Quantum Information and Computation, Vol. 7, No. 4 (2007) 329–334
© Rinton Press

A SIMPLE PARTICIPANT ATTACK ON THE BRÁDLER-DUŠEK PROTOCOL

FEI GAO*,[a] SU-JUAN QIN and QIAO-YAN WEN
School of Science, Beijing University of Posts and Telecommunications,
Beijing, 100876, China
**State Key Laboratory of Integrated Services Network, Xidian University,*
Xi'an, 710071, China

FU-CHEN ZHU
National Laboratory for Modern Communications, P.O.Box 810,
Chengdu, 610041, China

Received August 15, 2006
Revised December 22, 2006

The ring-arrangement quantum secret sharing protocol in the paper [K. Brádler and M. Dušek (2004) *J. Opt. B: Quantum Semiclass. Opt.* **6** 63] is analyzed and it is shown that this protocol is secure for any eavesdropper except for a dishonest participant. For example, by a special strategy, Bob can steal Charlie's portion of information without being detected and then recover Alice's secret by himself. We give a description of this strategy and point out a possible way to improve the protocol to stand against this attack.

Keywords: secret sharing, quantum cryptography, cryptanalysis, Brádler-Dušek protocol

Communicated by: H-K Lo H Zbinden

1 Introduction

As we know, the security of most conventional cryptosystems is based on computational complexity assumptions. In other words, this security is conditional. As a result, it is often heard that some cryptosystem is attacked successfully. To solve this problem, Bennett and Brassard [1] first came up with the idea of quantum cryptography [2] in 1984. Afterwards, lots of such schemes were presented (for example, see Refs. [3, 4, 5, 6, 7], more such schemes can be find in the references in Ref. [8]). It is alleged that the security of quantum cryptosystems is guaranteed by the fundamental laws of quantum mechanics and one cannot attack it successfully even if one has unlimited ability of computation. Indeed, for a well-designed protocol of quantum cryptography, any effective eavesdropping would be discovered by the legal users and then it can be said that this protocol has unconditional security in theory [9, 10, 11, 12]. Unfortunately, people cannot always propose this kind of well-designed schemes with proved security. In fact, giving a security proof for a scheme in general sense is more difficult than giving itself. Therefore, even carefully designed quantum cryptographic schemes may be also susceptible to certain subtle attacks which are not concerned in the original design [13, 14, 15].

[a] hzpe@sohu.com

Understanding those attack strategies will be helpful to improving the security of a protocol when it is designed [16].

Secret sharing is an important branch of cryptography. It is often introduced in the following conditions: Alice wants somebody to do an important business for her in a remote city where she has two agents, say Bob and Charlie. But Alice does not believe in both of them. Therefore, she encrypts her secret in two pieces, for Bob and Charlie respectively, and she knows the following: (1) One of the agents, and at least one, must be honest. (2) No agent alone has any knowledge of the secret, but both of them can jointly recover it. These assure Alice that her task would be accomplished in a secure manner.

The quantum counterpart of secret sharing is called quantum secret sharing (QSS). After the presentation of the first QSS protocol in 1999 [17], many kinds of QSS schemes are proposed (for example, see Refs. [18, 19], more such schemes can be find in the references in Ref. [20]).

In the paper [21] Brádler and Dušek proposed two quantum secret sharing protocols, the ring-arrangement one and the star-arrangement one. The security against several kinds of attacks was proved. However, we will show that by a special strategy Bob can totally obtain Alice's secret by himself without introducing any error in the three party ring-arrangement scheme. For simplicity, we call this scheme BD protocol hereafter.

Let us give a brief description of BD protocol first. Alice generates an entangled photon pair in one of four Bell states

$$\begin{aligned} |\Psi^{\pm}\rangle_{12} &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)_{12}, \\ |\Phi^{\pm}\rangle_{12} &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)_{12}, \end{aligned} \tag{1}$$

where the subscripts denote different photons. The initial state of the entangled pair corresponds to two bits of Alice's secret. Then Alice sends the second qubit (called travel qubit in Ref. [21], or TB for short) to Bob. Bob performs one of four Pauli operations $\{I, X, Y, Z\}$ at random on this qubit and then sends it to Charlie. Charlie randomly does one of the same four operations on TB and then sends it back to Alice. After that Alice performs a Bell measurement on qubits 1 and 2, and declares the outcome publicly. According to this measurement result Bob and Charlie can restore Alice's secret (the initial state of the entangled pair) by cooperation. This process would be redone for many times to distribute other secret bits from Alice (see figure 1(a)). Furthermore, at random time slot, Bob (or Charlie) switches to a "correlation measurement (CM)" to detect eavesdropping. More concretely, after the receipt of TB, Bob (or Charlie) performs a measurement in the basis $B_z = \{|0\rangle, |1\rangle\}$ instead of the Pauli operation on it. Afterward Bob (or Charlie) announces the measurement result. In this case Alice also does such a measurement on qubit 1. By comparing the two outcomes, Alice can judge whether there is any eavesdropper in the channel. If Charlie is the sponsor of a CM, Alice needs Bob's particular operation, which will be declared by Bob, as well as Charlie's measurement result to accomplish her judgement.

