIFT. The rest bits in SIFT are INFO bits.
  (c2) Bob verifies QBER in CTRL with his measurement results in (b1).
  (d0) If QBERs in SIFT and CTRL are tolerable, Alice and Bob can use INFO bits to generate final key bits after error-correction (EC) and privacy amplification (PA).[2]

3. Security Against Individual Attack

In the above protocol, the travel qubit will travel from Bob to Alice and then from Alice to Bob. Eve can first attack the travel qubit in the line Bob to Alice, in short B to A, and then attack on it in the line A to B. First of all, We will prove Eve's attack in line B to A is useless for her to eavesdrop on the communication.

Let us suppose that Eve attacks the travel qubit in the line B to A first. Since Bob always prepares his qubit in the X basis, Eve can perform a CNOT operation to map the state of the travel qubit into her ancilla

$$U_{\text{CNOT}}\,(|+\rangle|0\rangle_E) = |+\rangle|0\rangle_E,$$
$$U_{\text{CNOT}}\,(|-\rangle|0\rangle_E) = |-\rangle|1\rangle_E.$$

Suppose Alice lets the travel qubit go undisturbed this time. Eve can measure her ancilla after Bob measured the travel qubit, so that she can obtain the full

information about this qubit without disturbing it. However, this is unhelpful for Eve to gain information about Alice's key bit this time. On the other hand, if Alice refreshed the travel qubit this time, she will prepare another qubit in the classical {0,1} basis to encode her key bit so that Eve's attack in the line B to A is useless now. In consequence, Eve's attack in the line B to A is useless. Eve's effective strategy is that she attacks the travel qubit in the line A to B.

Eve's most general attack operations in line A to B can be described by a unitary operation together with an ancilla. Eve can map the states of the travel qubit into her ancilla (her quantum memory) first. After Bob published his measurement bases, Eve then measures her ancilla to gain information about Alice's key bits. Eve's operation may be written as

$$U|0\rangle|0\rangle_E = \sqrt{f_0}|0\rangle|0_0\rangle_E + \sqrt{1-f_0}|1\rangle|1_0\rangle_E, \tag{1}$$

$$U|1\rangle|0\rangle_E = \sqrt{f_1}|1\rangle|0_1\rangle_E + \sqrt{1-f_1}|0\rangle|1_1\rangle_E, \tag{2}$$

where f_0 and f_1 are fidelities of the states $|0\rangle$ and $|1\rangle$, respectively, and the four states $|0_0\rangle_E$, $|1_0\rangle_E$, $|0_1\rangle_E$, and $|1_1\rangle_E$ belong to the Hilbert space of Eve's ancilla and satisfy ${}_E\langle 0_0|1_0\rangle_E = {}_E\langle 0_1|1_1\rangle_E = 0$.[3] In practice, the error rate of the states $|0\rangle$ and $|1\rangle$ may be identical if Alice and Bob use an uncharacteristic quantum channel. In experiment, Alice and Bob will discard their key bits if the error rates of $|0\rangle$ and $|1\rangle$ are inequable. On this condition, we find that $f \equiv f_0 = f_1$, and $d = \sqrt{1-f}$. Here f is fidelity and d is QBER in SIFT. Taking the inner product of equalities (1) and (2), we can obtain that

$${}_E\langle 0_0|1_1\rangle_E + {}_E\langle 1_0|0_1\rangle_E = 0. \tag{3}$$

Suppose that ${}_E\langle 0_1|0_0\rangle_E = \cos x$, and ${}_E\langle 1_0|1_1\rangle_E = \cos y$. Let us calculate the probability that Eve may be detected (the QBER) in CTRL. From Eqs. (1) and (2), we can obtain that

