Quantum Information and Computation, Vol. 11, No. 7&8 (2011) 0615–0637

PROBABILISTIC QUANTUM KEY DISTRIBUTION

TZONELIH HWANG*, CHIA-WEI TSAI, SONG-KONG CHONG
Department of Computer Science and Information Engineering
National Cheng Kung University
No.1, Ta-Hsueh Road, Tainan City 701, Taiwan (R.O.C.)

Received October 13, 2010
Revised May 5, 2011

This work presents a new concept in quantum key distribution called the probabilistic quantum key distribution (PQKD) protocol, which is based on the measurement uncertainty in quantum phenomena. It allows two mutually untrusted communicants to negotiate an unpredictable key that has a randomness guaranteed by the laws of quantum mechanics. In contrast to conventional QKD (e.g., BB84) in which one communicant has to trust the other for key distribution or quantum key agreement (QKA) in which the communicants have to artificially contribute subkeys to a negotiating key, PQKD is a natural and simple method for distributing a secure random key. The communicants in the illustrated PQKD take Einstein-Podolsky-Rosen (EPR) pairs as quantum resources and then use entanglement swapping and Bell-measurements to negotiate an unpredictable key.

Keywords: Quantum Information; Quantum Cryptography; Quantum Key Agreement; Quantum Key Distribution.
Communicated by: S Braunstein & H Zbinden

1. Introduction

Quantum key distribution (QKD) is a method for distributing a secret key to two remote parties over insecure quantum channels [1, 2]. Since the first QKD protocol presented by Bennnett and Brassard [3] in 1984 (also known as BB84), a variety of QKD protocols have been proposed [4, 5, 6, 7, 8, 9, 10, 11, 12, 13].

Essentially, in a QKD (e.g., BB84), a secret key is determined by one communicant (Alice) and then distributed to the other communicant (Bob) through the transmission of quantum signals. Although a QKD can be unconditionally secure [14, 15, 16, 17, 18], it assumes that the communicants are mutually trusted and honest [19], i.e., that they always follow the protocol and must accept the key decided by the other communicant.

Consider a scenario in which two mutually-opposed countries, e.g., South Korea and North Korea, plan to hold a military negotiation without the involvement or interference of other countries. In this situation, they wish to establish a secret key in order to secure their subsequent communications. However, neither wishes the secret key to be pre-determined by the other. They are interested in "fairness" in determining the key; neither would want even one single bit of advantage to go to the other.

*Electronic address: hwangtl@ismail.csie.ncku.edu.tw (corresponding author)

A very intuitive solution for the above scenario is to run a QKD twice, e.g., South Korea and North Korea individually decide their raw keys, given as K_S and K_N respectively, and then exchange these keys separately using two QKD runs. The final key shared then is $K_{SN} = K_S \oplus K_N$, where "$\oplus$" denotes addition modulo 2 of two classical bit strings. Unfortunately, this intuitive idea fails to provide "fairness" to both countries because the final key can be determined by the country that first learns the raw key of the other. For instance, if the raw key K_S of South Korea is distributed to North Korea first using the first QKD, then North Korea can unilaterally decide a final shared key $\widehat{K}_{SN}$ by choosing its raw key, as $K_N = \widehat{K}_{SN} \oplus K_S$, or vice versa.

Recently, quantum key agreement (QKA) has been studied by [1, 20, 21, 22, 23, 24]. Communicants in a QKA are assumed to be mutually untrusted. Indeed, this method could provide a solution to the above mentioned scenario. However, for a party to contribute a subkey to a negotiating key, the subkey of that party must be artificially injected into an already inherently unpredictable quantum phenomenon. This, unfortunately, destroys the property of uncertainty in photons. Instead, this study tries to explore the useful nature of unpredictability in the entanglement swapping of quantum states as a way of generating and distributing an unpredictable key spontaneously. We aim to use this property to facilitate the distribution of an unpredictable key between two communicants. In some sense, one can also treat the key in a QKD as essentially decided by one communicant; and the key in a QKA decided cooperatively by both communicants, whereas that of a PQKD is determined by God.

Though there are QKDs, e.g., [25, 26], which have already exploited the measurement uncertainty in quantum phenomena to distribute a random key, these protocols are, essentially, QKD protocols, i.e., they assume that the communicants are mutually trusted and honest. Otherwise, as in BBM92 [25], if a communicant, say Alice, is malicious, then she can determine a secret key independently and then distribute it to Bob by selecting only those single photons that are polarized $|0\rangle, |1\rangle, |+\rangle$, or $|-\rangle$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Although she does not know which of the transmitted photons will be used as key bits and which will be used in the public discussion, in an extreme case, Alice can independently set the distributed photons to be all $|0\rangle$ states or all $|+\rangle$ states (decoded as the classical bit "0"). In this way, Alice can determine the shared key completely.

Similarly, in Deng et al.'s QKD protocol [26], although the shared key is derived randomly from a quantum mechanism, a malicious communicant can still manipulate that key by selecting those unwanted key bits for public discussion and the remaining bits as the shared secret key. Accordingly, these QKDs, though they promisingly applied the uncertainty of photons in their designs, cannot not be used to solve the problem in the above mentioned scenario as they are not designed from the very beginning for use in the mutually-untrusted environment, and thus, they have failed to incorporate "fairness" into their designs.

To summarize the above discussion, the newly proposed probabilistic quantum key distribution (PQKD) protocol has the following features:

1. "Unpredictability": Two mutually-untrusted communicants are allowed to negotiate an unpredictable key.

2. "Fairness": No one can pre-determine the key with even a single-bit advantage.

3. "Effectiveness": The intrinsic measurement uncertainty as well as entanglement swapping of photons are applied to facilitate the generation, as well as the distribution, of an unpredictable key.

The rest of this paper is as follows. Section 2 introduces the background including the entanglement swapping of EPR pairs and the Hadamard transformation which will be used to construct a PQKD. Then, a PQKD protocol is proposed in Section 3. The security analysis is given in Section 4. Section 5 concludes our result.

2. Background

In this section, the entanglement swapping of EPR pairs is first introduced, then the Hadamard transformation is presented in Section 2.2.

2.1. *The Entanglement Swapping of EPR pairs*

Entanglement is one of the most fascinating phenomena in quantum mechanics: whatever happens to one of the entangled particles has an instantaneous influence on the other, regardless of the distance between the particles. When two pairs of independent entangled particles, e.g., pair 1-2 and pair 3-4, are prepared, if the first particles of these two pairs (e.g., particle 1 and 3) are subject to a Bell-measurement, the remaining two particles (2 and 4) will automatically collapse into the entangled state. This attractive phenomenon is the so-called entanglement swapping, which was originally proposed by Zukowski et al. [27] and experimentally realized by Pan et al. [28].

In Einstein-Podolsky-Rosen (EPR) pairs, there are four maximally entangled states that can be used to perform entanglement swapping:

$$\begin{aligned} |\phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \\ |\psi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \end{aligned}$$

Suppose that Alice and Bob share two EPR pairs in the form

$$\begin{aligned} |\phi^{+}\rangle_{h_A t_A} &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{h_A t_A}, \\ |\phi^{+}\rangle_{h_B t_B} &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{h_B t_B}, \end{aligned}$$

e.g., Alice holds photons h_A and t_B of these EPR pairs, and Bob holds photons t_A and h_B. If Alice performs a Bell-measurement on h_A and t_B (denoted by $BM(h_A, t_B)$) and obtains $|\phi^{+}\rangle_{h_A t_B}$, she can deduce that Bob would also obtain $|\phi^{+}\rangle_{t_A h_B}$ if he performed a Bell-measurement on t_A and h_B. Eq. (1) shows the entanglement swapping of $|\phi^{+}\rangle_{h_A t_A}$ and $|\phi^{+}\rangle_{h_B t_B}$

$$\begin{aligned} |\phi^{+}\rangle_{h_A t_A} \otimes |\phi^{+}\rangle_{h_B t_B} &= \frac{1}{2}(|\phi^{+}\rangle_{h_A t_B} \otimes |\phi^{+}\rangle_{t_A h_B} + |\phi^{-}\rangle_{h_A t_B} \otimes |\phi^{-}\rangle_{t_A h_B} \\ &\quad + |\psi^{+}\rangle_{h_A t_B} \otimes |\psi^{+}\rangle_{t_A h_B} + |\psi^{-}\rangle_{h_A t_B} \otimes |\psi^{-}\rangle_{t_A h_B}). \end{aligned} \tag{1}$$

Similarly, Bob can deduce Alice's result from his Bell-measurement result via Eq. (1) without needing any further information from Alice.

Equation (1) shows that the Bell-measurements of Alice and Bob on (h_A, t_B) and (t_A, h_B), respectively, will result in one of the four measurement results $(|\phi^+\rangle_{h_At_B} \otimes |\phi^+\rangle_{t_Ah_B})$, $(|\phi^-\rangle_{h_At_B} \otimes |\phi^-\rangle_{t_Ah_B})$, $(|\psi^+\rangle_{h_At_B} \otimes |\psi^+\rangle_{t_Ah_B})$ and $(|\psi^-\rangle_{h_At_B} \otimes |\psi^-\rangle_{t_Ah_B})$ with equal probability (i.e., 25%). As these measurement results are completely unpredictable, Alice and Bob can use this quantum phenomenon, the entanglement swapping of EPR pairs, to generate and distribute an unpredictable key in a spontaneous manner.

Table 1. The entanglement swapping of $(|\phi^\pm\rangle, |\psi^\pm\rangle)$.