2 Participant attack

Now we show that Bob can cheat in this protocol. As described in figure 1(b), after his Pauli operation U_B on TB (qubit 2) Bob holds it and sends a fake photon (qubit 4) from his own

Bell state (for example, $|\Phi^+\rangle_{34}$) to Charlie. When Charlie sends this qubit to Alice, Bob intercepts it and sends the real TB (qubit $2'$) back to Alice. By this means Bob can obtain Alice's secret by himself after Alice performs the Bell measurement and declares the outcome. Furthermore, if needed, Bob can obtain U_C by a Bell measurement on qubits 3 and $4'$.

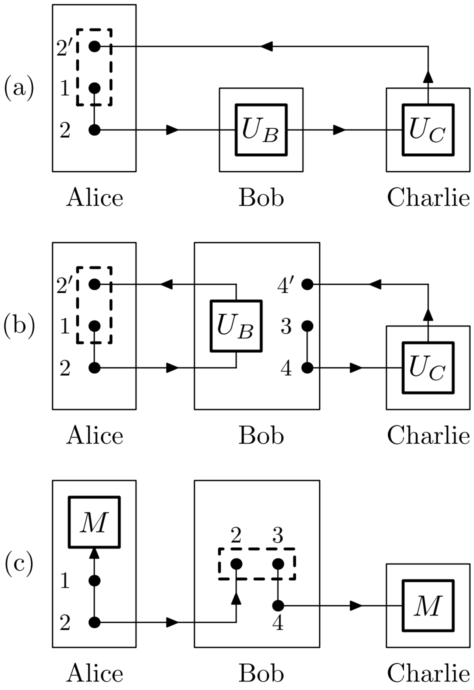

Fig. 1. BD protocol (a) and the participant attack (b,c). The black dots denote the photons and the two dots connected by a line construct an entangled pair. U_B (U_C) represents the Pauli operation performed by Bob (Charlie) and M is the measurement in the basis B_z. The dashed rectangle implies a Bell measurement. In addition, we use $2'$ ($4'$) to denote the photon 2 (4) after Pauli operation(s). See the text for details.

Above CM has not been concerned. The authors of Ref. [21] consider that Bob always introduces error by this kind of intercept-resend strategy. However, it is not the fact. Bob can avoid the detection by using entanglement swapping [22].

Suppose there are two Bell states $|\psi\rangle_{12}$ and $|\phi\rangle_{34}$. If one measures qubits 2 and 3 in Bell basis, entanglement swapping happens

$$|\psi\rangle_{12}|\phi\rangle_{34} \Rightarrow |\psi'\rangle_{14}|\phi'\rangle_{23}, \tag{2}$$

where both $|\psi'\rangle$ and $|\phi'\rangle$ are Bell states. Entanglement swapping has an interesting feature which has been discussed in Ref. [23]. That is, when the above entanglement swapping happens, there is a Pauli operator $U = \{I, X, Y, Z\}$ such that

$$\begin{aligned} & |\psi'\rangle = I \otimes U|\psi\rangle, \\ \mathit{and} \qquad & |\phi'\rangle = I \otimes U|\phi\rangle, \end{aligned} \tag{3}$$

where I and U are operators performed on the two photons in a Bell state respectively. In other words, after the entanglement swapping, if one knows any two Bell states among $|\psi\rangle$, $|\phi\rangle$, $|\psi'\rangle$, and $|\phi'\rangle$, he/she can infer the relation (that is, the particular U) between the other two states even though he/she does not know their particular states.

Based on the above feature, the dishonest Bob can avoid the detection craftily. His strategy is as follows (see figure 1(c)). When Bob requests CM he just does not implement his attack. Therefore, we consider only the case in which CM is initiated by Charlie. When Charlie sends a request for CM to Alice publicly (or Alice orders Bob to announce his Pauli operation on TB), Bob performs a Bell measurement on qubits 2 and 3 in his hand. As a result, entanglement swapping happens and qubits 1 and 4 would be projected onto a Bell state. According to his measurement result, Bob can give a declaration which always satisfies Alice. For example, if the initial state of qubits 3 and 4 is $|\Phi^+\rangle_{34}$ and his measurement result is $|\Psi^+\rangle_{23}$, Bob knows that the expected declaration is X (because $|\Psi^+\rangle = I \otimes X|\Phi^+\rangle$). This declaration implies that Bob has performed the operation $U_B = X$ on TB when it passes by him (in fact he did not perform such an operation, he just send a fake photon instead of the true TB to Charlie). With the help of (2)(3) it can be seen that this declaration is always consistent with the state shared by Alice and Charlie at this stage, that is, the Bell state of qubits 1 and 4 after entanglement swapping. By this means the dishonest Bob can always escape from Alice's detection.

