Quantum Inf Process (2016) 15:2881–2893
DOI 10.1007/s11128-016-1307-y

Authenticated semi-quantum key distributions without classical channel

Chuan-Ming Li[1] · **Kun-Fei Yu**[2] · **Shih-Hung Kao**[2] · **Tzonelih Hwang**[2]

Received: 27 August 2014 / Accepted: 19 March 2016 / Published online: 18 April 2016

Abstract Yu et al. have proposed the first authenticated semi-quantum key distribution (ASQKD) without using an authenticated classical channel. This study further proposes two advanced ASQKD protocols. Compared to Yu et al.'s schemes, the proposed protocols ensure better qubit efficiency and require fewer pre-shared keys. Security analyses show that the proposed ASQKD protocols also can be secure against several well-known outside eavesdropper's attacks.

Keywords Authentication · Semi-quantum key distribution · Quantum cryptography

1 Introduction

Since the conjugate coding was proposed by Wiesner [1] using the idea of quantum mechanics, various branches of quantum cryptography have progressed quickly. One well-established research is the quantum key distribution (QKD) [2–12], in which two or more participants share a secret key distributed by a key distribution center or a key dealer. In some QKD protocols [5–12], the participants are assumed to equip with

✉ Tzonelih Hwang
hwangtl@ismail.csie.ncku.edu.tw

Chuan-Ming Li
licm@ms.szmc.edu.tw

Shih-Hung Kao
shkao.ken@gmail.com

1 Department of Information Management, Shu-Zen Junior College of Medicine and Management, No. 452, Huanqiu Rd., Luzhu Dist., Kaohsiung 821, Taiwan, ROC

2 Department of Computer Science and Information Engineering, National Cheng Kung University, No. 1, University Rd., Tainan City 70101, Taiwan, ROC

advanced quantum devices (e.g., quantum state generators and quantum storage) to perform operations on their quantum system. In 2007, however, Boyer et al. [13] raised an interesting issue about how "quantum" a protocol needs for having great advantages over all classical protocols. They proposed an idea of "semi-quantum" to solve this question and applied it to the QKD protocols, which is also called semi-quantum key distribution (SQKD).

The setting of Boyer et al.'s semi-quantum scenario is as follows: There are two parties, a quantum party (Alice) and a classical party (Bob), who separately stay at their secure laboratory. A quantum channel leads from Alice's laboratory to the outside and goes back to her laboratory. Whenever a qubit passes through a particular segment on the channel, Bob can access the segment and perform the following operations: (1) measure the qubit in the classical basis $\{|0\rangle, |1\rangle\}$ (i.e., Z-basis), (2) prepare a fresh qubit in the classical basis and send it, (3) reorder the qubits via different delay lines, and (4) do nothing and reflect the qubit back. If Bob is restricted to perform these operations, he will always operate within classical basis and never get the superposition of the quantum states. Therefore, Bob's operation could be treated as "classical." Contrasting with classical Bob's restriction, the quantum Alice has full quantum capabilities in the scenario.

There are two variants of the SQKD protocol in Boyer et al.'s [14] study. One is *randomization-based*, and the other is *measure-resend*. The major difference between these two types is the capabilities of Bob. In the randomization-based protocol, Bob is restricted to perform the operations (1), (3), and (4). In the measure-resend protocol, Bob performs the operations (1), (2), and (4). Most of the subsequent semi-quantum research [15–22] usually follow this scenario to implement their protocols. In 2009, Zou et al. [15] proposed five protocols in which fewer quantum states than Boyer et al.'s are used to achieve the SQKD. After that, Zhang et al. [16] proposed an SQKD protocol in which the quantum Alice is able to share a secret key with numerous classical Bobs. In 2011, Wang et al. [17] proposed an SQKD protocol to promote the qubit efficiency by using maximally entangled states as their quantum resources.

In the above-mentioned schemes, authenticated classical channels are assumed to be established between the quantum party and the classical party. It means that the authenticity and the integrity of messages on the channel are always guaranteed. However, once the authenticated classical channels are not available anymore in the environment, these protocols will be vulnerable to man-in-the-middle attacks [23,24]. As a result, Yu et al. [18] recently proposed a study of authenticated SQKD (ASQKD) protocols to solve this problem, which utilizes maximally entangled Bell states and pre-shared secret keys to construct a shared session key without the assumption of the authenticated channels. In Yu et al.'s schemes, the pre-shared master secret key is divided into three subkeys for user authentication, and the generated session key is much shorter than the master secret key. In addition, Yu et al.'s schemes still require public classical channels to exchange messages during the execution of protocols.