Initial states of EPR pairs	After entanglement swapping
$(\|\phi^+\rangle, \|\phi^+\rangle)_{h_At_A,h_Bt_B}$ $[(\|\phi^-\rangle, \|\phi^-\rangle)$, $(\|\psi^+\rangle, \|\psi^+\rangle), (\|\psi^-\rangle, \|\psi^-\rangle)]_{h_At_A,h_Bt_B}$	$[(\|\phi^+\rangle, \|\phi^+\rangle), (\|\phi^-\rangle, \|\phi^-\rangle)$ $(\|\psi^+\rangle, \|\psi^+\rangle), (\|\psi^-\rangle, \|\psi^-\rangle)]_{h_At_B,t_Ah_B}$
$(\|\phi^-\rangle, \|\phi^+\rangle)_{h_At_A,h_Bt_B}$ $[(\|\phi^+\rangle, \|\phi^-\rangle)$, $(\|\psi^-\rangle, \|\psi^+\rangle), (\|\psi^+\rangle, \|\psi^-\rangle)]_{h_At_A,h_Bt_B}$	$[(\|\phi^+\rangle, \|\phi^-\rangle), (\|\phi^-\rangle, \|\phi^+\rangle)$ $(\|\psi^+\rangle, \|\psi^-\rangle), (\|\psi^-\rangle, \|\psi^+\rangle)]_{h_At_B,t_Ah_B}$
$(\|\psi^+\rangle, \|\phi^+\rangle)_{h_At_A,h_Bt_B}$ $[(\|\psi^-\rangle, \|\phi^-\rangle)$, $(\|\phi^+\rangle, \|\psi^+\rangle), (\|\phi^-\rangle, \|\psi^-\rangle)]_{h_At_A,h_Bt_B}$	$[(\|\phi^+\rangle, \|\psi^+\rangle), (\|\phi^-\rangle, \|\psi^-\rangle)$ $(\|\psi^+\rangle, \|\phi^+\rangle), (\|\psi^-\rangle, \|\phi^-\rangle)]_{h_At_B,t_Ah_B}$
$(\|\psi^-\rangle, \|\phi^+\rangle)_{h_At_A,h_Bt_B}$ $[(\|\psi^+\rangle, \|\phi^-\rangle)$, $(\|\phi^-\rangle, \|\psi^+\rangle)]_{h_At_A,h_Bt_B}$	$[(\|\phi^+\rangle, \|\psi^-\rangle), (\|\phi^-\rangle, \|\psi^+\rangle)$ $(\|\psi^+\rangle, \|\phi^-\rangle), (\|\psi^-\rangle, \|\phi^+\rangle)]_{h_At_B,t_Ah_B}$

The entanglement swapping of $(|\phi^\pm\rangle, |\psi^\pm\rangle)$ is summarized in Table 1. For instance, if the initial states of two EPR pairs are $|\phi^-\rangle_{h_At_A}$ and $|\phi^-\rangle_{h_Bt_B}$ (denoted as $(|\phi^-\rangle, |\phi^-\rangle)_{h_At_A,h_Bt_B}$ for simplicity), the results after entanglement swapping would be $(|\phi^+\rangle, |\phi^+\rangle)_{h_At_B,t_Ah_B}$, $(|\phi^-\rangle, |\phi^-\rangle)_{h_At_B,t_Ah_B}$, $(|\psi^+\rangle, |\psi^+\rangle)_{h_At_B,t_Ah_B}$, or $(|\psi^-\rangle, |\psi^-\rangle)_{h_At_B,t_Ah_B}$. Each occurs with equal probability (i.e., 25%). It should be noted that the entanglement swapping of n EPR pairs can also be derived from Table 1. For instance, in the entanglement swapping of three EPR pairs, $|\phi^+\rangle_{h_At_A}, |\phi^+\rangle_{h_Bt_B}$, and $|\phi^+\rangle_{h_Ct_C}$, Alice can first perform a Bell-measurement on (h_A, t_B). If the measurement result is $|\phi^+\rangle_{h_At_B}$, according to Eq. (1), photons t_A and h_B will automatically collapse into $|\phi^+\rangle_{t_Ah_B}$. Then, if Alice performs the Bell-measurement on (t_A, t_C) and obtains $|\psi^-\rangle_{t_At_C}$, the remaining two photons, h_B and h_C, will collapse into $|\psi^-\rangle_{h_Bh_C}$ as well.

2.2. *Hadamard Transformation*

In quantum information processing, the Hadamard transformation (or Hadamard gate) is a function that maps the non-superpositioned qubits $|0\rangle$ and $|1\rangle$ into two superposition states of the computational basis states $|0\rangle$ and $|1\rangle$ with equal weight. For instance, $H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + |1\rangle$, and $H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - |1\rangle$, where H denotes a Hadamard transformation and is defined as follows:

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

The Hadamard transformation is a unitary operation $H^\dagger H = HH^\dagger = I$. When one photon, e.g., t_A, of an EPR pair $|\phi^+\rangle_{h_At_A}$, is subject to a Hadamard operation, $|\phi^+\rangle_{h_At_A}$ is transformed into the state $|\phi^+\rangle^H_{h_At_A}$ as follows:

$$I \otimes H|\phi^+\rangle_{h_A t_A} = |\phi^+\rangle^H_{h_A t_A} = \frac{1}{\sqrt{2}}(|\phi^-\rangle + |\psi^+\rangle)_{h_A t_A}. \quad (2)$$

Therefore, the Bell-measurement of $|\phi^+\rangle^H_{h_A t_A}$ will result in one of the two measurement results, $|\phi^-\rangle_{h_A t_A}$ or $|\psi^+\rangle_{h_A t_A}$, with equal probability (i.e., 50%). However, if a Hadamard operation is performed on the other photon of the same EPR pair, e.g., h_A, of $|\phi^+\rangle^H_{h_A t_A}$ again, then $|\phi^+\rangle^H_{h_A t_A}$ will be transformed back into the original state $|\phi^+\rangle_{h_A t_A}$, i.e.,

$$H \otimes I|\phi^+\rangle^H_{h_A t_A} = |\phi^+\rangle_{h_A t_A}. \quad (3)$$

3. The Proposed PQKD

In this section, an ideal PQKD is demonstrated first. Then, a fair public discussion game used for PQKD is discussed. Finally, an illustrated PQKD protocol is proposed. Here, the classical communication channels are assumed to be authenticated, and the quantum channels are assumed to be noiseless.

3.1. *An Ideal PQKD*

Alice and Bob, two mutually-untrusted communicants, wish to share an unpredictable key, K, using the entanglement swapping of EPR pairs. A simplified version of PQKD proceeds as follows (see also Fig. 1):

Step 1. Alice prepares two EPR pairs, (a_1, a_2) and (a_3, a_4), in the state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Then she sends photons a_1 and a_3 to Bob through a quantum channel.

Step 2. Bob also prepares two EPR pairs, (b_1, b_2) and (b_3, b_4) in the state $|\phi^+\rangle$, and sends b_2 and b_4 to Alice. A raw key can be derived by Bob by entanglement swapping as $K_{BA} = \{BM(a_1, b_1), BM(a_3, b_3)\}$, where BM denotes the Bell-measurement operation.

Step 3. Alice derives the raw key as $K_{AB} = \{BM(a_2, b_2), BM(a_4, b_4)\}$. $K_{AB} = K_{BA}$.

Step 4. Alice and Bob perform public discussions for an eavesdropping check using a portion of the shared key.

Note that the measurement results of Alice and Bob can be used to encode two classical key bits, e.g., $|\phi^+\rangle \Rightarrow 00$, $|\phi^-\rangle \Rightarrow 01$, $|\psi^+\rangle \Rightarrow 10$, and $|\psi^-\rangle \Rightarrow 11$.

It is easy to see that the entanglement swapping of four EPR pairs in $|\phi^+\rangle$ after exchanging photons (a_1, a_3) and (b_2, b_4) enables Alice and Bob to share a four-bit unpredictable key. The ideal PQKD is quite natural and simple in the ideal environment where Alice and Bob are mutually trusted because the measurement uncertainty intrinsic to quantum phenomena is applied to the distribution of an unpredictable key. Unfortunately, we are in a mutually-untrusted environment where Alice and Bob are mutually opposed. Several problems arise from the ideal protocol if the public discussion is not designed carefully. These problems are explained in the following example.

Suppose that the shared key bits between Alice and Bob before Step 4 are "1010," i.e., $K_{AB} = K_{BA} =$ "1010." As mentioned in section 1, a malicious communicant may try to

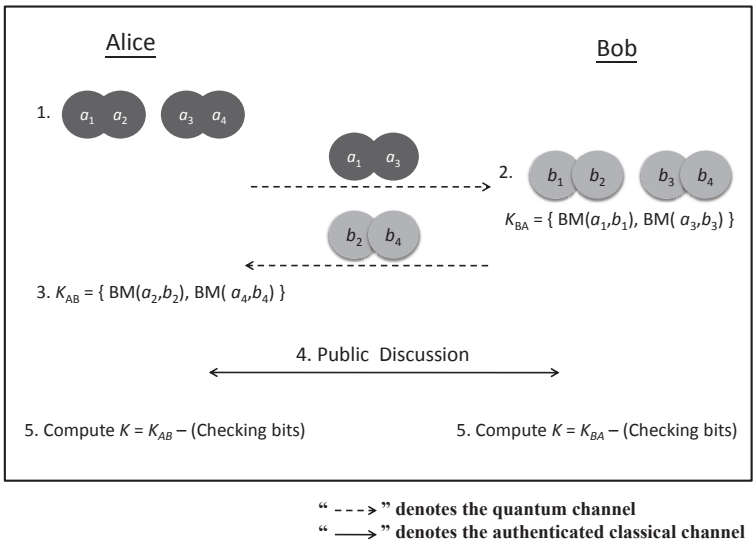

Fig. 1. An Ideal PQKD.

manipulate the key by selecting those unwanted key bits for public discussion and having the remaining bits become the shared secret key. For instance, in our ideal PQKD, if Bob prefers the key to be K_{AB}= "10," then he can select the bits in positions 1 and 2 (or 3 and 4, or 2 and 3) for public discussion and vice versa. Accordingly, Bob can control the final key through the public discussion, even though the unpredictability in the entanglement swapping of quantum is applied to generate and distribute the key. Thus, to achieve the requirement of "fairness," *a fair public discussion game* for PQKD is required (see Fig. 2).

3.2. *Fair Public Discussion Game in PQKD*

To provide "fairness" between two mutually-untrusted communicants in public discussion, a very intuitive solution is to let Alice and Bob decide the checking bits in turn. For instance, after sharing a raw key, one communicant, say Alice, selects the first checking bit first, then Bob selects the second checking bit, and so on, until all of the checking bits are decided and discussed.

