Vol 18 No 6, June 2009
1674-1056/2009/18(06)/2143-06

Chinese Physics B

© 2009 Chin. Phys. Soc.
and IOP Publishing Ltd

Quantum key distribution series network protocol with M-classical Bobs*

Zhang Xian-Zhou(张现周)[a)†], Gong Wei-Gui(公伟贵)[a)‡], Tan Yong-Gang(谭勇刚)[b)], Ren Zhen-Zhong(任振忠)[a)], and Guo Xiao-Tian(郭笑天)[a)]

[a)] *Physics and Information Engineering College, Henan Normal University, Xinxiang* 453007, *China*

[b)] *Physics and Information Engineering College, Luoyang Normal College, Luoyang* 471022, *China*

(Received 27 June 2008; revised manuscript received 24 September 2008)

Secure key distribution among classical parties is impossible both between two parties and in a network. In this paper, we present a quantum key distribution (QKD) protocol to distribute secure key bits among one quantum party and numerous classical parties who have no quantum capacity. We prove that our protocol is completely robust, i.e., any eavesdropping attack should be detected with nonzero probability. Our calculations show that our protocol may be secure against Eve's symmetrically individual attack.

Keywords: quantum key distribution, symmetrical attack, network protocol
PACC: 0367, 4250

1. Introduction

Cryptography is the art of rendering a message unintelligible to any unauthorized party. In symmetrical (secret-key) cryptosystems, symmetrical ciphers require the use of a single key for both encryption and decryption. These systems can be thought of as a safe in which the message is locked by Alice with a key and Bob in turns uses a copy of this key to unlock the safe. In the one-time pad scheme, because the bits of the scrambled text are as random as those of the key, they do not contain any information. This cryptosystem is thus provably secure according to information theory. In fact, it is the only provably secure cryptosystem known today. But, this system has a problem: it is essential for Alice and Bob to possess a common secret key, which must be at least as long as the message itself. They can only use the key for a single encryption, hence this type of protocol having the name one-time pad. If they used the key more than once, Eve could record all of the scrambled messages and start to build up a picture of the plain texts and thus also of the key. The one-time pad is currently used only for the most critical applications, because of the problem of distributing long sequences of key bits based on permutations and nonlinear functions to produce the cipher text blocks. So, like asymmetrical cryptosystems, they offer only computational security. If these algorithms were broken by mathematical advances, QKD would constitute the only way to solve the key distribution problem.

Quantum key distribution (QKD) is a protocol by which we can get private key bits between two parties over a quantum channel securely. The key bits can then be used in a classical private key cryptosystem, to enable the parties to communicate securely. QKD is the only physically secure way for the distribution of a secret key between two parties. Its security is based on the well-known fact that the measurement of an unknown quantum state modifies the state itself: thus an eavesdropper cannot get information on the key without introducing errors in the correlations between the sender and receiver. In other words, QKD is secure because of the no-cloning theorem in quantum mechanics: it is impossible to make a copy of an unknown quantum state. A key distributed via quantum cryptography techniques is secure against any eavesdropper, even if they have unlimited computational power.

The first quantum cryptography protocol was invented by Bennett and Brassard,[1] which is the well-known BB84 protocol. The BB84 protocol consists

*Project supported by the National Natural Science Foundation of China (Grant No 10774039).
†Corresponding author. E-mail: xz-zhang@henannu.edu.cn
‡Corresponding author. E-mail: gongweigui@163.com

of two major parts: first, creating a sifted key; second, extracting an error-free, secure, final key from the sifted key. In our work, we follow this protocol's definition: in the first, Alice chooses N random bits and she encodes each bit in $Z(|0\rangle, |1\rangle)$ basis or in $X(1/2(|0\rangle + |1\rangle), 1/2(|0\rangle + |1\rangle))$ basis, then she sends the encoded results to Bob. When Bob receives the qubits, he announces the fact and measures each bit in the Z or X basis at random. Then, Alice announces in which basis she encoded the bits; they then discard the bits which use the mismatching bases. The values of the rest of the bits we choose as the sifted key. In the second, Alice and Bob select some of the sifted key as a check. If the error bit rate is higher than an acceptable number, they abort the protocol. The final remaining bits are used as the INFO bits, now Alice and Bob perform information reconciliation (using an error correcting code "ECC") and privacy amplification (PA) in order to get m shared key bits. Then, quantum communication with two parties and its security was extensively studied.[2−5] It is interesting to study quantum communication with more than two parties. Sharing classical information via a multiple access quantum channel was first considered in Ref.[6]. The issue of sending quantum information in the general multiparty scenario has also been raised in Refs.[7] and [8]. In this paper, we present a protocol with one sender (who is generally called Alice) and multi-receiver Bobs (who are generally called Bob-1,...,Bob-M) in a series network.