In this regard, this paper further proposes two advanced ASQKD protocols, which present simpler and more efficient ways in the establishment of keys as compared to Yu et al.'s protocols. The proposed ASQKD protocols require fewer than three pre-shared keys to achieve mutually authentication. Moreover, no classical channel (including public and authenticated classical channels) is needed during the course of

the protocol execution unless a suspected eavesdropping attack has been detected. In this way, the schemes are simplified to design by abandoning the usage of classical channels and merely make use of two-step quantum communication to complete the distribution of the session key. The proposed ASQKD protocols can be useful in different practical environments. For example, in a client–server archetype, a client who has resource constraint devices wants to request a session key from the server. In order to ensure the higher level of security in the process of key distribution, both the client and server may use quantum communication. In this case, the proposed protocols can be highly helpful in which the quantum party having advanced quantum devices will be considered as a server and the classical party having resource constraint devices with only basic quantum operations will be treated as a client. In addition, as the description of Yu et al. [18], the idea of ASQKD enables the establishment of a key hierarchy in security systems that also eases the key management problem.

The rest of this paper is organized as follows: the next section presents the proposed ASQKD protocols. Section 3 provides security analyses of the proposed ASQKD protocols. Section 4 makes a comparison between the proposed protocols and Yu et al.'s. Finally, we make a summary for this paper in the last section.

2 Proposed ASQKD protocols

This section presents two variants of the ASQKD protocol: randomization-based and measure-resend ASQKD, in which the session key is distributed from a quantum party (Alice) to a classical party (Bob) by two-step transmission. A public secure one-way hash function H (e.g., SHA-2, SHA-3) is required to map the session key SK and the master key K_1 into an M-bit binary string. The hash function has the property that not only it is very difficult to deduce the message from its hashed value, but it is also extremely hard to find two messages that hash to the same value. In addition, there are two bases, classical basis (Z-basis) ($\{|0\rangle, |1\rangle\}$) and X-basis ($\{|+\rangle, |-\rangle\}$), used as the initial states of single particles. Moreover, Alice and Bob agree with the following rules: A classical bit '0' is encoded to $|0\rangle$; '1' is encoded to $|1\rangle$, and vice versa. To simplify the communication environment, the quantum channel established between Alice and Bob is assumed to be ideal (error free and noiseless), and therefore, any detected noise is the result of an eavesdropper attacking the channel.

2.1 Randomization-based ASQKD

Suppose that Alice and Bob have a pre-shared secret key, $K_1 \in \{0, 1\}^{N+M}$, which is used to determine the positions of checking particles and $N + M$ is a security parameter according to the security requirement. The process of the randomization-based protocol is described in detail as follows (shown in Fig. 1):

Step 1 Alice determines a string of classical bits, $\mathrm{SK} \in \{0, 1\}^N$, as the distributed session key. She puts $\mathrm{SK}||K_1$, where $||$ denotes concatenation operator, into the hash function H and then gets an M-bit hash value, h_{SK}. Alice generates a sequence of $N + M$ single particles (i.e., S_{A}) in Z-basis corresponding to SK and h_{SK}.

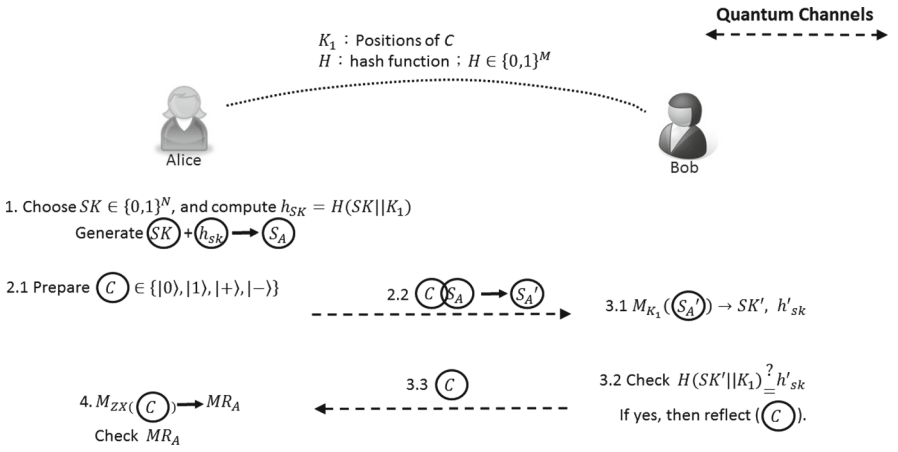

Fig. 1 Proposed randomization-based ASQKD

Step 2 Alice prepares a set of single particles, C, randomly in one of the four polarization states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ as the checking particles. She inserts C into S_{A} based on K_1 to form a new sequence S'_{A} (If the i-th bit of the secret key $K_1 = 1$, Alice puts a checking particle in front of the i-th particle of S_{A}. Otherwise, she puts a checking particle in the back, for instance). Then Alice sends the sequence S'_{A} to Bob via a quantum channel.