This solution (although the number of checking bits selected by Alice and Bob is equal and no one can fully decide the checking bits independently), fails to provide fairness between Alice and Bob because the communicant who selects the final checking bit has a one bit advantage in the final key. For example, Alice and Bob in Fig. 2 take turns selecting two checking bits for public discussion (Step 4). If Bob is the one to select the last checking bit from the remaining shared bits "101," he can set the last bit of the key to be "1" by selecting either the first bit or the second bit for public discussion or set the last bit of the key to be "0" by selecting the third bit for public discussion. Therefore, Bob has a one bit advantage in predicting the outcome of the final shared key. In the following, a PQKD with a proposed fair public discussion game is presented.

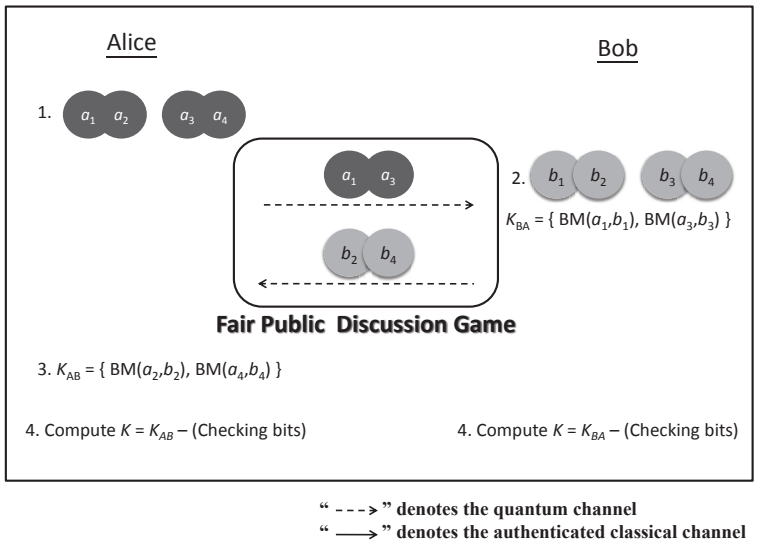

Fig. 2. The PQKD with a fair public discussion game.

3.3. *The Proposed PQKD Protocol*

This section proposes a PQKD protocol that can be applied to a mutually-untrusted environment. A PQKD is defined as follows:

Definition of PQKD: A PQKD protocol is one that allows two mutually-untrusted communicants to share an unpredictable key over public quantum channels. A PQKD protocol is said to be **fair** if no one can predict the outcome of even one bit of the key with more than 50% probability.

The proposed protocol proceeds as follows (see also Fig. 3):

Step 1. Alice prepares n EPR pairs in state $|\phi^+\rangle_{a_{hi}a_{ti}} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{a_{hi}a_{ti}}$, where $1 \leq i \leq n$, $A_h = [a_{h1}, a_{h2}, ..., a_{hn}]$ denotes the sequence of the first photons of these EPR pairs and $A_t = [a_{t1}, a_{t2}, ..., a_{tn}]$ denotes the sequence of the second photons. Thereafter, she randomly chooses some a_{ti}'s (approximately half of them) and applies Hadamard operation, H, on them (denoted as a_{ti}^H's), $1 \leq i \leq n$, and then puts them back into A_t to form a new sequence A_t^H, which is then sent to Bob through a quantum channel. Note that once H operates on a photon a_{ti}, $|\phi^+\rangle_{a_{hi}a_{ti}}$ would transformed into $|\phi^+\rangle_{a_{hi}a_{ti}}^H$.

Step 2. Upon receiving A_t^H, Bob also prepares n EPR pairs in state $|\phi^+\rangle_{b_{hi}b_{ti}} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{b_{hi}b_{ti}}$, where $1 \leq i \leq n$. He likewise prepares two sequences: $B_h = [b_{h1}, b_{h2}, ..., b_{hn}]$ and $B_t = [b_{t1}, b_{t2}, ..., b_{tn}]$. He performs a permutation π on B_t to form a new photon sequence B_t', which is then sent to Alice through the quantum channel.

Step 3. Alice randomly selects m measurement results as a checking set C for public discussion, and then applies the Hadamard operations on those a_{hi}'s, for which the cor-

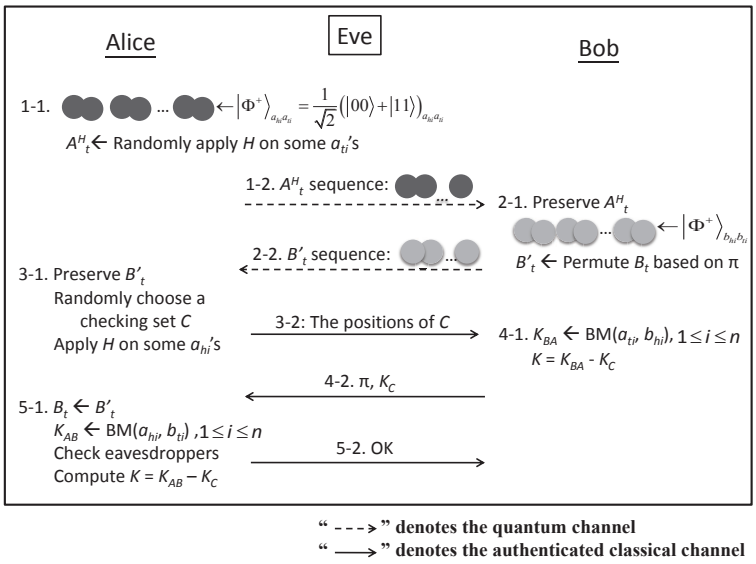

Fig. 3. The proposed PQKD protocol.

responding a_{ti}'s have had the same H as applied in Step 1. According to Eq. (2) and Eq. (3), $|\phi^+\rangle^H_{a_{hi}a_{ti}}$ would now be transformed back into $|\phi^+\rangle_{a_{hi}a_{ti}}$, i.e., the Hadamard operation's effect on a_{ti} in Step 1 would be counteracted (i.e. $a^H_{ti} \Rightarrow a_{ti}$) if a_{hi} is subject to H, where $1 \leq i \leq n$. Thereafter, she announces the positions of the selected m measurement results (i.e., C) to Bob through the authenticated classical channel.

Step 4. Bob derives the $2n$-bit raw key by Bell-measurement of the entanglement-swapped photons as $K_{BA} = \{BM(a_{t1}, b_{h1}), BM(a_{t2}, b_{h2}), ..., BM(a_{tn}, b_{hn})\}$. Next, he sends π, the permutation of B_t, and the measurement results of C, i.e., K_C (which are extracted from K_{BA} based on the positions of the m measurement results decided by Alice in Step 3) to Alice through the authenticated classical channel. He derives the key as $K = K_{BA} - K_C$, i.e., K is the number of remaining bits in K_{BA} after removing those checking bits of K_C.

Step 5. Alice recovers B_t from B'_t based on π and derives the $2n$-bit raw key as $K_{AB} = \{BM(a_{h1}, b_{t1}), BM(a_{h2}, b_{t2}), ..., BM(a_{hn}, b_{tn})\}$. $K_{AB} = K_{BA}$. According to the K_C received from Bob and that measured by Alice independently, Alice can check the presence of eavesdropping. If the result is positive, then she sets $K = K_{AB} - K_C$ (i.e., those remaining bits of K_{AB} after removing the checking bits in K_C) as the key shared with Bob and sends an acknowledgment to Bob through the authenticated classical channel. Otherwise, Alice asks Bob to abort the process and starts a new one.

It should be noted that $K_{AB} = K_{BA} = \{BM(a_{hi}, b_{ti})...\} = \{BM(a_{ti}, b_{hi})...\}$. In the proposed PQKD, Alice can perform a fairness check (in Step 5) through the verification of K_C (see Section 4.3.2). She will abort the protocol if the result is negative. Moreover, if Alice cannot detect Bob's attacks (i.e., control the key) through K_C, then with a high probability they

will share a different key (see also Section 4.3.2). In this situation, a secure communication between Alice and Bob will not be possible. Similarly, if Alice attempts to control the key, there is a high probability that they will share a different key (see Section 4.3.1).

In the proposed PQKD, the sequences A_t and B_t are protected by the Hadamard operation H and the permutation π, respectively. Therefore, no one can obtain the raw key before Step 4. Accordingly, the communicant, Alice, who decides the positions of the checking bits, cannot select unwanted bits (in the raw key K_{AB}) for public discussion. Although Alice can obtain the raw key as $K'_{AB} = BM(a_{hi}, b_{tj})$ in Step 3 without waiting for Bob's π, and then decide a suitable checking set C to control the final key K; her measurement will result in $K'_{AB} \neq K_{BA}$ (see the details of the security analysis in Section 4 below), where $1 \leq i, j \leq n$, and b_{tj} denotes a permuted photon. Since the proposed PQKD is designed from the very beginning for the mutually-untrusted environment, the security analysis below will demonstrate that the proposed PQKD is secure against both disturbance attacks and eavesdropping attacks. Furthermore, no one can predict the outcome of even one bit of $K_{AB} = (K_{BA})$ with more than 50% probability. Thus, the protocol provides fairness in the final key $K(= K_{AB} - K_C)$.

4. Security Analysis

This section analyzes the security of the proposed protocol. The first part focuses on disturbance attacks on the proposed protocol. The second part deals with a security analysis of eavesdropping attacks. The third part analyzes the fairness of the proposed protocol in distributing the key. The related lemmas used for the security analysis are given in the Appendix.

4.1. *Security against Disturbance Attacks*

In the proposed PQKD, an eavesdropper, Eve, may attempt to disrupt the communications between Alice and Bob by inducing a mismatch in the key shared between Alice and Bob without being detected. As a disturbance is usually created before the checking set C has been decided, with a high probability, the inconsistency will be incorporated into C, and thus, will be detected eventually.

Because the Hadamard operation H and the permutation π are used to provide "fairness" between two mutually-untrusted communicants, they will be counteracted by Alice and Bob, respectively, before performing any measurements. For easy recall, Note 1 is given below.

