Quantum Inf Process (2016) 15:947–958
DOI 10.1007/s11128-015-1182-y

Authenticated semi-quantum direct communication protocols using Bell states

Yi-Ping Luo[1] · **Tzonelih Hwang**[1]

Received: 1 April 2015 / Accepted: 2 November 2015 / Published online: 18 November 2015

Abstract This study presents the first two authenticated semi-quantum direct communication protocols without using any classical channel. By pre-sharing a master secret key between two communicants, a sender with advanced quantum devices can transmit a secret message to a receiver who can only perform classical operations without any information leakage. The receiver is then capable of verifying the message up to the single-qubit level, i.e., a one-qubit modification of the transmitted quantum sequence can be detected with a probability close to 1. Moreover, the proposed protocols are resistant to several well-known attacks.

Keywords Authentication · Authenticated semi-quantum communication · Bell states · Quantum communication · Quantum cryptography · Semi-quantum communication

1 Introduction

Authentication, which is a process used for guaranteeing the integrity and origin of a transmitted message, is an important topic in information security. Due to authentication of the message, the receiver (the verifier) can determine whether or not he/she is communicating with the alleged participant (the sender). Moreover, authentication concerns also about verifying the integrity of the received message. The feature of

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

Yi-Ping Luo
yiping@ismail.csie.ncku.edu.tw

[1] Department of Computer Science and Information Engineering, National Cheng Kung University, No. 1, Ta-Hsueh Rd., Tainan, Taiwan, ROC

authentication is a very important requirement in various quantum cryptographic environments, such as quantum key distribution (QKD) protocols, quantum secure direct communications (QSDC), deterministic secure quantum communications (DSQC), quantum dialogue (QD), quantum private comparison (QPC), and quantum secret sharing (QSS). To simplify the design, however, the majority of the above-mentioned environments focus on the following two methods of providing secrecy as well as authentication.

1. An authenticated classical channel (i.e., transmitted information that can be eavesdropped but not modified) is assumed to be available for providing authentication, which can be further used for detecting eavesdropping. Accordingly, both the information integrity and originality can be guaranteed. In practice, however, if two communicants want to communicate with each other, the QKD or QSDC protocol must be performed whenever a communication session is initiated. That is, both communicants must be in an environment where an authenticated classical channel is available, which could be a restriction for some applications. For example, a traveling mobile user will have difficulty maintaining an authenticated classical channel with low-power mobile devices.
2. All participants are required to have quantum capabilities. That is, the protocol requires that every participant has access to quantum memory and has the ability to prepare/measure arbitrary quantum states and to perform operations. However, not all participants can afford such expensive quantum resources and operations for various applications. In this case, it will be difficult to apply these protocols in practical environments.

To resolve these issues, Yu et al. [1] proposed authenticated semi-quantum key distribution (ASQKD) protocols. In these protocols, by pre-sharing a master secret key between two communicants, a sender with advanced quantum devices can transmit a working key to a receiver, who can only perform classical operations, without requiring an authenticated classical channel. According to the definition in [2,3], the term "semi-quantum" implies that the sender, Alice, is a powerful quantum communicant, whereas the receiver, Bob, has only classical capabilities. More precisely, the sender (Alice) has the ability to perform following operations: (a) prepare any quantum state such as single photons and Bell states, (b) perform any quantum measurement such as Bell measurement and multi-qubit joint measurement, and (c) store qubits in a quantum memory. Conversely, the classical receiver (Bob) is restricted to performing the following operations over the quantum channel: (1) prepare new qubits in the classical basis $\{|0\rangle, |1\rangle\}$ (i.e., the Z basis), (2) measure qubits in the classical basis, (3) reorder the qubits via different delay lines, and (4) send or reflect the qubits without disturbance. In this regard, since Bob would always be working with qubits in the $\{|0\rangle, |1\rangle\}$ basis, he should not be able to obtain any quantum superpositions of the $\{|0\rangle, |1\rangle\}$ basis. In this case, the qubits here can be considered as classical bits, and the operations [i.e., (1) to (4)] are considered as classical operations. This kind of Bob is designated as classical Bob and the QKD protocol that involves such Bob's is called the semi-QKD protocol (or QKD protocol with classical Bob).

Following Boyer et al., Yu et al. also proposed two types of ASQKD protocols, namely randomization-based ASQKD and measure-resend ASQKD. The difference

between these two protocols lies in the capability of the classical Bob. In the randomization-based ASQKD protocol, classical Bob is limited to performing operations (2), (3), and (4), whereas in the measure-resend ASQKD protocol, classical Bob is limited to performing operations (1), (2), and (4). Because the ASQKD protocol allows a classical Bob to be a receiver and does not require an authenticated classical channel, an authenticated semi-quantum protocol can reduce not only the computational burden of the communicants but also the cost of the quantum hardware devices in practical implementations.