Step 3 For each arrived particle, if it is a member of S_{A}, Bob measures it to derive SK' and h'_{SK} by the pre-agreed rules based on K_1. Otherwise, Bob prepares to reflect it without any disturbance. It is noteworthy that Bob puts every reflected particle into the delay line device whose traveling time is long enough to wait for the last reflected particle enters. After receiving all the particles of the sequence S'_{A}, Bob puts $\mathrm{SK}'||K_1$ into H and then compares the output with h'_{SK}. If $H(\mathrm{SK}'||K_1) = h'_{\mathrm{SK}}$, Bob can verify that the session key $\mathrm{SK}' = \mathrm{SK}$ which is sent by Alice. Then Bob sends all the reflected particles out in the original order to Alice. If Bob checks $H(\mathrm{SK}'||K_1) \neq h'_{\mathrm{SK}}$, he informs Alice to terminate the protocol and start it again.

Step 4 After receiving all the reflected particles (i.e., the sequence C), Alice measures C in the bases she prepared and then compares the measurement results with the initial states. If the error rate is higher than the pre-defined threshold, Alice informs Bob to abort the protocol. Otherwise, Alice can verify that the sequence is definitely sent from Bob.

In the above protocol, if the checks performed by Bob and Alice in Step 3 and Step 4 are correctly processed, no classical channel is needed and the pre-shared secret key K_1 can be used multiple times. However, if the checks are not passed or the protocol does not complete successfully, Alice and Bob must terminate the protocol and start it again. They may also verify whether there exists an eavesdropping attack in the processes of the protocol. Accordingly, an authenticated classical channel is required for the verification. Moreover, they should change the pre-shared secret key K_1 if the check processes have been failed many times (exceeding a threshold, e.g., $\frac{N+M}{2}$ times).

By utilizing the delay line device to postpone transmitting the reflected particles until the last one has entered and the result of $H(\mathrm{SK}'||K_1) = h'_{\mathrm{SK}}$ has obtained, the outside eavesdropper cannot tell which particles are measured and which are reflected by Bob in the sequence. As a consequence, the eavesdropper's CNOT attack [13] can be prevented. Furthermore, the proposed protocol does not need an additional pre-shared key for rearranging the particles.

In the proposed protocol, a public secure one-way hash function H is used for verifying the integrity of the session key. On the basis of the property of the one-way hash function, one-bit error in the input will cause significant changes in the output. This property is very useful in checking message integrity if the quantum channel is reliable or ideal. On the other hand, in reality, some states of the transmitted qubits may be changed due to the unexpected interference of the optical fiber or due to the environment. These changes of the transmitted qubits caused by noises would be detected as an eavesdropping attack, and then, Alice and Bob would always abort the protocol. The usage of one-way hash function makes the protocol very intolerant of any noise. To remedy this problem, error-correcting codes can be applied to encode the bit sequence $\mathrm{SK}+h_{\mathrm{SK}}$. This means, in Step 1, Alice can encode the sequence $\mathrm{SK}+h_{\mathrm{SK}}$ in a redundant way by using an error-correcting code. The redundancy allows Bob to detect and then to correct a limited number of errors when he derives the SK' and h'_{SK} in Step 3. The adoption of error-correcting codes may require a longer secret key K_1 to generate the sequence S'_{A} in Step 2. However, as a result, the small errors can be corrected by the introduced error-correcting codes, and the majority errors due to malicious eavesdroppers can be detected by the one-way hash function. By combining error-correcting codes and a one-way hash function with quantum mechanics, the proposed protocol can provide data privacy as well as message integrity on the noisy quantum channel.

2.2 Measure-resend ASQKD

In the measure-resend protocol, Alice and Bob pre-share a master secret key, which is divided into two parts, $K_1 \in \{0, 1\}^{N+M}$ and $K_2 \in \{0, 1\}^{N+M}$. K_1 is used to determine the positions of the checking particles, and K_2 is used to select either measurement or reflection. The detailed process is described as follows (shown in Fig. 2):

Step 1 Follow the same process in Sect. 2.1, Alice generates a sequence S_{A}, which contains SK and h_{SK}.

Step 2 Alice prepares a set of maximally entangled Bell states $S = \{s_1, s_2, \ldots, s_{N+M}\}$ in $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, where $s_i = \{q^i_{\mathrm{A}}, q^i_{\mathrm{B}}\}$, for $i = 1, 2, \ldots, N+M$. Alice divides these pairs into two sequences, $C_{\mathrm{A}} = \{q^i_{\mathrm{A}}\}$ and $C_{\mathrm{B}} = \{q^i_{\mathrm{B}}\}$, which include all the first and second particles of S, respectively, for $i = 1, 2, \ldots, N+M$. Alice keeps the sequence C_{A} for her own and inserts C_{B} into the sequence S_{A} based on K_1 to form a new sequence S'_{A}. After that, Alice sends the sequence S'_{A} to Bob via the quantum channel.