In this work, we present a QKD network protocol in which the sender (Alice hereafter) can share secret keys with any receiver (Bob hereafter) or any part of the receivers. In this protocol, the receivers are classical:[9] we can describe two orthogonal states of the quantum two-level system with the classically computational basis $|0\rangle$ and $|1\rangle$. Because the computational basis is "classical", we can use the classical notations to describe the two quantum states. In the protocol we will present, any Bob can access a segment of the channel which leads from the Alice's lab, and whenever a qubit passes through that segment he may either let it go undisturbed or (i) measure the qubit in the classical basis and (ii) prepare a (fresh) qubit in the classical basis and send it.

Quantum key distribution with classical Bob: Let us first review the novel semiquantum key distribution protocol, QKD with classical Bob.[9] Alice holds a quantum channel which leads from and then back to her lab and Bob can access one segment of the quantum channel. Alice generates N random qubits in the Z or X basis and sends them to Bob. For each qubit arriving, Bob chooses randomly either to reflect it (CTRL) or to measure it in the Z basis and resends it in the same state he found (to SIFT it). Alice measures each qubit in the basis she sent it and publishes which were her Z bits and Bob publishes which ones he chose to SIFT. For about $N/4$ bits, Alice used the Z basis and Bob chose to SIFT; these are the Z-SIFT bits, which form the sifted key. In the same way, for approximately $N/4$ bits, Alice and Bob get two strings of Z-CTRL and X-CTRL bits. The rest of the bits (those sent in the X basis but chosen as SIFT by Bob) are ignored. Alice checks the error rate on the CTRL bits. Alice also chooses at random n SIFT bits to be TEST bits. If the error rate is higher than some predefined threshold or the error on the SIFT bits and the CTRL bits are different, the protocol aborts. Lastly, Alice and Bob select the remaining SIFT bits to be used as INFO bits and they perform error correcting (EC) and privacy amplification (PA) to obtain final key from INFO bits.

2. A QKD network protocol

Here we present a QKD network protocol in a series network as shown in Fig.1. The protocol is aimed to create an n-bit INFO string for generating a shared secret key in the series network. In this network, Alice and Bobs (Bob-1, Bob-2, ..., Bob-M) are in the line. A qubit travels from Alice's lab to the outside and then goes back to her lab again. Each Bob-k ($k = 1, 2, \ldots, M$) can access the traveled qubit. In principle, there may be an Eavesdropper–Eve, who may attack the traveled qubit between two neighbor Bob-k and Bob-$(k + 1)$. In this protocol, Alice generates qubits in the Z basis and randomly selects whether to apply the Hadamard gate (H) or do nothing (I). Then she sends these qubits to Bobs in the line. For each qubit each Bob either lets it go without operating on it or measures it in Z basis and sends a new qubit to the next Bob in the state he obtained. The last Bob measures and resends the qubit or just reflects it to Alice. Before presenting the QKD with network protocol, we give a convention on some of the notations. Let n be the desired length of the INFO strings. $\delta > 0$ is a fixed parameter and N is the number of the qubits which Alice generates.