Note 1: In the proposed PQKD, Alice will remove the Hadamard operation's effect on a_{ti}^H's in Step 3 (i.e., $A_t^H \Rightarrow A_t$), and Bob will announce the permutation π of B'_t in Step 4 (i.e., $B'_t \Rightarrow B_t$). A_t is the original A_t^H sent from Alice in Step 1, and B_t is that of B'_t sent from Bob in Step 2.

The following shows that the proposed PQKD protocol is secure against various disturbance attacks.

4.1.1. *Single photon disturbance attack*

According to Note 1, Alice and Bob will exchange sequences A_t and B_t in Steps 1 and

2, respectively. Eve may randomly replace s photons, $1 \leq s \leq n$, in A_t (or B_t) by s single photons $d_i \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, $1 \leq i \leq n$, in hope that she can disturb the key without being detected. Suppose, without loss of generality, that $\frac{s}{2}$ of the attacked photons are selected for public discussion, Theorem 1 shows that the proposed PQKD is secure against the single photon disturbance attack.

Theorem 1: In the proposed PQKD, if Eve attempts to perform the single photon disturbance attack, she will be detected with the probability $1 - (\frac{1}{4})^{\lceil \frac{s}{2} \rceil} \approx 1$, if $s = n$, and n is a large number.

Proof: According to Lemma 5, if Bob performs $BM(d_i, b_{h_i})$, he will obtain one of the four measurement results $\{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle\}_{e_i, b_{h_i}}$ with equal probability (i.e., $\frac{1}{4}$). After Bob's measurement, b_{ti} in Alice's hand will collapse into a single photon. If Alice performs $BM(a_{hi}, b_{ti})$, she will also obtain one of the four measurement results $\{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle\}_{a_{hi}, b_{t_i}}$ with equal probability (i.e., $\frac{1}{4}$). Furthermore, there are four measurement results, $(|\phi^{+}\rangle, |\phi^{-}\rangle, |\psi^{+}\rangle, |\psi^{-}\rangle)$, that would make $BM(d_i, b_{h_i}) = BM(a_{h_i}, b_{t_i})$, therefore, the probability for $BM(d_i, b_{h_i}) = BM(a_{h_i}, b_{t_i})$ would be $\frac{1}{4} \times \frac{1}{4} \times 4 = \frac{1}{4}$. Accordingly, if $\frac{s}{2}$ of the attacked photons are selected for public discussion, then the probability to detect Eve's attack is $1 - (\frac{1}{4})^{\lceil \frac{s}{2} \rceil} \approx 1$, if $s = n$, and n is a large number. Similarly, if Eve randomly replaces s photons in B'_t by polarized single photons, then the probability to detect Eve is also $1 - (\frac{1}{4})^{\lceil \frac{s}{2} \rceil} \approx 1$, if $s = n$, and n is a large number. □

It should be noted that if s is small, then quantum error correcting/detecting codes [29, 30, 31] can be used in this situation.

4.1.2. *Hadamard operation attack*

Eve may also attempt to randomly perform H on s photons, $1 \leq s \leq n$, in A_t (B_t) in hope that she can disturb the key without being detected. Suppose that $\frac{s}{2}$ of the attacked photons are selected for public discussion, Theorem 2 shows that the proposed PQKD is secure against the Hadamard operation attack.

Theorem 2: In the proposed PQKD, if Eve attempts to perform the Hadamard operation attack, she will be detected with the probability $1 - (\frac{1}{2})^{\lceil \frac{s}{2} \rceil} \approx 1$, if $s = n$, and n is a large number.

Proof: Eve's attack can be divided into the following three cases:

- Case 1: Eve randomly performs H on s photons in A_t. If photon a_{ti}, $1 \leq i \leq n$, in A_t is subject to Eve's H (denoted as a_{ti}^H), i.e., $|\phi^{+}\rangle_{a_{hi}a_{ti}} \Rightarrow |\phi^{+}\rangle_{a_{hi}a_{ti}}^H$, and Bob performs $BM(a_{ti}^H, b_{hi})$. According to Lemma 2, Eve's attack must be detected with 100% if the attacked photon is selected for public discussion.
- Case 2: Eve randomly performs H on s photons in B_t. Similar to Case 1, if photon b_{ti}, $1 \leq i \leq n$, in B_t is subject to Eve's H (denoted as b_{ti}^H), i.e., $|\phi^{+}\rangle_{b_{hi}b_{ti}} \Rightarrow |\phi^{+}\rangle_{b_{hi}b_{ti}}^H$, and Alice performs $BM(a_{hi}, b_{ti}^H)$, then Eve's attack must be detected with 100% due to Lemma 2.

- Case 3: Eve randomly performs H on s photons in A_t and B_t. If photons a_{ti} and b_{ti}, $1 \leq i \leq n$, are subject to Eve's H (denoted as a_{ti}^H and b_{ti}^H), i.e., $|\phi^+\rangle_{a_{hi}a_{ti}} \Rightarrow |\phi^+\rangle_{a_{hi}a_{ti}}^H$ and $|\phi^+\rangle_{b_{hi}b_{ti}} \Rightarrow |\phi^+\rangle_{b_{hi}b_{ti}}^H$, and Alice performs $BM(a_{hi}, b_{ti}^H)$, Bob performs $BM(a_{ti}^H, b_{hi})$, then the probability to detect Eve is $\frac{1}{2}$ due to Lemma 3. Accordingly, if $\frac{s}{2}$ of the attacked photons are selected for public discussion, the probability to detect Eve's attack is $1 - (\frac{1}{2})^{\lceil \frac{s}{2} \rceil} \approx 1$, if $s = n$, and n is a large number. □

Similar to Theorem 1, if s is small, then the quantum error correcting/detecting codes [29, 30, 31] can be used to fix the errors.

4.2. *Security against Eavesdropping Attacks*

The following shows several popular attacks which Eve frequently uses to steal the key K shared between Alice and Bob. The probability of the illustrated PQKD to detect these attacks is analyzed.

4.2.1. *Intercept-and-resend attack with three sequences of EPR pairs entanglement swapping*

In this attack, Eve would prepare n EPR pairs in state $|\phi^+\rangle_{e_{hi}e_{ti}} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{e_{hi}e_{ti}}$, where $1 \leq i \leq n$. She divides these EPR pairs into two sequences: $E_h = [e_{h1}, e_{h2}, ..., e_{hn}]$ and $E_t = [e_{t1}, e_{t2}, ..., e_{tn}]$. Then she intercepts A_t^H in Step 1 and instead sends E_t (as a forged A_t^H) to Bob. Similarly, she also intercepts B_t' in Step 2 and sends E_h to Alice. Therefore, the photon sequences in Alice's hand would be (A_h, E_h). Bob holds (E_t, B_h), and Eve would have (A_t^H, B_t'). With this attack, Eve would attempt to obtain the shared key, K, between Alice and Bob without being detected through photons (A_t^H, B_t') in her hand. Suppose that $\frac{n}{2}$ of the attacked photons are selected for public discussion, Theorem 3 shows that the proposed PQKD is secure against the intercept-and-resend attack.

Theorem 3: In the proposed PQKD, if Eve attempts to perform the intercept-and-resend attack, she will be detected with the probability $1 - (\frac{1}{4})^{\lceil \frac{n}{2} \rceil} \approx 1$, if n is a large number.

Proof: In this attack, Eve will intercept A_t^H and B_t' and then replace them by E_t and E_h respectively. In Step 3, Alice will remove the Hadamard operation's effect on A_t^H (now in Eve's hand). And when Eve intercepts the permuted sequence B_t' sent from Bob, she has to figure out the permutation of B_t' before sending E_h to Alice. In the following, we first show that even if there is no permutation on B_t, i.e., $B_t' = B_t$, Eve's attack can still be detected because the inconsistency of the raw keys will be incorporated into C, and thus, will be detected eventually. After that, we will show that if B_t is permuted as B_t', i.e., $B_t' \neq B_t$, Eve's attack can be detected too.

- Case 1: $B_t' = B_t$. Since Bob cannot distinguish whether E_t is the original sequence, A_t^H, from Alice or a faked one, he will derive the raw key as $K_{BE} = BM(E_t, B_h) (= \{BM(e_{t1}, b_{h1}), BM(e_{t2}, b_{h2}), ..., BM(e_{hn}, b_{hn})\})$. After that, Bob sends π (here π does not permute B_t) and K_C to Alice in Step 4. Similarly, Alice also derives his raw key as $K_{AE} = BM(A_h, E_h)$ and then performs the public discussion with Bob.

  One can see that if Bob's measurement result on (e_{ti}, b_{hi}) is $|\phi^+\rangle_{e_{ti}b_{hi}}$(with $\frac{1}{4}$ probability), $1 \leq i \leq n$, then the photons e_{hi} (in Alice's hand) and b_{ti} (in Eve's hand)

will automatically form the entangled state $|\phi^+\rangle_{e_{hi}b_{ti}}$ (entanglement swapping between two EPR pairs). If the measurement result of Alice on (a_{hi}, e_{hi}) is still $|\phi^+\rangle_{a_{hi}e_{hi}}$(with $\frac{1}{4}$ probability), then Eve will obtain $|\phi^+\rangle_{a_{ti}b_{ti}}$ (entanglement swapping among three EPR pairs) of $K_{AE}(= K_{BE})$ without being detected. Since four measurement results, $(|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle)$, would make $K_{AE} = K_{BE}$, the probability for Eve to succeed the attack is $\frac{1}{4} \cdot \frac{1}{4} \cdot 4 = \frac{1}{4}$.

However, if Bob's measurement result on (e_{ti}, b_{hi}) is not $|\phi^+\rangle_{e_{ti}b_{hi}}$(with $\frac{3}{4}$ probability), then Eve's attack must be detected because the entanglement swapping of $|\phi^+\rangle_{a_{hi}a_{ti}}$ and $E \in \{|\phi^-\rangle_{e_{hi}b_{ti}}, |\psi^+\rangle_{e_{hi}b_{ti}}, |\psi^-\rangle_{e_{hi}b_{ti}}\}$ will definitely cause inconsistency between the raw keys derived by Alice and Bob respectively (refer to Table 1). Although the probability for Eve to succeed the attack is high, i.e., $\frac{1}{4}$ to obtain one measurement result of Alice and Bob accurately, she will be detected in the public discussion. That is, based on Lemma 6, if $\frac{n}{2}$ of the attacked photons are selected for public discussion, then the probability to detect Eve is $1 - (\frac{1}{4})^{\lceil \frac{n}{2} \rceil} \approx 1$, if n is a large number.