Step 3 For each arrived particle, if it is a member of S_{A} based on K_1, Bob measures it to derive SK' and h'_{SK}, and then prepares and sends a qubit in $\{|0\rangle, |1\rangle\}$ to Alice

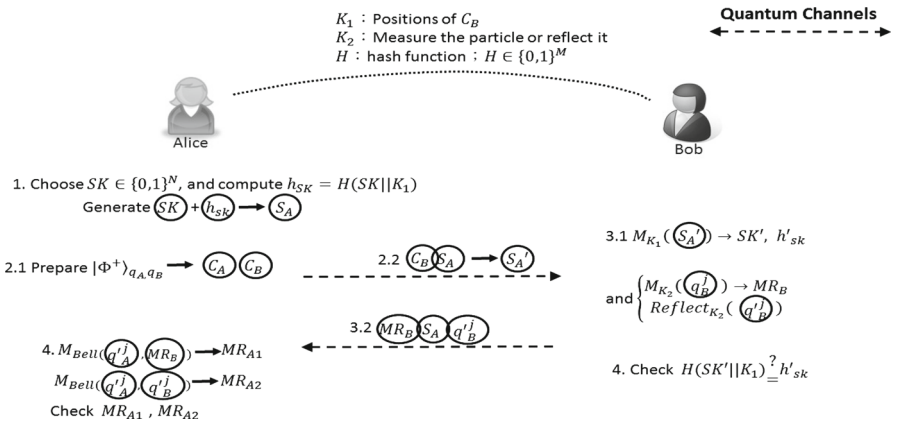

Fig. 2 Proposed measure-resend ASQKD

according to the measurement result. If the particle belongs to C_B, Bob decides either to measure it or to reflect it based on K_2. That is, if the j-th bit of the secret key $K_2 = 1$, Bob measures $|q_B^j\rangle$ and then returns a qubit in the same state as the measurement result (denoted by MR_B) to Alice. Otherwise, Bob reflects it (denoted by $|q'^j_B\rangle$) back to Alice without disturbance.

Step 4 After receiving all the returned particles, Alice begins to check the security of the channel:

- First, if j-th bit of the secret key $K_2 = 1$, she performs a Bell measurement on $\{q_A^j, q_B^j\}$ to detect whether the eavesdropper intercepts the sequence S'_A and then directly sends it back to her. More precisely, after Bob measures the second particle $|q_B^j\rangle$ of s_j in the Z-basis, Alice's measurement result MR_{A1}^j will be one of the two possibility ($|\Phi^+\rangle$ and $|\Phi^-\rangle$). If MR_{A1} are all still in the state $|\Phi^+\rangle$, it indicates that the sequence S'_A is suffering from the reflecting attack. Accordingly, the protocol will be aborted.
- Second, Alice performs Bell measurements again on the remaining pairs $\{q'^j_A, q'^j_B\}$ of S to check the entanglement correlation (i.e., the corresponding Bell states of $K_2 = 0$ should be $|\Phi^+\rangle$). If the error rate of measurement results MR_{A2} is higher than the pre-defined threshold, the protocol will be aborted. Otherwise, Alice can verify that the returned sequence is actually sent from Bob.

Meanwhile, Bob inputs the derived key $SK'||K_1$ to H and then compares the output with h'_{SK}. If the comparison is negative, the protocol will be aborted. Otherwise, Bob can also verify that the session key $SK' = SK$ which is sent from Alice.

The same as the proposed randomization-based ASQKD, the above protocol does not need a classical channel if all checks in Step 4 are correctly processed. However, if the checks are not passed or the protocol does not complete successfully, Alice and Bob must abort the protocol and then restart the protocol or use an authenticated classical channel to verify whether there exists an eavesdropping attack.

3 Security analyses

Basically, all existing semi-quantum protocols that have two transmissions of the same quantum signals, i.e., first from Alice to Bob and then from Bob to Alice, suffer from the Trojan-horse attacks [25–27]. To prevent this kind of attacks, the photon number splitter device and the wavelength filter device could be adopted [28–30]. In this section, we discuss three kinds of eavesdropper's attacks usually applied in the scenario where the authenticated channels are unavailable: (1) impersonation attack, (2) modification attack, and (3) intercept-resend attack. We show that the proposed ASQKD protocols are effective to detect such three attacks.

