International Journal of Theoretical Physics (2018) 57: 3651–3657
https://doi.org/10.1007/s10773-018-3878-0

New Probabilistic Quantum Key Distribution Protocol

Chun-Wei Yang[1,2]

Received: 5 June 2018 / Accepted: 28 August 2018 / Published online: 3 September 2018

Abstract
On the basis of entanglement swapping of Bell states, Hwang et al. proposed a probabilistic quantum key distribution (PQKD) protocol Hwang et al. (Quantum Inf. Comput. **11**(7-8), 615–637 2011). Recently, Lin et al. (Quantum Inf. Comput. **14**(9-10), 757–762 2014) proposed a unitary operation attack on Hwang et al.'s PQKD. However, unlike the unitary operation attack, this work points out that a malicious participant in Hwang et al.'s PQKD protocol can manipulate the secret key. As a result, the security requirements of a PQKD protocol, i.e., fairness, cannot be satisfied in their protocol. Moreover, the same attack can also crack the fairness requirement of the existing quantum key agreement (QKA) protocols. To overcome both problems, this paper proposes a new PQKD protocol based on the order rearrangement of the transmitted photons. Furthermore, the rearrangement method can also solve the key manipulation attack in QKA protocols.

Keywords Key manipulation problem · Quantum cryptography · Quantum key distribution · Quantum key agreement · Probabilistic quantum key distribution

1 Introduction

Quantum key distribution (QKD), which allows a sender to distribute a pre-determined secret key to a receiver through the transmission of quantum signals, is one of the most important research topics in quantum cryptography. Since the first QKD protocol was presented by Bennett and Brassard [1] in 1984 (also known as BB84), a variety of QKD protocols have been proposed [2–19]. Although the QKD protocols provide unconditional security [20, 21], they must assume that the participants are mutually trusted [22]. That is, they always follow the protocol and one participant must accept the key decided by the other participant.

✉ Chun-Wei Yang
cwyang@mail.cmu.edu.tw

[1] Center for General Education, China Medical University, Taichung 40402, Taiwan

[2] College of Humanities and Sciences, China Medical University, Taichung 40402, Taiwan

In contrast to the QKD protocols, the participants in a quantum key agreement (QKA) and a probabilistic quantum key distribution (PQKD) are assumed to be mutually untrusted. A QKA protocol [23–27] is one whereby two or more participants negotiate a key over quantum channels and classical channels on the basis of their exchanged messages. Unlike QKA protocols, Hwang et al. [28] proposed the first PQKD protocol using Bell states and entanglement swapping, where two mutually suspicious participants can share an unpredictable key based on quantum mechanics. The PQKD protocol has the following features:

1. Unpredictability: The key distributed is an unpredictable key.
2. Fairness: No one can pre-determine the key even with a single bit advantage.
3. Effectiveness: The intrinsic measurement uncertainty and entanglement swapping of photons are applied to facilitate the generation as well as distribution of a random key.

Recently, Lin et al. [29] proposed a unitary operation attack on Hwang et al.'s PQKD protocol. One malicious participant can manipulate the secret key by using the unitary operation attack without being detected. However, unlike the unitary operation attack, this paper reveals a common problem in these QKA protocols [23–27] and the PQKD protocol [28]. The problem further enables a key manipulation attack that threatens the security of these protocols. This study takes Hwang et al.'s PQKD protocol [28] as an example to show the key manipulation problem. That is, a legitimate but malicious participant can manipulate the secret key.

In order to avoid the unitary operation attack and the key manipulation attack, this paper proposes a new PQKD protocol using the entanglement swapping of Bell states and reordering of the transmitted qubits. Therefore, the malicious participant cannot obtain the correct secret key by performing a unitary operation attack and a key manipulation attack. Finally, two untrusted participants generate a random fairness secret key by using the entanglement swapping of Bell states.