$$U|+\rangle|0\rangle_E = |+\rangle|+_+\rangle_E + |-\rangle|-_+\rangle_E,$$

where $|+_+\rangle = 1/2(\sqrt{f}|0_0\rangle + \sqrt{d}|1_0\rangle + \sqrt{f}|0_1\rangle + \sqrt{d}|1_1\rangle)$, and $|-_+\rangle = 1/2(\sqrt{f}|0_0\rangle - \sqrt{d}|1_0\rangle - \sqrt{f}|0_1\rangle + \sqrt{d}|1_1\rangle)$, and

$$U|-\rangle|0\rangle_E = |-\rangle|+_-\rangle_E + |+\rangle|-_-\rangle_E,$$

where $|+_-\rangle = 1/2(\sqrt{f}|0_0\rangle - \sqrt{d}|1_0\rangle + \sqrt{f}|0_1\rangle - \sqrt{d}|1_1\rangle)$, and $|-_-\rangle = 1/2(\sqrt{f}|0_0\rangle + \sqrt{d}|1_0\rangle - \sqrt{f}|0_1\rangle - \sqrt{d}|1_1\rangle)$. With an uncharacteristic quantum channel, we may assume that $f_{\mathrm{CTRL}} = |{}_E\langle +_+|+_+\rangle_E| = |{}_E\langle +_-|+_-\rangle_E|$, which is the fidelity of the quantum states in CTRL. Likewise, $e_{\mathrm{CTRL}} = |{}_E\langle -_+|-_+\rangle_E| = |{}_E\langle -_-|-_-\rangle_E|$ is QBER in CTRL. A detailed calculation shows that

$$f_{\mathrm{CTRL}} = \frac{1}{2}(1 + f\cos x + d\cos y) + \frac{1}{2}\sqrt{df}({}_E\langle 0_0|1_1\rangle_E + {}_E\langle 1_0|0_1\rangle_E),$$

and

$$e_{\mathrm{CTRL}} = \frac{1}{2}(1 - f\cos x - d\cos y) - \frac{1}{2}\sqrt{df}({}_E\langle 0_0|1_1\rangle_E + {}_E\langle 1_0|0_1\rangle_E).$$

By applying the relations in Eq. (3), we can obtain

$$f_{\mathrm{CTRL}} = \frac{1}{2}(1 + f\cos x + d\cos y),$$

$$e_{\mathrm{CTRL}} = \frac{1}{2}(1 - f\cos x - d\cos y).$$

After Alice and Bob's announcements of SIFT, Eve can measure her ancilla to gain information about Alice and Bob's key bits. In order to find out Alice's states, Eve has to distinguish $|0_0\rangle_E$ from $|0_1\rangle_E$ or distinguish $|1_0\rangle_E$ from $|1_1\rangle_E$.[4] In SIFT, when Bob obtained a correct result with f, Eve has to distinguish $|0_0\rangle_E$ from $|0_1\rangle_E$. Otherwise, Eve needs to distinguish $|0_1\rangle_E$ from $|1_1\rangle_E$, according to Bob's incorrect results with probability d. The optimal measurement distinguishing two states with overlap $\cos x$ is known to provide Eve with the correct guess with probability $[1 + \sin x]/2$.[5] Eve's maximal Shannon information attained from her optimal measurement is thus given by

$$I(A:E) = f\left[1 - h\left(\frac{1+\sin x}{2}\right)\right] + d\left[1 - h\left(\frac{1+\sin y}{2}\right)\right], \tag{4}$$

where $h(p) = -p\log_2 p - (1-p)\log_2(1-p)$ is binary Shannon entropy. At first glance, Eve can gain information about Alice and Bob's key bits without inducing any QBER in SIFT when $d = 0$ according to Eq. (4). However, the information Eve can gain is dependent on $\cos x$ and $\cos y$, which will induce nonzero QBER in CTRL as long as Eve's information is nonzero. Therefore, Eve's eavesdropping attacks will be detected either in SIFT or in CTRL.