3.1 Security against impersonation attacks

- *The randomization-based protocol*

In the impersonation attacks, an outside eavesdropper, Eve, may try to impersonate a legitimate participant to communicate with the other one. Firstly, it is assumed that Eve intends to impersonate Alice. In Step 1 of the protocol, Eve must prepare two strings SK^E and h_{SK}^E. However, without the knowledge of the secret key K_1, it is difficult to produce the correct hash value h_{SK}^E in which $h_{\mathrm{SK}}^E = H(\mathrm{SK}^E||K_1)$. Moreover, it is also difficult for Eve to properly prepare the quantum sequence S'_{E} in Step 2 without knowing the secret key K_1. Consequently, Bob is sure to obtain incorrect measurement results and the check process will fail in Step 3 if Eve try to impersonate Alice.

On the other hand, Eve may try to impersonate Bob to share a session key with Alice. Eve can intercept the sequence S'_{A} and then performs the Z-basis measurements to derive Alice's SK and h_{SK}. However, without knowing the secret key K_1, Eve has no idea which positions in S'_{A} belong to SK and h_{SK}. She is thus unable to send the correct checking sequence C back to Alice in Step 3. Accordingly, Alice will find out the error by checking the particles of C in Step 4 and the impersonation attack made by Eve will fail.

- *The measure-resend protocol*

The same as the above analysis, it is difficult for Eve to prepare SK^E, h_{SK}^E, and the quantum sequence S'_{E} without the knowledge of the secret key K_1. Thus, Eve cannot impersonate Alice because the check process performed by Bob in Step 4 of the measure-resend protocol will fail.

Now, assume that Eve tries to impersonate Bob to communicate with Alice. She intercepts the sequences S'_{A} and performs the Z-basis measurements in Step 2. However, without knowing the secret key K_1, Eve cannot derive Alice's SK and h_{SK}. Besides, because Eve does not know the secret key K_2, she cannot properly decide to either measure or reflect the particle of C_{B}. If Eve measures the particles which are used for checking the entanglement of the Bell states, Alice will notice that the measurement results MR_{A2} are not consistent. More precisely, for each Bell state $|\Phi^+\rangle$, there is a probability of $\frac{1}{2}$ that Eve makes a wrong decision to either measure or reflect the particle of C_{B}. There is a probability of $\frac{1}{2}$ that Alice will get the original state

if the entanglement correlation is broken by Eve's Z-basis measurement. Therefore, there are approximately $\frac{N+M}{2}$ pairs used for entanglement check. In this regard, the probability of getting all the measurement results in $|\Phi^+\rangle$ will become $(\frac{1}{2})^{\frac{N+M}{2}}$. If the number of $(N + M)$ is large enough, Eve's attack will be certainly detected by Alice in Step 4.

3.2 Security against modification attacks

- *The randomization-based protocol*

In the modification attack, the outside eavesdropper, Eve, will try to alter the contents of transmitted messages on the channel. In the proposed randomization-based protocol, Eve is unable to accurately replace Alice's SK and h_{SK} in the sequence S'_{A} without the knowledge of the secret key K_1. Therefore, consider that Eve intercepts the sequence S'_{A} in Step 2. She randomly applies the unitary operator $i\sigma_y$ $(= |0\rangle\langle 1| - |1\rangle\langle 0|)$ to S'_{A} for arbitrary modification. However, it definitely results in changing the states of the particles in both S_{A} and C. Accordingly, Alice and Bob will detect Eve's modification attack by the subsequent comparison in Step 3 and Step 4.

- *The measure-resend protocol*

Likewise, Eve arbitrarily applies the unitary operator $i\sigma_y$ (or $\sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1|$) to the sequence S'_{A} for altering the messages sent from Alice to Bob. However, once the states of the particles are changed, Bob necessarily obtains incorrect measurement results SK$'$ and h'_{SK}. As a consequence, Bob will find out the error in Step 4. On the other hand, the Bell states will be transformed from $|\Phi^+\rangle$ into $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ (or $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$) after Eve performs the unitary operations. In this case, if the corresponding bits of $K_2 = 0$, Alice can never get the expected state $|\Phi^+\rangle$ by the Bell measurements. Besides, if the corresponding bits of $K_2 = 1$, Alice's Bell measurement results will be $|\Psi^+\rangle$ or $|\Psi^-\rangle$ at random after Bob performs the Z-basis measurements. No matter what results Alice found, Eve's modification will be detected in Step 4.