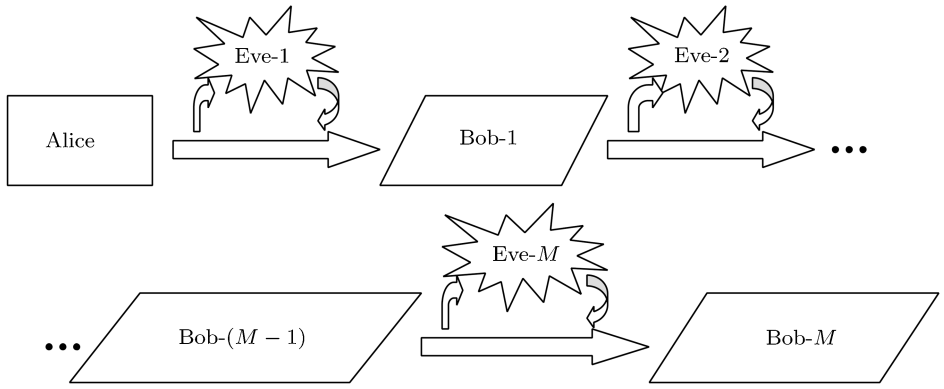


Fig.1. The schematic sketch of a sender and M receivers series network. Alice is the sender. Eve-1, ..., Eve-M are eavesdroppers in the line who may attack the qubit when traveling to Bob-M or back to Alice. Bob-1, ..., Bob-M are receivers in the line.

(i) Alice generates $N = 4n(2^M + \delta)$ random qubits in the Z basis. For each of the qubits, she randomly selects whether to apply the Hadamard gate (H) or do nothing (I).

(ii) For each qubit arriving, Bob-k chooses randomly to transfer it to the next Bob without touching it (CTRL) or to measure it in the Z basis and resend it to Bob-$k+1$ in the same state he found (If one of the Bobs selects to measure it in classical {0,1} bases, his results will be kept as SIFT this time). Finally, the qubit goes back to Alice.

(iii) Alice measures each qubit in the basis she sent it.

(iv) Alice publishes which were her Z bits and all of the M Bobs publish their operations to determine which bases as SIFT and which ones as CTRL.

(v) Alice checks the error rate on the CTRL bits and if either the X error rate or the Z error rate is higher than some predefined threshold or the error bit on the X-CTRL is different with that on Z-CTRL, the protocol aborts.

(vi) Alice chooses at random n SIFT bits to be TEST bits. She publishes which are the chosen bits. Bobs publish the values of these TEST bits. Alice checks the error rate on the TEST bits and if it is higher than some predefined threshold, the protocol aborts.

(vii) Alice and Bobs select the remaining n SIFT bits to be used as INFO bits to generate a secure final key.

(viii) In this way, Alice can share a secure key with different Bobs.

3. Security proof of the protocol

Generally speaking, according to Ref.[10], the eavesdropping on a quantum channel is as follows. When a qubit travels from Alice to Bob, Eve can let a system (a probe) interact with the qubit. The interaction chosen by Eve should be independent of the qubit state and should obey the laws of quantum mechanics (Considering a better eavesdropping scheme, Eve will not measure on Alice's qubit directly, so the interaction must be a unitary operation). After the interaction a qubit has to go to Bob; and then Eve may take a measurement of the state in her probe space, thus, she may get some information about the qubit.

In our protocol, Alice chooses two sets of symmetrical bases as that of BB84. And in non-bias quantum channel, the error rates on Z-CTRL and X-CTRL are the same. Or else, Alice and Bob can abort the protocol this time. In order to simplify the proof, we can regard the Alice as Bob-0, so there are $M+1$ Bobs in the line. If the whole line is security, we should guarantee that the quantum channel between any two Bobs is security.

Definition

H_{Eve}: *The Hilbert space of Eve's probe system;*

C^2: *The Hilbert space of the total qubit+probe system;*

$|m\rangle$, $|0^E\rangle$, U: *the qubit's and the probe's initial states and the unitary interaction, respectively.*

Since anyone who is outside Alice's lab has no prior information about Alice's bases selection, Alice's states are completely mixed to anyone outside Alice's

lab

$$\rho = \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{|-\rangle\langle -| + |+\rangle\langle +|}{2}. \quad (1)$$

Here $|0\rangle$ and $|1\rangle$ are the states prepared on basis Z, and $|-\rangle$ and $|+\rangle$ are the states prepared on basis X.