4. Information of Final Key

For a given d, $I(A:E)$ is maximal when $\cos x = \cos y$. Therefore, the maximal information Eve can gain $I(A:E)$ is given by

$$I(A:E) = 1 - h\left(\frac{1+\sin x}{2}\right).$$

On this condition, we have that

$$e_{\mathrm{CTRL}} = \frac{1}{2}(1 - \cos x).$$

Consequently, we can obtain that $\sin x = 2\sqrt{e_{\mathrm{CTRL}} - e_{\mathrm{CTRL}}^2}$. On the other hand, information Bob can gain only depends on QBER d in SIFT:

$$I(A:B) = 1 - h(d) = 1 + d\log_2 d + (1-d)\log_2(1-d).$$

EC and PA can be implemented whenever Bob has more information than Eve using only one-way communication. Thus, the secure information about Alice and Bob's INFO bits to generate final key bits with one-way communication can be obtained with

$$\Delta I = I(A:B) - I(A:E),$$

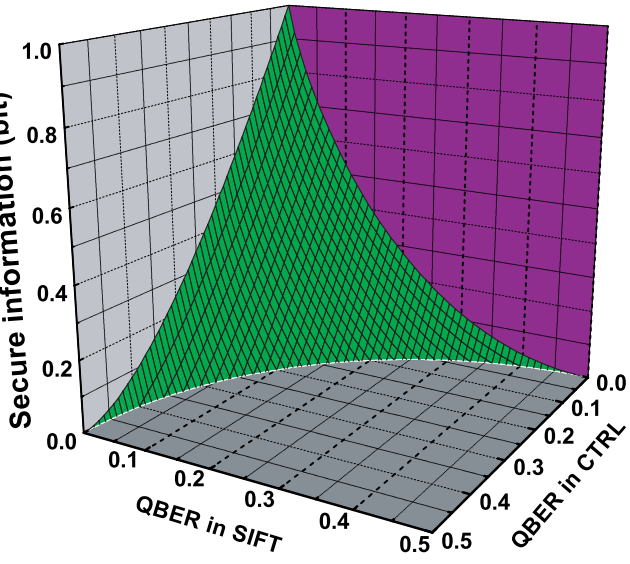

Fig. 1. (Color on line.) Numerical solution of secure information of INFO bits versus QBER in CTRL (e_{CTRL}) and SIFT (d). The rate of secure final key (the green) can be extracted from Alice and Bob's INFO bits when $I(A:B) \geq I(A:E)$ using only one-way communication. Since d and e_{CTRL} can be verified experimentally, Alice and Bob can verified the security of the final key bits with d and e_{CTRL}.

which is completely determined by two independent parameters d and e_{CTRL}. Alice and Bob can verify d and e_{CTRL} in their experiment by using their classical channel, so that they can verify the security of their final key. In Fig. 1, we present a numerical solution of ΔI with two independent parameters d and e_{CTRL}. In fact, this protocol can be perfectly implemented with a practical cryptosystem, since we have presented the amount of tolerable noise.

5. QKD without Quantum Capacity

It is interesting to ask whether QKD is still robust when both Alice and Bob have only classical capacities. The answer is positive. Here, we present a protocol to show that QKD is still robust even if neither Alice nor Bob has quantum capacities. Suppose Charlie, an assistant in this protocol, holds a round-trip quantum channel. Both Alice and Bob can access a segment of Charlie's quantum channel. In each run, Charlie always prepares a qubit in X basis and sends it out through his quantum channel. When a qubit is arriving, both Alice and Bob can either let it go undisturbed or measure it in classical {0,1} basis and prepare a fresh one in {0,1} basis and send it. Charlie receives the travel back qubit and measures it in X basis or Z basis randomly. There are three possibilities: (p0) Neither Alice nor Bob disturbed the travel qubit. (p1) One of them measured the travel qubit but the other did not. (p2) Both Alice and Bob measured the travel qubit. After all of

Charlie's qubits have been distributed, Alice, Bob and Charlie can publish some of their operations through their classical channel. When (p0) happened, the travel qubit has not been disturbed so that they can use this run as CTRL if Charlie has measured it in X basis. When (p1) happened, Alice or Bob publishes states of the travel back qubit and then they can also use this run as CTRL if Charlie has measured the travel qubit in Z basis. When (p2) happened, Bob knows the state Alice prepared so that Alice and Bob share a common bit as SIFT bit. In the end, Alice and Bob will publish some of their SIFT bits to verify QBER in SIFT. If both QBER in SIFT and QBER in CTRL are tolerable, Alice and Bob can use their INFO bits to generate final key bits after EC and PA. We will briefly discuss the security of this protocol below.