3.3 Security against intercept-resend attacks

- *The randomization-based protocol*

In the intercept-resend attack, Eve may first intercept the sequence S'_{A} sent by Alice in Step 2. She then has three possible activities to manipulate the sequence S'_{A}. The first, Eve may perform the Z-basis measurement on the sequence S'_{A} and then resend Bob a new quantum sequence according to the measurement results. This activity permits the check process performed by Bob in Step 3 to be passed. However, because Eve does not know the secret key K_1 and the exact polarization states of the checking particles C, the original states of the checking particles C must be disturbed. The check

process performed by Alice in Step 4 is surely failed. Alice will inform Bob to abort the protocol. The second, Eve may preserve the sequence S'_A for later resending to Bob. Since Alice sent Bob the sequence S'_A in Step 2 and does not receive Bob's response in Step 4, she must communicate with Bob to abort the protocol due to the incompleteness of protocol. Eve's attack will thus be found. The third, Eve may perform a bit-by-bit online guessing (BOG) attack over the sequence S'_A. More precisely, Eve performs the Z-basis measurement on one particle at a time (say starting from the first particle) over the sequence S'_A. Eve produces an opposite polarization state according to the measurement result (e.g., if the measurement result is $|0\rangle$, Eve produces $|1\rangle$) to replace the first particle of the sequence S'_A. Then, Eve resends the modified sequence S'_A to Bob and observes Bob's reaction. If Bob stops doing the protocol, Eve recognizes that the first particle is a member of S_A and the first bit of K_1 is "0". On the other hand, if Bob continues doing the protocol, Eve recognizes that the first particle is a member of C and the first bit of K_1 is "1." Each BOG attack may reveal one bit of the secret key K_1. Because the sequence S'_A is organized into pairs—each pair contains a member of S_A and a member of C, Eve needs to perform $N + M$ BOG attacks to reveal the whole secret key K_1. However, with the assumption of an ideal quantum channel, if the position of the substituted particle belongs to S_A, Eve's BOG attack will surely be detected by Bob in Step 3. If the position of the substituted particle belongs to C, there is a probability of $\frac{1}{4}$ that Alice agrees the check process in Step 4. In this regard, the probability that Eve reveals the whole secret key K_1 without being detected by Alice or Bob will be $(\frac{1}{8})^{N+M}$. If the number of $(N + M)$ is large enough, Eve's attack will be certainly detected. In addition, if the check processes performed by Alice and Bob have been failed many times (exceeding a threshold, e.g., $\frac{N+M}{2}$ times), they should change the pre-shared secret key K_1 according to the security requirement. On the other hand, with the assumption of using error-correcting codes, Eve's BOG attack will be treated as an error and then be corrected. Thus, the BOG attack cannot work in this assumption.

- *The measure-resend protocol*

The same as the above description, Eve has three possible activities after intercepting the sequence S'_A. The security analyses of first two activities are the same as the above analyses in which Eve's attacks will be detected by Alice in Step 4. In the third activity, Eve may perform a BOG attack over the sequence S'_A. There is a probability of $\frac{1}{2}$ that the substituted particle is a member of S_A and Eve's attack will be detected by Bob in Step 4. If the substituted particle is a member of C_B, there is a probability of $\frac{3}{4}$ that Alice agrees the check process in Step 4. Accordingly, the probability that Eve reveals the whole secret key K_1 without being detected by Alice and Bob will be $(\frac{3}{8})^{N+M}$. If the number of $(N + M)$ is large enough, Eve's attack will be certainly detected.

Basically, both proposed ASQKD protocols are secure against Eve's intercept-resend attacks. However, Eve may perform a "replay attack" in which she first intercepts the sequence of qubits sent by Alice and measures them in the Z basis, and then, she uses the measurement results to impersonate Alice to prepare and send Z basis qubits to Bob. Since the secret portion is identical to what Alice sent, Bob always thinks the session key SK is properly sent by Alice. Although Eve knows

nothing about the session key SK, she may make Bob to use the same SK for some cryptographic purpose many times. This attack may make the session key SK insecure if it is used as a one-time pad. Both proposed ASQKD protocols are difficult to resist the replay attack because of the adoption of two-step transmission. Two suggestions can be considered to remedy this attack. First, Bob can keep a record of all used keys and abort the protocol if he receives the same twice. Secondly, the proposed measure-resend protocol adopts three-step transmission rather than two-step transmission. That is, Bob starts the protocol by choosing a random number N. Then, he encodes N into Z basis qubits and sends them to Alice. After receiving the qubits, Alice decodes them to get N and uses $N||\mathrm{SK}||K_1$ as the input of the hash function H. Then, Alice continues the rest of steps of the proposed measure-resend protocol. Since the random number N selected by Bob is different every execution of the protocol and Eve cannot generate the correct hash value h^E_{SK} in which $h^E_{\mathrm{SK}} = H(N||\mathrm{SK}^E||K_1)$, Eve cannot impersonate Alice to make Bob to use the same session key SK twice for one-time pad.