The rest of this paper is organized as follows. Section 2 introduces Bell states and the entanglement swapping of Bell states. Section 3 reviews Hwang et al.'s PQKD protocol. Section 4 discusses the key manipulation problem of Hwang et al.'s protocol. Section 5 describes the proposed PQKD protocol. Section 6 analyzes the security and the fairness of the proposed PQKD protocol. Finally, Section 7 concludes our results.

2 Background

The Einstein-Podolsky-Rosen (EPR) pair, also called the Bell state, is a two-particle quantum entangled state. It can be described by four orthogonal maximal states as follows:

$$\left|\phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) = \frac{1}{\sqrt{2}}\left(|{+}{+}\rangle + |{-}{-}\rangle\right)$$

$$\left|\phi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) = \frac{1}{\sqrt{2}}\left(|{+}{-}\rangle + |{-}{+}\rangle\right)$$

$$\left|\psi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) = \frac{1}{\sqrt{2}}\left(|{+}{+}\rangle - |{-}{-}\rangle\right)$$

$$\left|\psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) = \frac{1}{\sqrt{2}}\left(|{+}{-}\rangle - |{-}{+}\rangle\right)$$

The entanglement swapping is shown in Table 1. Suppose that Alice and Bob prepare Bell states $\left|\phi^{+}\right\rangle$, respectively. Then, they exchange the second qubit of $\left|\phi^{+}\right\rangle$ and perform

Table 1 The entanglement swapping of Bell states

Initial state of Bell state	Possible results of entanglement swapping
$(\|\phi^+\rangle_{12}, \|\phi^+\rangle 34), (\|\phi^-\rangle_{12}, \|\phi^-\rangle_{34})$, $(\|\psi^+\rangle_{12}, \|\psi^+\rangle_{34}), (\|\psi^-\rangle_{12}, \|\psi^-\rangle_{34})$	$(\|\phi^+\rangle_{13}, \|\phi^+\rangle_{24}), (\|\phi^-\rangle_{13}, \|\phi^-\rangle_{24})$, $(\|\psi^+\rangle_{13}, \|\psi^+\rangle_{24}), (\|\psi^-\rangle_{13}, \|\psi^-\rangle_{24})$
$(\|\phi^-\rangle_{12}, \|\phi^+\rangle_{34}), (\|\phi^+\rangle_{12}, \|\phi^-\rangle_{34})$, $(\|\psi^-\rangle_{12}, \|\psi^+\rangle_{34}), (\|\psi^+\rangle_{12}, \|\psi^-\rangle_{34})$	$(\|\phi^+\rangle_{13}, \|\phi^-\rangle_{24}), (\|\phi^-\rangle_{13}, \|\phi^+\rangle_{24})$, $(\|\psi^+\rangle_{13}, \|\psi^-\rangle_{24}), (\|\psi^-\rangle_{13}, \|\psi^+\rangle_{24})$
$(\|\psi^+\rangle_{12}, \|\phi^+\rangle_{34}), (\|\phi^-\rangle_{12}, \|\psi^-\rangle_{34})$, $(\|\phi^+\rangle_{12}, \|\psi^+\rangle_{34}), (\|\phi^-\rangle_{12}, \|\psi^-\rangle_{34})$	$(\|\phi^+\rangle_{13}, \|\psi^+\rangle_{24}), (\|\phi^-\rangle_{13}, \|\psi^-\rangle_{24})$, $(\|\psi^+\rangle_{13}, \|\phi^+\rangle_{24}), (\|\psi^-\rangle_{13}, \|\phi^-\rangle_{24})$
$(\|\psi^-\rangle_{12}, \|\phi^+\rangle_{34}), (\|\psi^+\rangle_{12}, \|\phi^-\rangle_{34})$, $(\|\phi^-\rangle_{12}, \|\psi^+\rangle_{34}), (\|\phi^+\rangle_{12}, \|\psi^-\rangle_{34})$	$(\|\phi^+\rangle_{13}, \|\psi^-\rangle_{24}), (\|\psi^-\rangle_{13}, \|\phi^+\rangle_{24})$, $(\|\psi^+\rangle_{13}, \|\phi^-\rangle_{24}), (\|\psi^-\rangle_{13}, \|\phi^+\rangle_{24})$