- Case 2: $B'_t \neq B_t$. If Eve has to figure out the permutation of Bob before sending E_h to Alice, she is with the probability $\frac{1}{n!}$ to succeed. Therefore, the probability to detect Eve is $1 - ((\frac{1}{4})^{\lceil \frac{n}{2} \rceil} \cdot \frac{1}{n!}) \approx 1$, if n is a large number. □

4.2.2. *Man-in-the-middle attack*

In this attack, Eve prepares n EPR pairs in state $|\phi^+\rangle_{e_{hi}e_{ti}} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{e_{hi}e_{ti}}$ and another n EPR pairs in state $|\phi^+\rangle_{e'_{hi}e'_{ti}} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{e'_{hi}e'_{ti}}$, where $1 \leq i \leq n$. She divides these EPR pairs into four sequences: $E_h = [e_{h1}, e_{h2}, ..., e_{hn}]$, $E_t = [e_{t1}, e_{t2}, ..., e_{tn}]$, $E'_h = [e'_{h1}, e'_{h2}, ..., e'_{hn}]$, and $E'_t = [e'_{t1}, e'_{t2}, ..., e'_{tn}]$. Thereafter, she intercepts A'_t sequence from Alice and sends E'_t sequence to Bob instead. She likewise intercepts B'_t from Bob and sends E_t to Alice instead. Therefore, the photon sequences in Alice's hand would be (A_h, E_t) , Bob would hold (E'_t, B_h), and Eve would have (A'_t, E_h) and (E'_h, B'_t).

The goal of Eve is to share a key, K_{AE}, with Alice, through the photon sequences (A'_t, E_h) in her hand without being detected. Moreover, Eve would also like to share another key, K_{BE}, with Bob, through the photon sequences (E'_h, B'_t) in her hand without being detected. Therefore, when Alice uses K_{AE} to send a secret message M_a to Bob, Eve can eavesdrop the contents of M_a, and then re-encrypt M_a or $\hat{M}_a$ (a forged message) to Bob using K_{BE}, and vice versa. Since Eve's attack is created before C has been decided, with a high probability, the inconsistency of K_{BE} and K_{AE} will be incorporated into C, and thus, will be detected eventually. Theorem 4 shows that the proposed PQKD is secure against the man-in-the-middle attack.

Theorem 4: In the proposed PQKD, if Eve attempts to perform the man-in-the-middle attack, she will be detected with the probability $1 - (\frac{1}{4})^{\lceil \frac{n}{2} \rceil} \approx 1$, if n is a large number.

Proof: In the following, we first show that even if Bob does not permute B_t, i.e., $B'_t = B_t$, Eve's attack can still be detected. After that, we will show that if B_t is permuted as B'_t, i.e., $B'_t \neq B_t$, Eve's attack can be detected too.

- Case 1: $B'_t = B_t$. The probability that $K_{BE} = K_{AE}$ is $\frac{1}{4}$ for every two measurement results due to Lemma 7. Although the probability for Eve to succeed the attack is high, i.e., $\frac{1}{4}$ to make one measurement result in K_{BE} equal to the corresponding measurement result in K_{AE}, she will be detected in the public discussion. That is, if $\frac{n}{2}$ of the attacked photons are selected for public discussion, the probability to detect Eve is $1-(\frac{1}{4})^{\lceil \frac{n}{2} \rceil} \approx 1$, if n is a large number.

- Case 2: $B'_t \neq B_t$. In Step 5, Alice will permute E_t according to the permutation π announced by Bob in Step 4. Since Eve can also overhear π, she can permute E_h in her hand according to π too. Accordingly, the key K_{AE} shared between Alice and Eve is still identical. Similar to Case 1, the probability that $K_{AE} = K_{BE}$ is $\frac{1}{4}$ for every two measurement results due to Lemma 7. Although the probability for Eve to succeed the attack is high, she will be detected in the public discussion. That is, if $\frac{n}{2}$ of the attacked photons are selected for public discussion, the probability to detect Eve is still $1 - (\frac{1}{4})^{\lceil \frac{n}{2} \rceil} \approx 1$, if n is a large number. □

4.3. *Fairness of the Proposed PQKD protocol*

Although the proposed PQKD is secure against disturbance attacks and eavesdropping attacks (as discussed above), either Alice or Bob may wish to control the key both independently and without being detected by the other. According to the definition of a fair PQKD protocol, no one should have a one bit advantage in controlling (predicting) the secret key. Therefore, the fairness of the protocol is given as follows.

4.3.1. *Fair to Bob: Can Alice control the key?*

The following shows an attack that Alice may use to control K.

4.3.1.1 *Permutation guessing attack*

In the proposed PQKD, Alice is the one who decides the checking set for public discussion. Upon receiving B'_t which contains n permuted photons from Bob, if Alice can figure out the permutation of m photons in B'_t, then she can perform Bell-measurements to deduce m measurement results in the raw key $K_{AB} = (K_{BA})$. Accordingly, she can select those unwanted measurement results for public discussion and thus control a portion of the final key K. Theorem 5 shows that the proposed PQKD is secure against Alice's permutation guessing attack.

Theorem 5: In the proposed PQKD, if Alice attempts to perform the permutation guessing attack, she is with the probability $(\prod_{i=1}^{m} C_1^{n-(i-1)})^{-1}$ to guess π. Otherwise, she is with the probability $1 - (\frac{1}{4})^{\lceil \frac{m}{2} \rceil} \approx 1$ to share a different key with Bob, if $m = n$, and n is a large number.

Proof: Upon receiving A'_t from Alice, Bob will send B'_t to Alice. Since Bob does not perform any operation on A'_t but just perserve it, Alice cannot obtain any useful information about the key. Therefore, the only way for Alice to control the key K is to guess Bob's permutation π. The probability for Alice to guess π is $(\prod_{i=1}^{m} C_1^{n-(i-1)})^{-1}$. For otherwise, the probability

that $K_{AB} \neq K_{BA}$ is with $1 - \frac{1}{4} = \frac{3}{4}$ for each measurement result in the raw keys K_{AB} and K_{BA} due to Lemma 6 and 7. Although Alice can control the key K (through K_{AB}) with a high probability, the probability for Alice to share a different key with Bob is $1 - (\frac{1}{4})^{\lceil \frac{m}{2} \rceil} \approx 1$, if $m = n$, and n is a large number. □

4.3.2. *Fair to Alice: Can Bob control the key?*

The following shows several attacks that Bob may attempt to use to control K.

4.3.2.1 *Permutation adjustment attack*

In the proposed PQKD, after receiving a permuted B_t, i.e., B_t', from Bob in Step 2, Alice will first remove the Hadamard operation's effect on A_t' and then announce the positions of C to Bob in Step 3. Then, Bob can derive the raw key K_{BA} and K_C, before Alice in Step 4.

In order to control the key $K(= K_{BA} - K_C)$, a malicious Bob (who knows K_{BA} and K_C) may send a faked $\pi'(\neq \pi)$ to Alice in Step 4 by adjusting s positions in the original π to form π' in hope that he can control K through π'. Although Bob's attack is performed after C has been announced, with a high probability, he will share a different key with Alice and then cause their subsequent communications failure. Theorem 6 shows that the proposed PQKD is secure against Bob's permutation adjustment attack.

Theorem 6: In the proposed PQKD, if Bob attempts to perform the permutation adjustment attack, he is with the probability $1 - (\frac{1}{16})^s \approx 1$ to share a different key with Alice, if $s = \frac{n}{2}$, and n is a large number.

Proof: According to Lemma 4, the probability that $K_{BA} = K_{AB}$ is $\frac{1}{16}$ for every four measurement results after permuting two positions of the photons in B_t' maliciously. Although Bob can adjust s positions in π (which are not included in C) to control the raw key without being detected with a high probability, however, he is with the probability $1 - (\frac{1}{16})^s \approx 1$ to share a different key with Alice, if $s = \frac{n}{2}$, and n is a large number. □

4.3.2.2 *Controlled-NOT attack*

In the proposed PQKD, the sequence A_t is protected by H. Therefore, Bob cannot obtain the raw key K_{BA} before sending his sequence B_t' to Alice. The following shows that H is essential to protect the fairness of the protocol. For otherwise, Bob can first use the controlled-NOT (CNOT) gate to entangle the single photons with the photons in A_t, and then control the measurement result into $|\phi^+\rangle$ or $|\phi^-\rangle$. The attacking scenario is described as follows.

(a) Bob prepares an D sequence which is formed by n single photons $|0\rangle$, e.g., $D = [d_1, d_2, ..., d_n]$, where d_i denotes the ith single photon $|0\rangle$.

(b) Bob uses a CNOT gate to entangle the D sequence with the A_t sequence, i.e., CNOT$(a_{ti} \otimes d_i)$, where a_{ti} is the control bit and d_i is the target bit, $i = 1, 2, 3, ..., n$. After Bob's operations, the entangled state $|\phi^+\rangle_{a_{hi}a_{ti}} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{a_{hi}a_{ti}}$ prepared by Alice will transform into a three-particle entangled state $|\psi_1\rangle$ as shown in Eq. (4):

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{a_{hi}a_{ti}d_i}$$

$$= \frac{1}{\sqrt{2}}[|+\rangle_{a_{ti}}(|\phi^+\rangle)_{a_{hi}d_i} + |-\rangle_{a_{ti}}(|\phi^-\rangle)_{a_{hi}d_i}]. \quad (4)$$

The CNOT gate can be represented as follows:

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

(c) Then, Bob measures a_{ti}'s with the basis $\{|+\rangle, |-\rangle\}$ and then returns the D sequence to Alice. According to Eq. (4), if Bob's measurement result is $|+\rangle_{a_{ti}}$ ($|-\rangle_{a_{ti}}$), Alice would obtain $|\phi^+\rangle_{a_{hi}di}$ ($|\phi^-\rangle_{a_{hi}di}$) after performing $BM(a_{hi}, d_i)$. Therefore, although Bob is not the checking set selector, he can control the measurement result into $|\phi^+\rangle$ or $|\phi^-\rangle$. Since Bob can also deduce the measurement result of Alice from a_{ti} in his hand, his cheating cannot be detected.