Of course, Eve can attack on Alice's qubit symmetrically with her probes.[10] After interaction, the states can be written in the following form

$$U|0\rangle|0^E\rangle = f_1|0\rangle\phi_{00} + d_1|1\rangle\phi_{01}, \quad (2)$$
$$U|1\rangle|0^E\rangle = f_2|1\rangle\phi_{10} + d_2|0\rangle\phi_{11}. \quad (3)$$

Here the four normalized states ϕ_{00}, ϕ_{01}, ϕ_{10} and ϕ_{11} belong to the Hilbert space of Eve's probe $H_{\rm Eve}$ and satisfy $\phi_{01}\perp\phi_{02}$ and $\phi_{10}\perp\phi_{11}$. By symmetry, $f_1^2 = f_2^2 \equiv F \in \mathbb{R}$ (The fidelity: the probability that Bob gets the correct result) and $d_1^2 = d_2^2 \equiv D \in \mathbb{R}$ (The error rate: the probability that Bob gets the wrong result). Unitary implies $F + D = 1$, and with Eq.(3) and Eq.(4) one can get

$$\phi_{00}^\dagger\phi_{11} + \phi_{10}^\dagger\phi_{01} = 0, \quad (4)$$

where ϕ_{00} and ϕ_{10} correspond to Eve's states when Bob receives the qubit undisturbed, while ϕ_{01} and ϕ_{11} are Eve's states when the qubit is disturbed.

By symmetry, Eve's attacks on the states prepared on X basis produce

$$\begin{aligned} U|+\rangle|0^E\rangle &= U\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0^E\rangle \\ &= \frac{1}{\sqrt{2}}U|0\rangle|0^E\rangle + \frac{1}{\sqrt{2}}U|1\rangle|0^E\rangle, \end{aligned} \quad (5)$$

and

$$\begin{aligned} U|-\rangle|0^E\rangle &= U\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|0^E\rangle \\ &= \frac{1}{\sqrt{2}}U|0\rangle|0^E\rangle - \frac{1}{\sqrt{2}}U|1\rangle|0^E\rangle. \end{aligned} \quad (6)$$

Here the following relationship has been used

$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle), \quad (7)$$
$$|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle). \quad (8)$$

Using Eq.(3), one can get

$$U|+\rangle|0^E\rangle = f_3|+\rangle|\phi_{+0}\rangle + d_3|-\rangle|\phi_{+1}\rangle, \quad (9)$$
$$U|-\rangle|0^E\rangle = f_4|-\rangle|\psi_{-0}\rangle - d_4|-\rangle|\phi_{-1}\rangle. \quad (10)$$

Here one can also have $f_3^2 = f_4^2 \equiv F \in \mathbb{R}$ and $d_3^2 = d_4^2 \equiv D \in \mathbb{R}$, and the following relationship can be obtained by calculation

$$\phi_{+0} = \frac{1}{2}(f\phi_{00} + d\phi_{01} + f\phi_{10} + d\phi_{11}), \quad (11)$$

$$\phi_{+1} = \frac{1}{2}(f\phi_{00} - d\phi_{01} - f\phi_{10} + d\phi_{11}). \quad (12)$$

Similarly,

$$\psi_{-0} = \frac{1}{2}(f\phi_{00} - d\phi_{01} + f\phi_{10} - d\phi_{11}), \quad (13)$$

$$\phi_{-1} = \frac{1}{2}(f\phi_{00} + d\phi_{01} - f\phi_{10} - d\phi_{11}). \quad (14)$$

As in any quantum key distribution protocol, we can assume that Eve's ability is only limited by the quantum principle. She can of course make her probes in a large Hilbert space so that more unitary interacting results can be read out from her probes directly. Optimally, she can make $\phi_{+0}\perp\phi_{+1}$ and $\phi_{-0}\perp|\phi_{-1}$ as the case of the attack on Z-basis. If choosing proper phases, $\phi_{00}^\dagger\phi_{11}$ can be made real and then by Eq.(5) $\phi_{01}^\dagger\phi_{10}$ is also real, and so do $\phi_{+0}^\dagger\phi_{-1}$ and $\phi_{+1}^\dagger\phi_{-0}$.