First of all, we want to point out that Eve's attack is effective only in SIFT. In SIFT, Eve's attack before Alice is useless since Alice will refresh the travel qubit. However, Eve cannot distinguish SIFT from CTRL until Alice and Bob's public announcements. Therefore, the optimal attack scheme is that Eve attacks each travel qubit after Alice in each run. Eve's such attack operations can be described by Eqs. (1) and (2). Likewise, such attack operations will induce nonzero QBER in CTRL, which should be detected in experiment. After Alice and Bob verified QBER in SIFT, they can generate final key bits with their INFO bits. We want to emphasize that Charlie cannot share Alice and Bob's key bits since Bob refreshes each travel qubit in SIFT. Therefore, Alice and Bob can distribute secure key bits even if neither of them has quantum capacities.

Along the line above, we can present a QKD network scheme with numerous parties who do not have quantum capacities. Suppose that A (the assistant) holds a round-trip quantum channel and always prepares qubit in X basis. B_i $(1 \leq i \leq n)$ are communication parties who can access a segment of the quantum channel. When a qubit passed, all of them can either let it go undisturbed or measure it in classical $\{0,1\}$ basis and prepare a fresh one and send it. There are three possibilities: (p0) None of B_i measured the travel qubit. (p1) One of B_i measured the travel qubit but the other did not. (p2) More than one of B_i measured the travel qubit. Likewise, (p0) and (p1) can be used as CTRL when A measured the travel back in correct bases. When (p2) occurred (suppose B_k measured the travel qubit after B_m), B_k and B_m then use their results as SIFT bits. In the end, B_k and B_m should also publish some of their SIFT bits to verify QBER in SIFT. If both QBER in CTRL and QBER in SIFT are tolerable, B_k and B_m can use their INFO bits to generate the final key. In this way, secure key bits can be distributed among those parties who can access a segment of the quantum channel.

6. Discussion and Conclusion

In Ref. 1, it has been shown that QKD is secure when Bob is classical. In this paper, we proved that QKD is still robust when Alice has only classical capacities. Even if Alice only encodes her bit information in a fixed basis and Eve knows this

fact, Alice and Bob can distribute secure key bits robustly. We have presented the amount of tolerable noise, so that, in principle, QKD with classical Alice can be implemented with practical quantum cryptosystems.

It is surprising that secure key bits can be distributed between two classical parties, which may conflict with the traditional concept that both Alice and Bob are required to have quantum capacities, at least Alice should have quantum capacities. In fact, the security of QKD is based on the fact that Eve cannot distinguish nonorthogonal quantum states. Therefore, quantum is necessary in QKD for security reason, but both Alice and Bob may be classical.

Acknowledgment

This work is supported by National Natural Sciences Foundation of China (Grant No. 10504039) and the Youth Chenguang Project of Science and Technology of Wuhan City.

References

1. M. Boyer, D. Kenigsberg and T. Mor, *Phys. Rev. Lett.* **99** (2007) 140501.
2. N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, *Rev. Mod. Phys.* **74** (2002) 145.
3. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).
4. On this condition, Eve's optimal approach to distinguishing Alice's states is that she sets ${}_E\langle 0|3\rangle_E = {}_E\langle 1|2\rangle_E = 0$. This does not influence Alice and Bob's QBERs in SIFT and CTRL but help Eve to optimally distinguish her ancilla states to gain information about Alice and Bob's key bits.
5. A. Peres, *Phys. Lett. A* **128** (1988) 19.