By randomly performing H on a_{ti}, $|\phi^+\rangle_{a_{hi}a_{ti}}$ would be transformed into the state $|\phi^+\rangle^H_{a_{hi}a_{ti}}$ (refer to Eq. (2)), $1 \le i \le n$. If Bob uses a CNOT gate to entangle d_i with a^H_{ti}, i.e., $\text{CNOT}(a^H_{ti} \otimes d_i)$, the entangled state $|\phi^+\rangle^H_{a_{hi}a_{ti}}$ will transform into a three-particle entangled state $|\psi_1\rangle'$ as shown in Eq. (5):

$$\begin{aligned} |\psi_1\rangle' &= \frac{1}{2}(|000\rangle + |011\rangle + |100\rangle + |111\rangle)_{a_{hi}a_{ti}d_i} \\ &= \frac{1}{2}(|+\rangle_{a_{ti}}(|\phi^-\rangle + |\psi^+\rangle)_{a_{hi}d_i} + |-\rangle_{a_{ti}}(|\phi^+\rangle + |\psi^-\rangle)_{a_{hi}d_i}). \end{aligned} \quad (5)$$

Since Alice will randomly choose some a_{ti}'s (approximately half of them) and apply H on them, Bob will not be able to differentiate $|\psi_1\rangle$ and $|\psi_1\rangle'$ from his measurement result and will be detected in the public discussion. Theorem 7 shows that the proposed PQKD is secure against Bob's CNOT attack.

Theorem 7: In the proposed PQKD, if Bob attempts to perform the CNOT attack, he will be detected with the probability $1 - (\frac{7}{8})^{\lceil \frac{s}{2} \rceil} \approx 1$, if $s = n$, and n is a large number.

Proof: Since Alice will randomly perform H on a_{ti}, $1 \le i \le n$, the probability for Bob to guess whether or not a photon a_{ti} is subject to H is $\frac{1}{2}$. According to Eq. (4), if a_{ti} is not subject to H, Bob can deduce Alice's measurement result from a_{ti} in his hand. In this case, with the probability $\frac{1}{2}$, the attacked photon a_{ti} is not selected by Alice for public discussion (Since Bob can deduce Alice's measurement result accurately herein, his cheating cannot be detected even if this a_{ti} is selected for public discussion.)

On the other hand, even if a_{ti} is subject to H (with $\frac{1}{2}$ probability), he also has the probability $\frac{1}{2}$ to deduce Alice's measurement result due to Eq. (5), and with the probability $\frac{1}{2}$, this a_{ti} is not selected for public discussion. Accordingly, the probability that Bob correctly controls one measurement result of K_{BA} is $\frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{8}$. Similarly, the probability for Bob to pass the public discussion is also $\frac{3}{8}$ because he can deduce Alice's measurement result accurately in the above cases.

Moreover, if the following three situations occur simultaneously: (a) a_{ti} is subject to H (with $\frac{1}{2}$ probability); (b) Bob deduces Alice's measurement result wrongly (with $\frac{1}{2}$ probability); and (c) a_{ti} is not selected for public discussion (with $\frac{1}{2}$ probability), Alice and Bob have the probability $\frac{1}{8}$ to share a different key. However, in Situations (a) and (b), if this a_{ti} is selected for public discussion (with $\frac{1}{2}$ probability too), then the probability for Alice to detect Bob's attack is $\frac{1}{8}$. Accordingly, if s photons in A'_t are subject to Bob's CNOT attacks, the probability for Alice to detect Bob's cheating is $1-(\frac{7}{8})^{\lceil \frac{s}{2} \rceil} \approx 1$, if $s = n$, and n is a large number. □

Note that, since no one should have one bit advantage in controlling the secret key in a fair PQKD, one can see that from the above analysis, Bob has a high probability, i.e., $\frac{3}{8}(> \frac{1}{4})$, to control one of the four measurement results, $|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle$, and $|\psi^-\rangle$, without being detected. This weakness can be solved by letting each of the measurement result represents one classical key bit, e.g., $|\phi^+\rangle \Rightarrow 0; |\phi^-\rangle \Rightarrow 1; |\psi^+\rangle \Rightarrow 0$; and $|\psi^-\rangle \Rightarrow 1$. For instance, if Alice's and Bob's measurement results are $|\phi^+\rangle_{h_A t_B}$ and $|\phi^+\rangle_{t_A h_B}$ respectively, then they share one classical bits "0." On the other hand, if Alice's and Bob's measurement results are $|\psi^-\rangle_{h_A t_B}$ and $|\psi^-\rangle_{t_A h_B}$ respectively, then they share "1."

4.3.2.3 *Direct measurement attack*

In the proposed PQKD, although the sequence A'_t is protected by H, a malicious Bob still can obtain s measurement results of the raw key K_{BA} directly in Step 2 by performing Bell-measurements on s entanglement-swapped photon pairs (without waiting for Alice to remove her Hadamard operation's effect on A'_t). With such direct measurement attack, a malicious Bob may wish to control the key independently without being detected by Alice. Since Bob's attack is performed before C has been decided, with a high probability, the inconsistency of K_{BA} and K_{AB} will be incorporated into C, and thus, will be detected eventually. Theorem 8 shows that the proposed PQKD is secure against Bob's direct measurement attack.

Theorem 8: In the proposed PQKD, if Bob attempts to perform the direct measurement attack, he will be detected with the probability $1-(\frac{7}{8})^{\lceil \frac{s}{2} \rceil} \approx 1$, if $s = n$, and n is a large number.

Proof: Since Alice will randomly perform H on a_{ti}, $1 \leq i \leq n$, the probability for Bob to guess whether a_{ti} is subject to H is $\frac{1}{2}$. According to Eq. (1), if a_{ti} is not subject to H, Bob can deduce Alice's measurement result from (a_{ti}, b_{hi}) in his hand. Because Bob's attack is performed before C has been decided, with the probability $\frac{1}{2}$, this a_{ti} is not selected by Alice for public discussion (Since Bob can deduce Alice's measurement result accurately, his cheating cannot be detected even if this a_{ti} is selected for public discussion.)

Even if a_{ti} is subject to H (with $\frac{1}{2}$ probability), he also has probability $\frac{1}{2}$ to deduce Alice's measurement result due to Lemma 2, and with the probability $\frac{1}{2}$, this a_{ti} is not selected for public discussion. Accordingly, the probability that Bob correctly controls two bits of K_{BA} is $\frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{8}$. Similarly, the probability for Bob to pass the public discussion is also $\frac{3}{8}$ because he can deduce Alice's measurement result accurately in the above cases.

Moreover, if the following three situations occur simultaneously: (a) a_{ti} is subject to H (with $\frac{1}{2}$ probability); (b) Bob deduces Alice's measurement result wrongly (with $\frac{1}{2}$ proba-

bility), and (c) a_{ti} is not selected for public discussion (with $\frac{1}{2}$ probability), Alice and Bob have the probability $\frac{1}{8}$ to share a different key. However, in Situations (a) and (b), if this a_{ti} is selected for public discussion (with $\frac{1}{2}$ probability too), then the probability for Alice to detect Bob's attack is $\frac{1}{8}$. Accordingly, if Bob performs Bell-measurements on s entanglement-swapped photon pairs directly in Step 2, the probability for Alice to detect Bob's cheating is $1-(\frac{7}{8})^{\lceil \frac{s}{2} \rceil} \approx 1$, if $s = n$, and n is a large number. □

Since Bob can control one of the four measurement results without being detected with a high probability, i.e., $\frac{3}{8}(> \frac{1}{4})$, by letting each of the measurement result represents one classical key bit (see the security analysis to the CNOT attack described above), the weakness can be solved.

4.3.2.4 *Single photon measurement attack*

Upon receiving A'_t from Alice, a malicious Bob may replace s photons, $1 \leq s \leq n$, in B'_t by s single photons $d_i \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, $1 \leq i \leq n$. After hearing from Alice about the positions of C (which also means that $A_t^H \Rightarrow A_t$), Bob will measure s photons in A_t (which are included in C) with the basis $\{|0\rangle, |1\rangle\}$ (or $\{|+\rangle, |-\rangle\}$). After that, the corresponding photons in A_h will also collapse into single photons. In order to control the key, Bob may send $\pi'(\neq \pi)$ to Alice by adjusting the positions of d_i's to the positions of key bits. Although Bob can send a forged π' to Alice after C has been decided, with a high probability, he will share a different key with Alice and then cause their subsequent communications failure. Theorem 9 shows that the proposed PQKD is secure against Bob's single photon measurement attack.

Theorem 9: In the proposed PQKD, if Bob attempts to perform the single photon measurement attack, he is with the probability $1-(\frac{1}{2})^s \approx 1$ to share a different key with Alice, if $s = \frac{n}{2}$, and n is a large number.

Proof: According to Lemma 8, the probability that $(K_{BA} - K_C) = (K_{AB} - K_C)$ is $\frac{1}{2}$ for every measurement result after Bob's attack. Accordingly, he is with the probability $1-(\frac{1}{2})^s \approx 1$ to share a different key, K, with Alice, if $s = \frac{n}{2}$, and n is a large number. □

In the proposed PQKD, Bob can control the measurement result of K with the probability $\frac{1}{2}$ for every measurement result (In an ideal case, this probability should be $\frac{1}{4}$ for every measurement result.) By letting each of the measurement result represents one classical key bit (see the security analysis to the CNOT attack described above), the weakness can be solved.

Though the proposed PQKD assumes quantum channels to be noiseless, in practical experiment, there are always noises, and Alice (Bob) may hide her (his) attack in the noises of quantum channels [32]. Suppose that the quantum bit error rate (QBER) caused by the noise of the channels is τ (≈2%∼8.9% [33, 34, 35, 36, 37]). If the QBER caused by Alice's (Bob's) attack is smaller than τ, then her (his) attack may not be detected by Bob (Alice). However, in the proposed protocol, the QBER caused by the attack is about 12.5% (due to Theorems 7 and 8) which is higher than τ. Thus, this kind of attack eventually will be detected by the other party.