With $|\phi_{+0}\rangle\perp|\phi_{+1}\rangle$, we have

$$\begin{aligned} \phi_{+0}\perp\phi_{+1} = {} & F\phi_{00}^\dagger\phi_{00} - \sqrt{FD}\phi_{00}^\dagger\phi_{01} \\ & - F\phi_{00}^\dagger\phi_{10} + \sqrt{FD}\phi_{00}^\dagger\phi_{11} \\ & + \sqrt{FD}\phi_{01}^\dagger\phi_{00} - D\phi_{01}^\dagger\phi_{01} \\ & - \sqrt{FD}\phi_{01}^\dagger\phi_{10} + D\phi_{01}^\dagger\phi_{11} \\ & + F\phi_{10}^\dagger\phi_{00} - \sqrt{FD}\phi_{10}^\dagger\phi_{01} \\ & - F\phi_{10}^\dagger\phi_{10} + \sqrt{FD}\phi_{10}^\dagger\phi_{11} \\ & + \sqrt{FD}\phi_{11}^\dagger\phi_{00} - D\phi_{11}^\dagger\phi_{01} \\ & - \sqrt{FD}\phi_{11}^\dagger\phi_{10} + D\phi_{11}^\dagger\phi_{11} \\ = {} & 0. \end{aligned} \quad (15)$$

Then one can obtain

$$\langle\phi_{00}|\phi_{11}\rangle = \langle\phi_{01}|\phi_{10}\rangle, \quad (16)$$

together with Eq.(4), one gets

$$\langle\phi_{00}|\phi_{11}\rangle = \langle\phi_{01}|\phi_{10}\rangle = 0. \quad (17)$$

By using this symmetric attack, Eve's probes record some information of Alice's qubits. And with Eqs.(1)–(17), one can find that the maximum information Eve can obtain is totally determined by her ability to differentiate ϕ_{00} from ϕ_{10}, ϕ_{01} from ϕ_{11}, ϕ_{-0} from ϕ_{+0} and ϕ_{-1} from ϕ_{+1} (Because Eve can measure her probes after Alice and Bob's basis reconciliation, so Eve does not need to differentiate between

probe states from different bases). And the optimal measurement distinguishing two states with overlap $\cos\theta$ is known to provide Eve with the correct guess with probability $(1+\sin\theta)/2$.[11] Then the maximum information she can obtain from her probes is

$$\begin{aligned} I(\alpha,\epsilon) &= F\left[1-h\left(\frac{1+\sin\theta}{2}\right)\right] \\ &\quad + D\left[1-h\left(\frac{1+\sin\theta}{2}\right)\right] \\ &= \left[1-h\left(\frac{1+\sin\theta}{2}\right)\right]. \end{aligned} \tag{18}$$

After Alice, Bob and Eve's measurement, they are left with classical random variables α, β, and ϵ, respectively. Secret-key agreement between Alice and Bob is then possible using only error correction and privacy amplification if and only if the Alice-Bob mutual Shannon information $I_{\alpha,\beta}$ is greater than the Alice-Eve or the Bob-Eve mutual information, $I_{\alpha,\beta} > I_{\alpha,\epsilon}$ or $I_{\alpha,\beta} > I_{\beta,\epsilon}$. The Alice-Bob mutual Shannon information depends only on the error rate D:

$$\begin{aligned} I(\alpha,\beta) &= 1-h(D) \\ &= 1+D\log_2(D)+(1-D)\log_2(1-D). \end{aligned} \tag{19}$$

Then Alice and Bobs can estimate the security of the quantum channel by the QBER on X-CTRL and Z-CTRL. If they are different, Alice and Bob will abort the communication this time. Then Alice and Bobs can calculate information Bobs can gain from the Alice. If Eve's information gain is bigger than a predefined value (Usually, it is smaller than the mutual information between the communication parties so that privacy amplification can be implemented), they abort their communication this time. So this protocol is secure against Eve's symmetrically individual attack.

4. Discussion

As mentioned above, in this protocol, Eve can extract the secret key with part of Bobs or with any Bob or even with all Bobs in the series quantum network. In fact, the efficiencies of different parties to share the secret information is not the same, which can be shown in Table 1.