In this paper, we propose authenticated semi-quantum direct communication (ASQDC) protocols using Bell states. To the best of our knowledge, there is no existing ASQDC protocol that enables the quantum sender to directly send a secret message to the classical receiver without any information leakage. Furthermore, the proposed ASQDC protocols have the following features:

1. The protocols do not require any classical channel.
2. The pre-shared secret key between two communicants can be reused.
3. The protocols can satisfy the requirements of a quantum direct communication protocol, which was defined by Deng et al. [4]. First, the secret messages should be directly read out by the legitimate user Bob when he receives the quantum states, and no additional classical information is needed after the qubit transmission. Second, the secret messages, which have been previously encoded with quantum states, should not leak even though an eavesdropper may access the channel.
4. The security of the proposed ASQDC protocols is guaranteed by quantum mechanics, i.e., by the uncertainty of quantum measurement and the no-cloning theory.
5. The protocols can resist impersonation attacks, intercept-and-resend attacks, modification attacks, and other well-known attacks.

Therefore, the proposed ASQDC protocols can be useful in various physical environments, such as in a client server paradigm, where a client (say Bob) having resource constraint devices (such as mobile device) wants to acquire some messages from the server. In order to ensure the higher level of security in their communication, both the client and server desire to use quantum communications. In this case, our proposed protocols can be highly expedient, where the quantum party having advanced quantum devices will be considered as a service provider. On the other hand, the classical party, having resource constraint devices with only basic quantum operations, will be treated as a client (classical Bob).

The remainder of this paper is organized as follows. Section 2 presents the proposed ASQDC protocols using Bell states. Section 3 provides security analyses of the proposed protocols. Finally, our conclusions are given in Sect. 4.

2 Proposed ASQDC protocols

This section presents two ASQDC protocols, which enable a quantum sender, Alice, to send an $\frac{n}{8}$-bit secret message m to a classical receiver, Bob. In Sect. 2.1, the randomization-based protocol is proposed. After that, the measure-resend one is given.

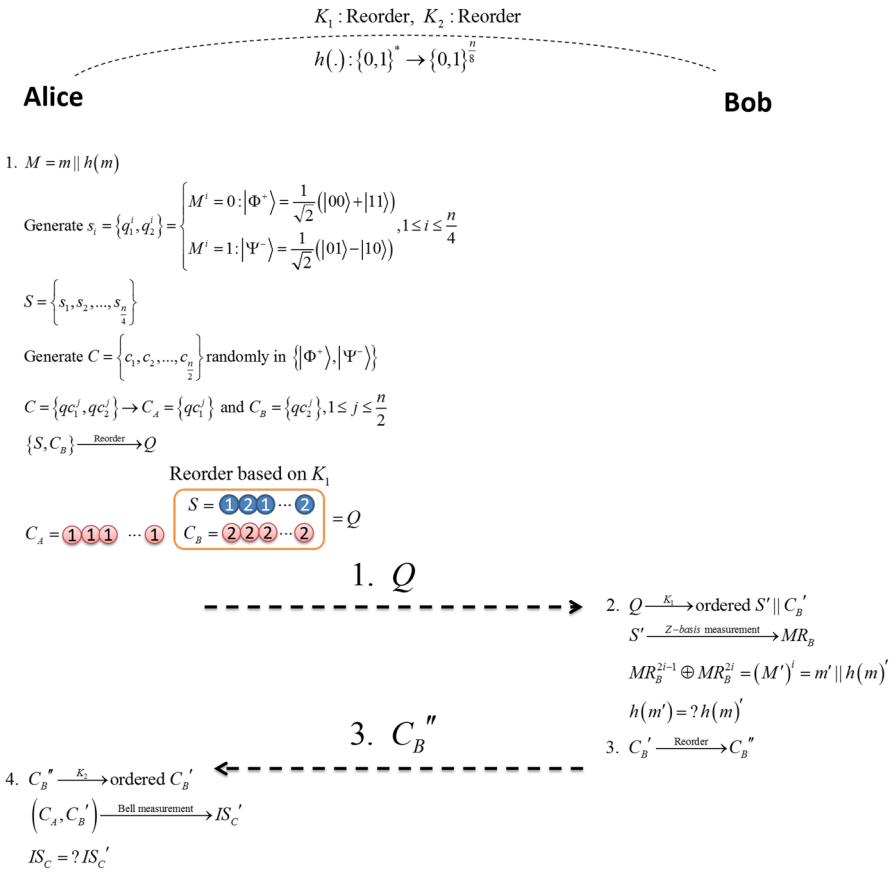

Fig. 1 The proposed randomization-based ASQDC protocol

2.1 Randomization-based ASQDC protocol

Let us assume that Alice and Bob pre-shared two secret keys K_1 and K_2, where $K_1 \in \{0, 1\}^n$ and $K_2 \in \{0, 1\}^{\frac{n}{2}}$. Besides, the quantum channels here are assumed to be noiseless and lossless. The procedure of the randomization-based ASQDC is described in the following steps (see also Fig. 1):