5. Conclusions

This paper has presented a PQKD protocol, based on the measurement uncertainty property in the entanglement swapping of EPR pairs, to facilitate the distribution of an unpredictable key between two mutually-untrusted communicants. In order to prevent a potentially malicious communicant from manipulating the shared secret key in the process of public discussion, a fair public discussion game is proposed. By randomly performing the Hadamard operations and permutations on the exchanged photon sequences, the communicants will not be able to obtain a raw key stealthily, and thereafter control the final key via the public discussion.

The security analysis demonstrates that the illustrated PQKD is secure against both disturbance attacks and eavesdropping attacks, and no user can manipulate the outcome of even one bit of the final key with more than 50% probability. Thus, this method is suitable for solving the fair key distribution problem in a mutually-untrusted environment. Further design of a fair public discussion game to propose a fair PQKD protocol for a mutually-untrusted environment will be the focus of future research.

Acknowledgements

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the clarity and readability of this article. This article is supported partially by the National Science Council of the Republic of China, Taiwan under the Contract No. NSC 98-2221-E006-097-MY3.

References

1. S. K. Chong and T. Hwang (2010), *Quantum key agreement protocol based on BB84,* Opt. Commun., vol. 283, no. 6, pp. 1192–1195.
2. T. Hwang and C. M. Li (2008), *Secure direct communication using deterministic BB84 protocol,* Int. J. Mod. Phys. C, vol. 19, no. 4, pp. 625–635.
3. C. H. Bennett and G. Brassard (1984), *Quantum cryptography: Public key distribution and coin tossing (invited paper),* in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175–179.
4. C. H. Bennett (1992), *Quantum cryptography using any two nonorthogonal states,* Phys. Rev. Lett., vol. 68, pp. 3121–3124.
5. D. Bruss (1998), *Optimal eavesdropping in quantum cryptography with six states,* Phys. Rev. Lett., vol. 81, no. 14, pp. 3018–3021.
6. H. Bechmann-Pasquinucci and N. Gisin (1999), *Incoherent and coherent eavesdropping in the 6-state protocol of quantum cryptography,* Phys. Rev. A, vol. 59, no. 6, pp. 4238–4248.
7. A. K. Ekert (1991), *Quantum cryptography based on Bell's theorem,* Phys. Rev. Lett., vol. 67, pp. 661–663.
8. G. Gan (2009), *Quantum key distribution scheme with high efficiency,* Commun. Theor. Phys., vol. 51, no. 5, pp. 820–822.
9. C. Li, H. S. Song, L. Zhou, and C. F. Wu (2003), *A random quantum key distribution achieved by using Bell states,* J. Opt. B: Quantum Semiclass. Opt., vol. 5, no. 2, pp. 155–157.
10. D. Song (2004), *Secure key distribution by swapping quantum entanglement,* Phys. Rev. A, vol. 69, no. 3, p. 034301.
11. X. F. Ma, B. Qi, Y. Zhao, and H. K. Lo (2005), *Practical decoy state for quantum key distribution,* arXiv:quant-ph/0503005v5.
12. Y. Zhao, B. Qi, X. F. Ma, H. K. Lo, and L. Qian (2005), *Experimental quantum key distribution with decoy states,* arXiv:quant-ph/0503192v4.

13. D. Gottesman, H. K. Lo, N. Lütkenhaus, and J. Preskill (2004), *Security of quantum key distribution with imperfect devices,* Quantum Inf. Comput., vol. 4, no. 5, pp. 325–360.
14. E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury (2000), *A proof of the security of quantum key distribution,* in Proceedings of the thirty-second annual ACM symposium on Theory of computing, Portland, Oregon, United States, pp. 715–724.
15. D. Gottesman and H. K. Lo (2003), *Proof of security of quantum key distribution with two-way classical communications,* IEEE T. Inform. Theory, vol. 49, no. 2, pp. 457–475.
16. H. K. Lo and H. F. Chau (1999), *Unconditional security of quantum key distribution over arbitrarily long distances,* Science, vol. 283, pp. 2050–2056.
17. D. Mayers (2001), *Unconditional security in quantum cryptography,* J. ACM, vol. 48, pp. 351–406.
18. H. K. Lo, X. Ma, and K. Chen (2005), *Decoy state quantum key distribution,* Phys. Rev. Lett., vol. 94, p. 230504.
19. M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim (2005), *The universal composable security of quantum key distribution,* in Proceedings of the 2nd Theory of Cryptography Conference, (Lecture Notes in Computer Science/Security and Cryptology), vol. 3378, Cambridge, MA, USA, pp. 386–406.
20. S. K. Chong, C. W. Tsai, and T. Hwang (2011), *Improvement on "quantum key agreement protocol with maximally entangled states",* Int. J. Theor. Phys., vol. 50, no. 6, pp. 1793–1802.
21. C. C. Hsueh and C. Y. Chen (2004), *Quantum key agreement protocol with maximally entangled states,* in Proceedings of the 14th Information Security Conference (ISC 2004), National Taiwan University of Science and Technology, Taipei, Taiwan, pp. 236–242.
22. C. W. Tsai, S. K. Chong, and T. Hwang (2010), *Comment on quantum key agreement protocol with maximally entangled states,* in Proceedings of the 20th Cryptology and Information Security Conference (CISC 2010), National Chiao Tung University, Hsinchu, Taiwan, pp. 210–213.
23. C. W. Tsai and T. Hwang (2009), *On "quantum key agreement protocol",* Technical Report, C-S-I-E, NCKU, Taiwan, R.O.C..
24. N. Zhou, G. Zeng, and J. Xiong (2004), *Quantum key agreement protocol,* Electron. Lett., vol. 40, no. 18, pp. 1149–1150.
25. C. H. Bennett, G. Brassard, and N. D. Mermin (1992), *Quantum cryptography without Bell's theorem,* Phys. Rev. Lett., vol. 68, p. 557.
26. F. G. Deng, G. L. Long, Y. Wang., and L. Xiao (2004), *Increasing the efficiencies of random-choice-based quantum communication protocols with delayed measurement,* Chinese Phys. Lett., vol. 21, pp. 2097–2100.
27. M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert (1993), *"Event-ready-detectors" Bell experiment via entanglement swapping,* Phys. Rev. Lett., vol. 71, p. 4287.
28. J. W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger (1998), *Experimental entanglement swapping: Entangling photons that never interacted,* Phys. Rev. Lett., vol. 80, p. 3891.
29. Y. Guo and G. Zeng (2005), *Quantum event-error detection codes,* J. Phys. Soc. Jpn., vol. 74, pp. 2949–2956.
30. Y. Guo and G. Zeng. (2006), *How to combat quantum bursts of errors efficiently,* J. Phys. Soc. Jpn., vol. 75, p. 034402.
31. D. Z. Huang, Z. G. Chen, and Y. Guo (2007), *Quantum error-correction codes based on multilevel constructions of hadamard matrices,* in Proceedings of the 3rd International Conference on Intelligent Computing, Qingdao, China, pp. 18–24.
32. J. Wang, Q. Zhang, L. M. Liang, and C. J. Tang (2005), *Comment on: "arbitrated quantum signature scheme with message recovery",* Phys. Lett. A, vol. 347, pp. 262–263.
33. T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger (2000), *Quantum cryptography with entangled photons,* Phys. Rev. Lett., vol. 84, no. 20, pp. 4729–4732.
34. C. Gobby, Z. L. Yuan, and A. J. Shields (2004), *Quantum key distribution over 122km standard telecom fiber,* Appl. Phys. Lett., vol. 84, pp. 3762–3764.
35. R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson (2002), *Practical free-space quan-*

tum key distribution over 10 km in daylight and at night, New J. Phys., vol. 4, pp. 43.1–43.14.
36. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden (2002), *Quantum key distribution over 67 km with a plug&play system,* New J. Phys., vol. 4, pp. 41.1–41.8.
37. A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, and P. Grangier (2002), *Single photon quantum cryptography,* Phys. Rev. Lett., vol. 89, no. 18, p. 187901.

Appendix A

In this appendix, the lemmas which will be used to show the security of the proposed PQKD are given below.

Lemma 1: Let $EPR^H_{a_1a_2}$ be the result after performing H on one photon of an EPR pair $EPR_{a_1a_2}$. $BM(EPR^H_{a_1a_2})$ will be in two of all four possible measurement results with equal probability, i.e., $\frac{1}{2}$.

Proof: Let $EPR_{a_1a_2} \in \{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}_{a_1a_2}$, and $EPR^H_{a_1a_2} \in \{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}^H_{a_1a_2}$. After the measurement, the system will evolve in the following states:

$$\begin{aligned}
I \otimes H|\phi^+\rangle_{a_1a_2} &= |\phi^+\rangle^H_{a_1a_2} &&= \frac{1}{\sqrt{2}}(|\phi^-\rangle + |\psi^+\rangle)_{a_1a_2},\\
I \otimes H|\phi^-\rangle_{a_1a_2} &= |\phi^-\rangle^H_{a_1a_2} &&= \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\psi^-\rangle)_{a_1a_2},\\
I \otimes H|\psi^+\rangle_{a_1a_2} &= |\psi^+\rangle^H_{a_1a_2} &&= \frac{1}{\sqrt{2}}(|\phi^+\rangle - |\psi^-\rangle)_{a_1a_2},\\
I \otimes H|\psi^-\rangle_{a_1a_2} &= |\psi^-\rangle^H_{a_1a_2} &&= \frac{1}{\sqrt{2}}(|\phi^-\rangle - |\psi^+\rangle)_{a_1a_2}.
\end{aligned}$$

□

Lemma 2: The measurement results of the entanglement swapping of $EPR^H_{a_1a_2}$ and $EPR_{b_1b_2}$ are distinct.