Then one can draw some conclusions:

(i) In general, if m Bobs want to know each other's information, they choose the string $(X)^{M-m}$-CTRL-$(Z)^m$-SIFT as their sifted key (In this case, these m Bobs choose to SIFT).

Table 1. The probability for Alice to extract sifted key with $m = 1, \ldots, M$ Bobs. The middle column denotes operations of Bobs in the quantum series network.

m	operations	probability
0	$(X)^M$-CTRL$(Z)^0$-SIFT	$\frac{1}{4*2^M}$
1	$(X)^{M-1}$-CTRL$(Z)^1$-SIFT	$\frac{M}{4*2^M}$
$\cdots,$	$\cdots,$	$\cdots$
m	$(X)^{M-m}$-CTRL$(Z)^m$-SIFT	$\frac{\frac{M!}{(M-m)!m!}}{4*2^M}$
$\cdots,$	$\cdots,$	$\cdots$
M	$(X)^0$-CTRL$(Z)^M$-SIFT	$\frac{2}{2^M}$

(ii) There are still two special cases: Alice wants to communicate with any Bob or all Bobs.

(a) If Alice just wants to communicate with the m^{th} Bob and the others cannot get the information, they can choose the sting $(Z)^{M-1}$-CTRL-$(Z)^1_{\text{Bob}-m}$-SIFT as their sifted bits (the m_{th} Bob chooses to SIFT and the others choose to CTRL).

(b) If Alice wants every Bob to know each others information, they can choose the string $(Z)^M$-SIFT as their sifted key (all m Bobs choose to SIFT).

(iii) Let us suppose that $M = 2$ (i.e., there are only two Bobs in the line):

(a) If Alice does not want Bob-1 and Bob-2 to know each other's information, she chooses the string $(Z)^1$-CTRL$(Z)^1_{\text{Bob1}}$-SIFT (Bob-1 chooses to SIFT and Bob-2 chooses to CTRL) as the Alice and Bob-1's sifted key, and choose the string $(Z)^1$-CTRL$(Z)^1_{\text{Bob2}}$-SIFT as the Alice and Bob-2's sifted key.

(b) If Alice wants Bob-1 and Bob-2 to know each other's information, she chooses the string $(Z)^2$-SIFT (both two Bobs choose to SIFT) as their sifted key.

In this protocol, we find a very interesting phenomenon: Each Bob can have no relations with the others in a series network. When they communicate with Alice they can keep independent from each other and when receivers communicate with each other the sender can get the information. So, the sender here can be regarded as a commander. Alternately, we can choose any Bob as a sender at random and regard this Bob as a commander and then communicate in this mode. It is impossible in the classical series network.

5. Summary and conclusion

In summary, we have presented a protocol for a QKD series network with classical parties and proved its robustness. We believe that our work provides a new approach to construct the quantum key distribution network. Such research on the QKD network may be implemented experimentally with current technologies.

Acknowledgements

We have benefited greatly from enlightening discussions with Cai Qing-Yu and thank him for providing the motivation for this research.

References

[1] Bennett C H and Brassard G "*Quantum Cryptography: Public-key Distribution and Coin Tossing, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*", Bangalore, India, December 1984 pp175–179
[2] Cai Q Y and Li B W 2004 *Phys. Rev.* A **69** 054301
[3] Cai Q Y 2003 *Phys. Rev. Lett.* **91** 109801
[4] Lü H, Chen A X and Yan X D 2007 *Chin. Phys.* **16** 2862
[5] Yang Y G, Wen Q Y and Zhu F C 2007 *Chin. Phys.* **16** 910
[6] Winter A 2001 *Information Theory, IEEE Transactions* **47** 3059
[7] Dür W, Cirac J I and Horodecki P 2004 *Phys. Rev. Lett.* **93** 020503
[8] Demianowicz M and Horodecki P 2006 *Phys. Rev.* A **74** 042336
[9] Boyer M, Kenigsberg D and Mor T 2007 *Phys. Rev. Lett.* **99** 140501
[10] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[11] Peres A 1998 *Phys. Lett.* A **128** 19