the Bell measurement on their first qubit and the received second qubit. After that, one of the following four measurement results, $\{(|\phi^+\rangle_{a1b2}, |\phi^+\rangle_{b1a2}), (|\phi^-\rangle_{a1b2}, |\phi^-\rangle_{b1a2}), (|\psi^+\rangle_{a1b2}, |\psi^+\rangle_{b1a2}), (|\psi^-\rangle_{a1b2}, |\psi^-\rangle_{b1a2})\}$, appears randomly. It is obvious that Alice and Bob can derive the same unitary operation, which transforms the initial state to the measurement result.

3 Review of Hwang et al.'s PQKD Protocol

Alice and Bob, two mutually untrusted communicants, wish to share a fair n-bit random key by using the entanglement swapping of Bell states. Let the four Bell states $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$ and $|\Psi^-\rangle$ represent two-bit information "00," "01," "10," and "11," respectively. Here, the classical communication channels are assumed to be authenticated, and the quantum channels are assumed to be ideal. The PQKD protocol proceeds as follows:

Step 1. Alice generates a sequence of n Bell states in $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$,$S = \{s_1,s_2,\ldots,s_n\}$, where $s_i = \{q^i_{A1}, q^i_{A2}\}$,$i$ = 1,2,…,n. She takes the second qubit to form a new sequence $S_B = \{q^i_{A2}\}$, and the first qubit to form the other sequence $S_A = \{q^i_{A1}\}$, for i = 1,2,…,n. Then, Alice arbitrarily performs a Hadamard operation H $(= \frac{1}{\sqrt{2}}[(|0\rangle + |1\rangle)\langle 0| + (|0\rangle - |1\rangle)\langle 1|])$ or an identity operation I $(= |0\rangle\langle 0| + |1\rangle\langle 1|)$ on $S_B = \{q^i_{A2}\}$ to form a new sequence $S'_B = \{q'^i_{A2}\}$, and then sends it to Bob.

Step 2 Upon receiving $S'_B = \{q'^i_{A2}\}$, Bob also generates a sequence of n Bell states in $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$,$T = \{t_1,t_2,\ldots,t_n\}$, where $t_i = \{q^i_{B1}, q^i_{B2}\}$,$i$= 1,2,…,$n$. He takes the second qubit to form a new sequence $T_B = \{q^i_{B2}\}$, and the first qubit to form the other sequence $T_A = \{q^i_{B1}\}$, for i = 1,2,…,n. He performs a permutation π on $T_A = \{q^i_{B1}\}$ to form a new sequence $T'_A = \{q'^i_{B1}\}$ and then sends it to Alice.

Step 3 Alice randomly chooses j positions as a check set C for an eavesdropping check. Then, she performs H on $S_A = \{q^i_{A1}\}$, for which the corresponding $S_B = \{q^i_{A2}\}$ were performed with the same H in Step 1. After that, she announces the positions of C to Bob through an authenticated classical channel.

Step 4 Bob derives the $2n$-bit raw key by performing a Bell measurement on $S_B = \{q^i_{A2}\}$ and $T_B = \{q^i_{B2}\}$, i.e., $K_{BA} = \{BM(q^1_{A2}, q^1_{B2}), BM(q^2_{A2}, q^2_{B2}), K, BM(q^n_{A2}, q^n_{B2})\}$.

Then, he sends π and the Bell measurement results K_C of C to Alice through an authenticated classical channel. He derives the key as $K = K_{BA} - K_C$. Let K be the remaining bits in K_{BA} after removing the checking bits in K_C.