As we pointed out in Refs. [24, 25], a participant generally has more power to attack than an outside eavesdropper in the secret sharing protocols because the participant can take advantage of the right to access the carrier state partly and participate in the process of eavesdropping detection. However, this kind of participant attack is prone to be omitted when we analyze various attack strategies. Therefore, we have to pay attention to this attack later.

To improve BD protocol against the participant attack, an additional detect process can be added. That is, Charlie performs another operation $U_{C'}$ on TB after the Pauli operation U_C, where $U_{C'}$ is I or H at random. Here H denotes the Hadamard operator, i.e.,

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{4}$$

After Alice received TB from Charlie, she does one of the following two process. (i) With a certain probability δ Alice requests Bob to declare his Pauli operation U_B and Charlie to announce U_C and $U_{C'}$. Note that in this stage Bob must give his declaration first. Afterward Alice performs the same $U_{C'}$ on TB to restore the Bell states and then a Bell measurement on qubits 1 and $2'$. According to U_B, U_C, the initial state and the final state of the entangled pair, Alice can judge whether an eavesdropper (especially a dishonest participant) exists. (ii) With the probability $1-\delta$ Alice requests Charlie to announce $U_{C'}$. Alice also performs such a $U_{C'}$ on TB and then a Bell measurement on qubits 1 and $2'$. At last Alice declares her measurement result as goes in BD protocol.

It is not difficult to show that Bob's attack will be detected by this additional process. As we know, the operator I does not change Bell states while H rotates them into

$$|\Gamma^\pm\rangle = I \otimes H|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|\Phi^\mp\rangle + |\Psi^\pm\rangle),$$

$$|\Omega^{\pm}\rangle = I \otimes H|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|\Phi^{\pm}\rangle - |\Psi^{\mp}\rangle). \tag{5}$$

These states construct a rotated basis $\{|\Gamma^{+}\rangle, |\Gamma^{-}\rangle, |\Omega^{+}\rangle, |\Omega^{-}\rangle\}$, which is conjugate with the Bell basis. As a result, when Bob intercepts qubit $4'$ (see figure 1(b)) Charlie sent to Alice, he cannot distinguish which of the two operations Charlie has performed. On the other hand, Bob does not know whether he should perform an additional H on qubit $2'$ before he sends it to Alice. Once Bob does it wrong, he cannot give a declaration which always satisfies Alice. For example, Bob did not perform H on qubit $2'$ but Charlie did on $4'$. Without loss of generality, suppose the state of qubits 1 and $2'$ is $|\Phi^{+}\rangle$ at this stage. When Charlie declares her operation of H, Alice will perform H on qubit $2'$, too. Consequently, the state $|\Phi^{+}\rangle$ will be changed into $|\Gamma^{+}\rangle$. Therefore, Alice will obtain $|\Phi^{-}\rangle$ or $|\Psi^{+}\rangle$ at random when she performs Bell measurement on qubits 1 and $2'$. Since the outcome is indeterministic it is impossible for Bob to give a correct declaration with certainty.

3 Conclusion

In summary, we present a simple but efficient attack, i.e. participant attack, on the ring-arrangement quantum secret sharing protocol in Ref. [21], in which Bob can obtain Alice's total secret by himself. In fact, the multi-party generalization of this protocol also faces to this kind of threat. As said in Ref. [16], breaking cryptosystems is as important as building them. Making clear different attack strategies is helpful for the work of scheme-designing. We point out that the participant attack should be paid more attention to when we analyze the security of multi-party quantum protocols because such schemes are inclined to suffer it [24, 25]. Finally a possible improvement of this protocol is given, which supplies a possible way to render such schemes immune from this kind of attack.

Acknowledgements

This work is supported by the National High Technology Research and Development Program of China, Grant No. 2006AA01Z419; the National Natural Science Foundation of China, Grant Nos. 90604023, 60373059; the National Research Foundation for the Doctoral Program of Higher Education of China, Grant No. 20040013007; the National Laboratory for Modern Communications Science Foundation of China, Grant No. 9140C1101010601; the Natural Science Foundation of Beijing; the Graduate Students Innovation Foundation of BUPT; and the ISN Open Foundation.