4 Comparison

The ASQKD protocols proposed by Yu et al. [18] and this study are designed to distribute a shared session key without the assumption of the authenticated channels. However, in Yu et al.'s [18] ASQKD protocols, public classical channels are still needed by Alice and Bob to exchange checking information during the processes of protocols. By contrast, the proposed ASQKD protocols do not need classical channels (including public and authenticated classical channels) during the course of the protocol execution unless a suspected eavesdropping attack has been detected. The proposed ASQKD protocols have several advantages as compared to Yu et al.'s [18] ASQKD protocols (given in Table 1).

Table 1 Comparison between two ASQKD studies

	Randomization-based		Measure-resend	
	Yu et al.'s ASQKD	Proposed ASQKD	Yu et al.'s ASQKD	Proposed ASQKD
Quantum resources	Bell states	Single particles	Bell states	Bell states
Qubit efficiency	$\frac{1}{8}$	$\frac{1}{4}$	$\frac{1}{10}$	$\frac{1}{9}$
The bit number of the pre-shared keys	3(N+M)	(N+M)	3(N+M)	2(N+M)
Classical channels required during key distribution	3	0	1	0

In Table 1, the qubit efficiency [31] is defined as follows:

$$QE = \frac{b_s}{q_t},$$

where the parameter b_s denotes the number of secret key bits shared between the participants and q_t denotes the total number of generated qubits. It is assumed that the length of session key SK is equal to the length of hashing value h_{SK} (i.e., $N = M$). In addition, the number of bit "1" and bit "0" in the secret key K_2 is equal. Thus, we can see that the qubit efficiency of the proposed randomization-based protocol is $\frac{1}{4}$, namely $\frac{N}{(N+M)+(N+M)}$, where $(N + M) + (N + M)$ is the length of sequence S'_{A}.

The qubit efficiency of the proposed measure-resend protocol is $\frac{1}{9}$, namely

$$\frac{N}{(N + M) + 2(N + M) + (N + M) + \frac{1}{2}(N + M)},$$

where $(N + M) + 2(N + M) + (N + M) + \frac{1}{2}(N + M)$ represents the total number of generated qubits for S_{A}, the bell states S (i.e., $C_{\mathrm{A}} + C_{\mathrm{B}}$), Bob's S_{A} and MR_{B}. It is obvious that the qubit efficiency of the proposed randomization-based protocol and the measure-resend protocol is better than Yu et al.'s ($\frac{1}{8}$ and $\frac{1}{10}$). Nevertheless, if the check steps are not passed or the protocol does not complete successfully, Alice and Bob must terminate the protocol and start it again. In this situation, the qubit efficiency of both Yu et al.'s protocols and the proposed protocols will become "0." Besides, the bit number of the pre-shared secret keys in the proposed ASQKD protocols is $(N+M)$ and $2(N+M)$, which are fewer than Yu et al.'s need. Furthermore, no classical channel is required during our protocol execution.

5 Conclusion

This paper has proposed two variants of the ASQKD protocol which follow the setting of Boyer et al.'s semi-quantum scenario. The proposed ASQKD protocols are simplified to design by abandoning the usage of classical channels and merely utilize two-step transmission to complete the distribution of a session key. The pre-shared secret keys K_1 and K_2 can be used many times if the protocols are properly completed and no attacks are detected. However, if Alice and Bob detected a suspected attack during the course of the protocol execution, they should abort the process and restart the protocol. In addition, depending on the requirement of security, Alice and Bob may need to change the pre-shared secret keys if the check processes have been failed many times (exceeding a threshold, e.g., $\frac{N+M}{2}$ times).

Compared to Yu et al.'s ASQKD protocols, the proposed ASQKD protocols have better qubit efficiency and less pre-shared keys. Although the adoption of one-way hash function makes the quantum channel very intolerant of any noise, the error-correcting codes are suggested to relieve this problem. This paper has shown that the proposed ASQKD protocols are secure against the impersonation attacks, the modification attacks and the intercept-resend attacks which commonly occur in the

scenario of non-authenticated channels. Since the proposed protocols use two-step transmission to complete the distribution of a session key, they are difficult to resist the "replay attack." This paper gives two suggestions to remedy this attack, one is to ask Bob to keep a record of all used keys, and the other is to apply three-step transmission instead of two-step transmission. Nevertheless, both suggestions would add another level of complexity to the proposed protocols. Therefore, how to design an efficient ASQKD protocol which is secure against the replay attack will be an interesting future research.

Acknowledgments The authors would like to thank the editor and the anonymous reviewers for their very helpful and valuable comments to enhance the clarity of the manuscript. The authors also thank the Ministry of Science and Technology of the Republic of China, Taiwan, for partially supporting this research in finance under the Contract no. MOST 103-2221-E-471 -001 - and MOST 103-2221-E-006 -177 -.