Step 5 Alice recovers $T_A = \{q^i_{B1}\}$ from $T'_A = \{q'^i_{B1}\}$ on the basis of the π and derives the $2n$-bit raw key as $K_{AB} = \{BM(q^1_{A1}, q^1_{B1}), BM(q^2_{A1}, q^2_{B1}), K, BM(q^n_{A1}, q^n_{B1})\}$. It is noted that $K_{AB} = K_{BA}$. According to K_C received from Bob and that measured by Alice herself, Alice can detect the presence of eavesdropping. If there is no eavesdropper, then she sets $K = K_{AB} - K_C$ as the key shared with Bob. Otherwise, they abort the process and start a new one.

It appears that neither Alice nor Bob can manipulate the outcome of the shared key K, because the result of entanglement swapping is unpredictable. However, this paper reveals in the following section that Bob can determine one key bit completely.

4 Key Manipulation Problem

The PQKD protocol is in a mutually untrusted environment where Alice and Bob are mutually opposed to each other. Several problems could arise from the PQKD protocol if the public discussion is not carefully designed. These are explained in the following example.

Suppose that the first bit of the raw key between Alice and Bob in Step 4 is "0." If Bob prefers the first bit of the raw key to be "0," then he will follow the protocol. If, however, Bob prefers the first bit of the raw key to be "1," then he can send an incorrect KC as his fake Bell measurement result C to Alice for public discussion, which will fail eventually. Hence, they will abort the process in Step 5 and start a new one until the first bit of the raw key is "1." Accordingly, Bob could manipulate the first bit of the raw key through the public discussion, even though the unpredictability in the Bell state entanglement swapping is applied to generate and distribute the key. Thus, the PQKD protocol fails to provide "fairness" between both participants because one bit of the final shared key can be determined by the participant who first knows the raw key of the other. The same problem can also be identified in the QKA protocols described in [23–27].

5 The Proposed PQKD Protocol

To solve the unitary operation attack and key manipulation attack, this section introduces a new PQKD protocol. Suppose that two untrusted participants, Alice and Bob, want to distribute an unpredictable key K^M_P by a quantum channel. Here, the classical channels are assumed to be authenticated, and the quantum channels are ideal.

Step 1 Alice prepares n Bell states randomly chosen from $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$. She takes all of the first qubits and second qubits from each Bell state to form the ordered sequences S_{A1} and S_{A2}, respectively; then, Alice shuffles S_{A2} to obtain S'_{A2}. Alice generates n decoy photons arbitrarily chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and then randomly inserts these decoy photons into S'_{A2} to form S'^*_{A2}. Similarly, Bob can produce S_{B1} and S'^*_{B2} in the same way. Finally, Alice delivers S'^*_{A2} to Bob.

Step 2 After Bob receives the sequences sent from Alice, Alice announces the measurement positions and the bases of the decoy photons in S'^{*}_{A2}. According to the measurement results of decoy photons replied from Bob, Alice can check the existence of eavesdroppers. If there is no eavesdropper, she sends an acknowledgment to Bob through an authenticated classical channel. Otherwise, they abort the process and start a new one. Similarly, Bob sends S'^{*}_{B2} to Alice and performs the eavesdropping check.

Step 3 After the eavesdropping check, Alice has two sequences S_{A1} and S'_{B2}, and Bob also has two sequences S_{B1} and S'_{A2}. Bob announces his shuffled information. According to the shuffled information sent from Bob, Alice can recover S'_{B2} into the correct order of S_{B2}. Then, Alice performs the Bell measurement on S_{A1} and S_{B2} to obtain $2n$ bits of an unpredictable key K_P, where the K_P is "00" if the unitary operation is I, "01" if σ_z, "10" if σ_x, and "11" if $i\sigma_y$.

Step 4 After Alice obtains the unpredictable key K_P, she announces her shuffled information of S'_{A2}. Then, Bob also can recover the correct order of S_{A2} and performs the Bell measurement on S_{B1} and S_{A2} to obtain an unpredictable key K_P.

According to Section 2, Alice and Bob can obtain the same unpredictable key K_P. Furthermore, neither one can manipulate the unpredictable key K_P.