References

1. C. H. Bennett and G. Brassard (1984), *Quantum cryptography: public-key distribution and coin tossing*, Proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore Press (India), pp. 175-179.
2. N. Gisin, G. Ribordy, W. Tittel, *et al.* (2002), *Quantum cryptography*, Rev. of Mod. Phys., Vol.74, pp. 145-195.
3. A. K. Ekert (1991), *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett., Vol.67, pp. 661-663.
4. C. H. Bennett (1992), *Quantum cryptography using any two nonorthogonal states*, Phys. Rev. Lett., Vol.68, pp. 3121-3124.

5. L. Goldenberg, L. Vaidman (1995), *Quantum Cryptography Based on Orthogonal States*, Phys. Rev. Lett., Vol.75, pp. 1239-1243.
6. B. Huttner, N. Imoto, N. Gisin, *et al.* (1995), *Quantum cryptography with coherent states*, Phys. Rev. A, Vo.51, pp. 1863-1869.
7. M. Koashi, N. Imoto (1997), *Quantum cryptography based on split transmission of one-bit information in two steps*, Phys. Rev. Lett., Vov.79, pp. 2383-2386.
8. F. Gao, F. Guo, Q. Wen, *et al.* (2006), *Quantum key distribution without alternative measurements and rotations*, Phys. Lett. A, Vol.349, pp. 53-58.
9. N. Lütkenhaus (1996), *Security against eavesdropping in quantum cryptography*, Phys. Rev. A, Vol.54, pp. 97-111.
10. H. K. Lo and H. F. Chau (1999), Unconditional security of quantum key distribution over arbitrarily long distances, Science, Vol. 283, pp. 2050-2056.
11. P. W. Shor and J. Preskill (2000), Simple proof of security of the BB84 quantum key distribution scheme, Phys. Rev. Lett., Vol. 85, pp.441-444.
12. D. Gottesman and H. K. Lo (2003), *Proof of security of quantum key distribution with two-way classical communications*, IEEE Transactions on Information Theory, Vol. 49, pp. 457-475.
13. A. Wójcik (2005), *Comment on "Quantum dense key distribution"*, Phys. Rev. A, Vol.71, p. 016301.
14. F. Gao, F. Guo, Q. Wen, *et al.* (2005), *Comment on "Quantum secret sharing based on reusable Greenberger-Horne-Zeilinger states as secure carriers"* Phys. Rev. A, Vol.72, p. 036302.
15. F. Deng, X. Li, H. Zhou, *et al.* (2005), *Improving the security of multiparty quantum secret sharing against Trojan horse attack*, Phys. Rev. A, Vol.72, p. 044302.
16. H. K. Lo and T. M. Ko (2005), *Some attacks on quantum-based cryptographic protocols*, Quantum Inf. Comput., Vol.5, pp. 40-47.
17. M. Hillery, V. Buzěk and A. Berthiaume (1999), *Quantum secret sharing*, Phys. Rev. A, Vol.59, pp.1829-1834.
18. R. Cleve, D. Gottesman, H. K. Lo (1999), *How to share a quantum secret*, Phys. Rev. Lett., Vol.83, pp. 648-651.
19. H. Imai, J. Mueller-Quade, A.C.A. Nascimento, P. Tuyls and A. Winter (2005), *An information theoretical model for quantum secret sharing schemes*, Quantum Inf. Comput., Vol.5, pp. 68-80.
20. F. Yan, T. Gao (2005), *Quantum secret sharing between multiparty and multiparty without entanglement*, Phys. Rev. A, Vol.72, p. 012304.
21. K. Brádler and M. Dušek (2004), *Secret-message sharing via direct transmission*, J. Opt. B: Quantum Semiclass. Opt., Vol.6, pp. 63-68.
22. M. Żukowski, A. Zeilinger, M. A. Horne and A. K. Ekert (1993), *"Event-ready-detectors" Bell experiment via entanglement swapping*, Phys. Rev. Lett., Vol.71, pp. 4287-4290.
23. Y. Zhang, C. Li and G. Guo (2001), *Comment on "Quantum key distribution without alternative measurements"*, Phys. Rev. A, Vol.63, 036301.
24. S. Qin, F. Gao, Q. Wen, *et al.* (2006), *Improving the security of multiparty quantum secret sharing against an attack with a fake signal*, Phys. Lett. A, Vol.357, pp. 101-103.
25. F. Gao, Q. Wen and F. Zhu (2007), *Comment on: "Quantum exam" [Phys. Lett. A 350 (2006) 174]*, Phys. Lett. A, Vol.360, pp. 748-750.