References

1. Wiesner, S.: Conjugate coding. SIGACT News **15**(1), 78–88 (1983)
2. Bennett, C. H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175–179 (1984)
3. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**(6), 661–663 (1991)
4. Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without Bell's theorem. Phys. Rev. Lett. **68**(5), 557–559 (1992)
5. Cabello, A.: Quantum key distribution without alternative measurements. Phys. Rev. A **61**(5), 052312, (2000)
6. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**(3), 032302 (2002)
7. Li, C., Song, H.S., Zhou, L., Wu, C.F.: A random quantum key distribution achieved by using Bell states. J. Opt. B Quantum Semiclassical Opt. **5**(2), 155–157 (2003)
8. Hwang, T., Lee, K.C.: EPR quantum key distribution protocols with potential 100 % qubit efficiency. IET Inf. Secur. **1**(1), 43–45 (2007)
9. Li, X.H., Deng, F.G., Zhou, H.Y.: Efficient quantum key distribution over a collective noise channel. Phys. Rev. A **78**, 022321 (2008)
10. Shih, H.C., Lee, K.C., Hwang, T.: New efficient three-party quantum key distribution protocols. IEEE J. Sel. Topics Quantum Electron. **15**(6), 1602–1606 (2009)
11. Hong, C.H., Heo, J.O., Khym, G.L., Lim, J., Hong, S.-K., Yang, H.J.: Quantum channels are sufficient for multi-user quantum key distribution protocol between users. Opt. Commun. **283**(12), 2644–2646 (2010)
12. Zhou, N., Wang, L., Gong, L., Zuo, X., Liu, Y.: Quantum deterministic key distribution protocols based on teleportation and entanglement swapping. Opt. Commun. **284**(19), 4836–4842 (2011)
13. Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical Bob. Phys. Rev. Lett. **99**(14), 140501 (2007)
14. Boyer, M., Gelles, R., Kenigsberg, D., Mor, T.: Semiquantum key distribution. Phys. Rev. A **79**(3), 032341 (2009)
15. Zou, X., Qiu, D., Li, L., Wu, L., Li, L.: Semiquantum-key distribution using less than four quantum states. Phys. Rev. A **79**(5), 052312 (2009)
16. Zhang, X.Z., Gong, W.G., Tan, Y.G., Ren, Z.Z., Guo, X.T.: Quantum key distribution series network protocol with M-classical Bobs. Chin. Phys. B **18**(6), 2143 (2009)
17. Wang, J., Zhang, S., Zhang, Q., Tang, C.J.: Semiquantum key distribution using entangled states. Chin. Phys. Lett. **28**(10), 100301 (2011)
18. Yu, K.F., Yang, C.W., Liao, C.H., Hwang, T.: Authenticated semi-quantum key distribution protocol using Bell states. Quantum Inf. Process. **13**(6), 1457–1465 (2014)
19. Li, Q., Chan, W.H., Long, D.-Y.: Semiquantum secret sharing using entangled states. Phys. Rev. A **82**(2), 022303 (2010)

20. Wang, J., Zhang, S., Zhang, Q., Tang, C.-J.: Semiquantum secret sharing using two-particle entangled state. Int. J. Quantum Inf. **10**(05), 1250050 (2012)
21. Li, L., Qiu, D., Mateus, P.: Quantum secret sharing with classical Bobs. J. Phys. A Math. Theor. **46**(4), 045304 (2013)
22. Yang, C.-W., Hwang, T.: Efficient key construction on semi-quantum secret sharing protocols. Int. J. Quantum Inf. **11**(05), 1350052 (2013)
23. Lin, J., Yang, C.-W., Tsai, C.-W., Hwang, T.: Intercept-resend attacks on semi-quantum secret sharing and the improvements. Int. J. Theor. Phys. **52**(1), 156–162 (2013)
24. Yang, C.W., Hwang, T., Lin, T.H.: Modification attack on QSDC with authentication and the improvement. Int. J. Theor. Phys. **52**(7), 2230–2234 (2013)
25. Yang, C.W., Hwang, T., Luo, Y.P.: Enhancement on quantum blind signature based on two-state vector formalism. Quantum Inf. Process. **12**(1), 109–117 (2013)
26. Deng, F.G., Zhou, P., Li, X.H., Li, C.Y., Zhou, H.Y.: Robustness of two-way quantum communication protocols against trojan horse attack. Quantum Phys. (2005). arXiv:quant-ph/0508168v1z
27. Cai, Q.Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A **351**(1–2), 23–25 (2006)
28. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A **72**(4), 044302 (2005)
29. Li, X.H., Deng, F.G., Zhou, H.Y.: Improving the security of secure direct communication based on the secret transmitting order of particles. Phys. Rev. A **74**(5), 054302 (2006)
30. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A **73**(4), 049901 (2006)
31. Lin, J., Hwang, T.: An enhancement on Shi et al.'s multiparty quantum secret sharing protocol. Opt. Commun. **284**(5), 1468–1471 (2011)