6 Security Analysis

In this section, we discuss the security and the fairness of the proposed PQKD protocol. The security of the proposed PQKD protocol is analyzed from the eavesdropping attack, Lin et al.'s unitary operation attack [29], and the key manipulation problem.

6.1 The Eavesdropping Attack

In order to avoid the eavesdropping attack, two untrusted participants use enough decoy photons, which are randomly generated from one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Then, they randomly insert these decoy photons in their transmitted sequences. Because an eavesdropper does not know the bases and the positions of the decoy photons, an eavesdropper is detected in public discussion when he or she tries to measure and resend the quantum sequences. The probability of detecting an eavesdropper is $1-(\frac{3}{4})^d$, where $\frac{3}{4}$ is the probability that an eavesdropper can pass the eavesdropping check in each decoy photon, and d is the total number of decoy photons. Therefore, if d is large enough, the probability $1-(\frac{3}{4})^d$ will be close to 1.

6.2 Lin et al.'s Unitary Operation Attack

In Lin et al.'s attack, the malicious communicant, e.g., Bob, can perform unitary operations on the qubits sent from Alice and resend these qubits to Alice to manipulate the secret key. However, in the proposed PQKD protocol, Alice shuffles her transmitted qubits S_{A2} to S'_{A2} in Step 1. Then, she asks Bob to announce his order first in Step 3. Because Bob does not know the correct order of S'_{A2} before Step 4, he cannot manipulate the secret key by performing unitary operations on S'_{A2} and resending to Alice. Therefore, the proposed protocol does not enable this attack.

6.3 Key Manipulation Problem

In order to avoid the key manipulation problem, Alice and Bob shuffle their transmitted qubits in Step 1 and Step 2. Because the measurement results are unpredictable on two different EPR pairs, the malicious communicant cannot obtain the correct secret key by performing the Bell measurement in public discussion. Therefore, the malicious participant does not deliver the fake measurement results in public discussion. The proposed PQKD protocol is fair under the key manipulation problem.

7 Conclusions

This study showed that there is a key manipulation problem in the QKA protocols and the PQKD protocol. Moreover, in order to avoid Lin et al.'s unitary operation attack [29] and the key manipulation problem, this paper proposes a new PQKD protocol based on the entanglement swapping of Bell states and order rearrangement of the transmitted photons. It also can avoid the eavesdropping attack by using decoy photons. Because the fairness of the proposed PQKD protocol is based on the order rearrangement of the transmitted photons, the PQKD protocol might be unsecure if the bit length of the shared key is too short. Therefore, how to design a secure PQKD protocol without this problem will be an interesting topic of future research.

Acknowledgments This research was partially supported by the Ministry of Science and Technology, Taiwan, R.O.C., under the Contract No. MOST 106-2218-E-039-002-MY3, and also was partially supported by China Medical University under the Contract No. CMU106-N-07.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE international conference on computers systems and signal processing (1984)
2. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**(21), 3121–3124 (1992)
3. Braunstein, S.L., Pirandola, S.: Side-channel-free quantum Key distribution. Phys. Rev. Lett. **108**(13), 130502 (2012)
4. Chen, P., Li, Y.S., Deng, F.G., Long, G.L.: Measuring-basis encrypted quantum key distribution with four-state systems. Commun. Theor. Phys. **47**(1), 49–52 (2007)
5. Deng, F.G., Long, G.L., Wang, Y., Xiao, L.: Increasing the efficiencies of random-choice-based quantum communication protocols with delayed measurement. Chinese Phys. Lett. **21**(11), 2097–2100 (2004)
6. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**(6), 661–663 (1991)
7. Gao, G.: Quantum key distribution by comparing Bell states. Opt. Commun. **281**(4), 876–879 (2008)
8. Hwang, T., Hwang, C.C., Tsai, C.W.: Quantum key distribution protocol using dense coding of three-qubit W state. Eur. Phys. J. D. **61**(3), 785–790 (2011)
9. Hwang, T., Lee, K.C.: EPR Quantum key distribution protocols with potential 100% qubit efficiency. Iet Inform. Secur. **1**(1), 43–45 (2007)
10. Hwang, T., Lee, K.C., Li, C.M.: Provably secure three-party authenticated quantum key distribution protocols. IEEE T Depend Secure **4**(1), 71–80 (2007)
11. Li, X.H., Deng, F.G., Zhou, H.Y.: Efficient quantum key distribution over a collective noise channel. Phys. Rev. A **78**(2), 022321 (2008)
12. Li, X.H., Zhao, B.K., Sheng, Y.B., Deng, F.G., Zhou, H.Y.: Fault tolerant quantum key distribution based on quantum dense coding with collective noise. Int. J. Quant. Infor. **7**(8), 1479–1489 (2009)