Proof: Let $EPR^H_{a_1a_2} = |\phi^+\rangle^H_{a_1a_2}$, and $EPR_{b_1b_2} = |\phi^+\rangle_{b_1b_2}$. After the entanglement swapping, the system will evolve in the following states:

$$\begin{aligned}
|\phi^+\rangle^H_{a_1a_2} \otimes |\phi^+\rangle_{b_1b_2} = \frac{1}{2}&(|\phi^+\rangle_{a_1b_2}(|\phi^-\rangle + |\psi^+\rangle)_{a_2b_1} +\\
&|\phi^-\rangle_{a_1b_2}(|\phi^+\rangle - |\psi^-\rangle)_{a_2b_1} +\\
&|\psi^+\rangle_{a_1b_2}(|\phi^+\rangle + |\psi^-\rangle)_{a_2b_1} -\\
&|\psi^-\rangle_{a_1b_2}(|\phi^-\rangle + |\psi^+\rangle)_{a_2b_1}).
\end{aligned}$$

□

Lemma 3: The probability for the measurement results of the entanglement swapping of $EPR^H_{a_1a_2}$ and $EPR^H_{b_1b_2}$ to be the same is $\frac{1}{2}$.

Proof: Let $EPR^H_{a_1a_2} = |\phi^+\rangle^H_{a_1a_2}$, $EPR^H_{b_1b_2} = |\phi^+\rangle^H_{b_1b_2}$. After the entanglement swapping,

the system will evolve in the following states:

$$\begin{aligned}|\phi^+\rangle^H_{a_1a_2} \otimes |\phi^+\rangle^H_{b_1b_2} &= \frac{1}{2}(|\phi^+\rangle_{a_1b_2}|\phi^+\rangle_{a_2b_1} + |\phi^-\rangle_{a_1b_2}|\psi^+\rangle_{a_2b_1} + \\ &\quad |\psi^+\rangle_{a_1b_2}|\phi^-\rangle_{a_2b_1} - |\psi^+\rangle_{a_1b_2}|\psi^+\rangle_{a_2b_1}.\end{aligned}$$

□

Let EPR_1, EPR_2, EPR_3, and EPR_4 be four Bell states, Lemma 4 is described as follows:

Lemma 4: Let EPR'_1, EPR'_3 be the entanglement swapping of EPR_1, EPR_3, and EPR'_2, EPR'_4 be the entanglement swapping of EPR_2, EPR_4. Again let EPR_1", EPR_2" be the entanglement swapping of EPR'_1, EPR'_2. The probability for $BM(EPR_1") = BM(EPR'_3)$ and $BM(EPR_2") = BM(EPR'_4)$ is $\frac{1}{16}$.

Proof: Let $EPR_1 = |\phi^+\rangle_{a_1a_2}$, $EPR_2 = |\phi^+\rangle_{b_1b_2}$, $EPR_3 = |\phi^+\rangle_{c_1c_2}$, and $EPR_4 = |\phi^+\rangle_{d_1d_2}$. According to Eq. (1), the entanglement swapping of $|\phi^+\rangle_{a_1a_2}$ and $|\phi^+\rangle_{c_1c_2}$ will result in one of the four measurement results with equal probability (i.e., $\frac{1}{4}$), which can be denoted as EPR'_1 and EPR'_3 respectively, and $EPR'_1 = EPR'_3$. Similarly, the entanglement swapping of $|\phi^+\rangle_{b_1b_2}$ and $|\phi^+\rangle_{d_1d_2}$ will also result in one of the four measurement results with equal probability (i.e., $\frac{1}{4}$), which can be denoted as EPR'_2 and EPR'_4 respectively, and $EPR'_2 = EPR'_4$. After that, if EPR'_1 and EPR'_2 are performed an entanglement swapping again, they will also result in one of the four measurement results with equal probability (i.e., $\frac{1}{4}$) due to Eq. (1), which can denoted as $EPR_1", EPR_2"$. Accordingly, the probability for $BM(EPR_1") = BM(EPR'_3)$ and $BM(EPR_2") = BM(EPR'_4)$ is $\frac{1}{4} \cdot \frac{1}{4} = \frac{1}{16}$. □

Lemma 5: If one photon of an EPR pair is replaced by a single photon $(|0\rangle, |1\rangle, |+\rangle, |-\rangle)$, then the Bell measurement result of the new pair of photons will be one of the four $(|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle)$ with equal probability, i.e., $\frac{1}{4}$.

Proof: Let a single photon be $w \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}_p$, and the EPR pair be $|\phi^+\rangle_{a_1a_2}$. After the measurement, the system will evolve in the following states:

$$\begin{aligned}&\text{If} \quad w = |0\rangle_p, \\ &\quad BM(p, a_1) = \frac{1}{2}(|\phi^+\rangle_{pa_1}|0\rangle_{a_2} + |\phi^-\rangle_{pa_1}|0\rangle_{a_2} + \\ &\qquad |\psi^+\rangle_{pa_1}|0\rangle_{a_2} + |\psi^-\rangle_{pa_1}|0\rangle_{a_2}), \\ &\text{If} \quad w = |1\rangle_p, \\ &\quad BM(p, a_1) = \frac{1}{2}(|\psi^+\rangle_{pa_1}|0\rangle_{a_2} + |\psi^-\rangle_{pa_1}|0\rangle_{a_2} + \\ &\qquad |\phi^+\rangle_{pa_1}|1\rangle_{a_2} + |\phi^-\rangle_{pa_1}|1\rangle_{a_2}), \\ &\text{If} \quad w = |+\rangle_p, \\ &\quad BM(p, a_1) = \frac{1}{2}(|\phi^+\rangle_{pa_1}|+\rangle_{a_2} + |\phi^-\rangle_{pa_1}|-\rangle_{a_2} + \\ &\qquad |\psi^+\rangle_{pa_1}|+\rangle_{a_2} - |\psi^-\rangle_{pa_1}|-\rangle_{a_2}),\end{aligned}$$

$$\begin{aligned} \text{If} \quad & w = |-\rangle_p, \\ & BM(p, a_1) = \frac{1}{2}(|\phi^+\rangle_{pa_1}|-\rangle_{a_2} + |\phi^-\rangle_{pa_1}|+\rangle_{a_2} - \\ & \qquad |\psi^+\rangle_{pa_1}|-\rangle_{a_2} + |\psi^-\rangle_{pa_1}|+\rangle_{a_2}). \end{aligned}$$

□

Lemma 6: The probability for the measurement results of the entanglement swapping of three EPR pairs to be equal is $\frac{1}{4}$.

Proof: Let the three EPR pairs be $|\phi^+\rangle_{a_1a_2}, |\phi^+\rangle_{b_1b_2}$, and $|\phi^+\rangle_{c_1c_2}$. According to Eq. (1), the entanglement swapping of $|\phi^+\rangle_{a_1a_2}$ and $|\phi^+\rangle_{b_1b_2}$ will result in one of the four measurement results with equal probability, i.e., $\frac{1}{4}$. The probability for the measurement results is not $|\phi^+\rangle$ will be $1 - \frac{1}{4} = \frac{3}{4}$, e.g., $D \in \{|\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$. The entanglement swapping of $|\phi^+\rangle_{c_1c_2}$ and D will result in twelve measurement results, and these results are not identical (see Table 1). Since the entanglement swapping of $|\phi^\pm\rangle$ and $|\psi^\pm\rangle$ will result in sixteen measurement results (see also Table 1), therefore the probability for the measurement results of the entanglement swapping of three EPR pairs to be equal is $1 - \frac{12}{16} = \frac{1}{4}$. □

Lemma 7: The probability for the measurement results of two independent entanglement swapping of four EPR pairs to be equal is $\frac{1}{4}$.

Proof: Let the four EPR pairs be $|\phi^+\rangle_{a_1a_2}, |\phi^+\rangle_{b_1b_2}, |\phi^+\rangle_{c_1c_2}$, and $|\phi^+\rangle_{d_1d_2}$. According to Eq. (1), the entanglement swapping of $|\phi^+\rangle_{a_1a_2}$ and $|\phi^+\rangle_{b_1b_2}$ ($|\phi^+\rangle_{c_1c_2}$ and $|\phi^+\rangle_{d_1d_2}$) will result in one of the four measurement results with the equal probability (i.e., $\frac{1}{4}$), which can be denoted as K_1 (K_2). Since there are four measurement results will make $K_1 = K_2$, i.e., $(|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle)$, the probability for $K_1 = K_2$ is $\frac{1}{4} \times \frac{1}{4} \times 4 = \frac{1}{4}$. □

Lemma 8: The measurement of Z-basis $\{|0\rangle, |1\rangle\}$ on one photon of each EPR pair divides these EPR pairs into two groups $|\phi^\pm\rangle, |\psi^\pm\rangle$. The unitary operation $i\sigma_y$ transforms an element on one group to the other group. Similarly, the measurement of X-basis $\{|+\rangle, |-\rangle\}$ on one photon of each EPR pair divides these EPR pairs into two groups $\{|\phi^+\rangle, |\psi^+\rangle\}$, and $\{|\phi^-\rangle, |\psi^-\rangle\}$. The unitary operation $i\sigma_y$ transforms an element on one group to the other group.

Proof: Let the EPR pair be one of the $(|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle)_{a_1a_2}$, and $i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$. After the measurement, the system will evolve in the following states:

$$\begin{aligned} |00\rangle &= \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\phi^-\rangle), \\ |01\rangle &= \frac{1}{\sqrt{2}}(|\psi^+\rangle + |\psi^-\rangle), \\ |10\rangle &= \frac{1}{\sqrt{2}}(|\psi^+\rangle - |\psi^-\rangle), \\ |11\rangle &= \frac{1}{\sqrt{2}}(|\phi^+\rangle - |\phi^-\rangle), \end{aligned}$$

$$
\begin{aligned}
|++\rangle &= \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\psi^+\rangle), \\
|+-\rangle &= \frac{1}{\sqrt{2}}(|\phi^-\rangle - |\psi^-\rangle), \\
|-+\rangle &= \frac{1}{\sqrt{2}}(|\phi^-\rangle + |\psi^-\rangle), \\
|--\rangle &= \frac{1}{\sqrt{2}}(|\phi^+\rangle - |\psi^+\rangle).
\end{aligned}
$$

□