13. Li, X.-H., Duan, X.-J., Deng, F.-G., Zhou, H.-Y.: Error-Rejecting Bennett–Brassard–Mermin Quantum key distribution protocol based on linear optics over a Collective-Noise channel. Int. J. Quantum. Inf. **08**(07), 1141–1151 (2010)
14. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**(3), 032302 (2002)
15. Pirandola, S., Garcia-Patron, R., Braunstein, S.L., Lloyd, S.: Direct and rever se secret-key capacities of a quantum channel. Phys. Rev. Lett. **102**(5), 050503 (2009)
16. Shih, H.C., Lee, K.C., Hwang, T.: New efficient Three-Party quantum key distribution protocols. IEEE J. Sel. Top Quant. **15**(6), 1602–1606 (2009)
17. Yuan, H., Song, J., Han, L.F., Hou, K., Shi, S.H.: Improving the total efficiency of quantum key distribution by comparing Bell states. Opt. Commun. **281**(18), 4803–4806 (2008)
18. Zhang, Z.J., Man, Z.X., Shi, S.H.: An efficient multiparty quantum key distribution scheme. Int. J. Quant. Infor. **3**(3), 555–560 (2005)
19. Zhao, B.K., Sheng, Y.B., Deng, F.G., Zhang, F.S., Zhou, H.Y.: Stable and deterministic quantum key distribution based on differential phase shift. Int. J. Quantum Inf. **7**(4), 739–745 (2009)
20. Lo, H.K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. Science **283**(5410), 2050–2056 (1999)
21. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**(2), 441–444 (2000)
22. Ben-Or, M., Horodecki, M., Leung, D.W., Mayers, D., Oppenheim, J.: The universal composable security of quantum key distribution. Theory of Cryptography Proceedings **3378**, 386–406 (2005)
23. Zhou, N., Zeng, G., Xiong, J.: Quantum key agreement protocol. Electron Lett. **40**(18), 1149–1150 (2004)
24. Chong, S.K., Hwang, T.: Quantum key agreement protocol based on BB84. Opt. Commun. **283**(6), 1192–1195 (2010)
25. Chong, S.K., Tsai, C.W., Hwang, T.: Improvement on Quantum key agreement protocol with maximally entangled states. Int. J. Theor. Phys. **50**(6), 1793–1802 (2011)
26. Shi, R.H., Zhong, H.: Multi-party quantum key agreement with bell states and bell measurements. Quantum Inf. Process **12**(2), 921–932 (2013)
27. Liu, B., Gao, F., Huang, W., Wen, Q.Y.: Multiparty quantum key agreement with single particles. Quantum Inf. Process **12**(4), 1797–1805 (2013)
28. Hwang, T., Tsai, C.W., Chong, S.K.: Probabilistic quantum key distribution. Quantum Inf. Comput. **11**(7-8), 615–637 (2011)
29. Lin, T.-H., Yang, C.-W., Hwang, T.: Unitary operation attack and the improvement on probabilistic quantum key distribution. Quantum Inf. Comput. **14**(9-10), 757–762 (2014)