Step 1 Alice calculates $M = m||h(m)$, where '||' denotes concatenation and $h()$ is a one-way hash function [5,6] to produce an $\frac{n}{8}$-bit checking value of m. After that, Alice generates a sequence of Bell states, $S = \{s_1, s_2, \ldots, s_{\frac{n}{4}}\}$, based on M, where $s_i = \{q_1^i, q_2^i\}$ for $i = 1, 2, \ldots, \frac{n}{4}$. That is, if the ith bit of M is zero, i.e., $M^i = 0$, Alice produces s_i in $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Otherwise, Alice produces $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. Then, Alice generates the checking state $C = \{c_1, c_2, \ldots, c_{\frac{n}{2}}\}$ randomly in the states of $|\Phi^+\rangle$ and $|\Psi^-\rangle$ whose initial state is denoted as IS_C, where $c_j = \{qc_1^j, qc_2^j\}$ for $j = 1, 2, \ldots, \frac{n}{2}$. After

that, she divides these $\frac{n}{2}$ Bell states into two ordered sequences, $C_A = \{qc_1^j\}$ and $C_B = \{qc_2^j\}$. Now, she reorders the quantum sequences S and C_B together according to the secret key K_1 to obtain the new quantum sequence Q. After the above preparation, Alice retains the sequence C_A and sends the sequence Q to Bob.

Step 2 When Bob receives the qubits in Q, he puts every qubit into the delay line device whose traveling time is long enough to wait for the last qubit enters so that he can get the ordered sequence S' and C'_B according to K_1. After that, he performs a Z-basis measurement on each qubit in S' and obtains the measurement result MR_B. Then, Bob can calculate $(M')^i = MR_B^{2i-1} \oplus MR_B^{2i}$ to derive $M' = m'||h(m)'$. That is, if $MR_B = 00$ (11), then $M' = 0 \oplus 0 = 0$ ($1 \oplus 1 = 0$). If $MR_B = 01$ (10), then $M' = 0 \oplus 1 = 1$ ($1 \oplus 0 = 1$). Bob calculates $h(m')$ and compares it with the received $h(m)'$. If $h(m') = h(m)'$, Bob believes that the message m' is indeed sent from Alice without any disturbance. Otherwise, Alice and Bob will terminate the protocol and start it again.

Step 3 Bob reorders the qubits C'_B based on the secret key K_2 to obtain C''_B and reflects C''_B back to Alice via different delay lines.

Step 4 Upon receiving C''_B, Alice can recover the reflected qubits in the correct order based on K_2 to obtain the ordered sequence $C'_B = \{(qc'_2)^j\}$. Then Alice performs Bell measurement on $\{qc_1^j, (qc'_2)^j\}$ for $j = 1, 2, \ldots, \frac{n}{2}$ to obtain IS'_C and then check whether each corresponding set of two qubits in IS'_C is consistent with the states she generated in Step 1, IS_C. If the transmission between Alice and Bob is secure, then it means Alice has successfully transmitted the secret message to Bob.

2.2 Measure-resend ASQDC protocol

Here, a measure-resend ASQDC protocol, which modifies the operations that Bob is allowed to perform in the randomization-based ASQKD described in Sect. 2.1, is as follows (see also Fig. 2). The modified steps (*) are listed in detail, as follows. The others are the same as those described in Sect. 2.1. In this case, we assume Alice and Bob pre-share a secret key K_1, where $K_1 \in \{0, 1\}^n$. Besides, the quantum channels here are assumed to be noiseless and lossless.

Step 2* Based on the secret key K_1, Bob decides to perform either SHARE or CHECK on each received qubit. In the SHARE mode, Bob measures the received qubit using the Z basis to obtain the measurement result MR_B and returns a qubit of the same state to Alice. However, in the CHECK mode, Bob reflects the qubit without any disturbance back to Alice. Let assume the returned quantum sequence is Q'.

Step 3* Bob recovers MR_B to the ordered sequence MR'_B based on K_1. After that, he calculate $(M')^i = (MR'_B)^{2i-1} \oplus (MR'_B)^{2i}$ to derive $M' = m'||h(m)'$. That is, if $MR_B = 00$ (11), then $M' = 0 \oplus 0 = 0$ ($1 \oplus 1 = 0$). If $MR_B = 01$ (10), then $M' = 0 \oplus 1 = 1$ ($1 \oplus 0 = 1$). Then, Bob calculates $h(m')$ and compares

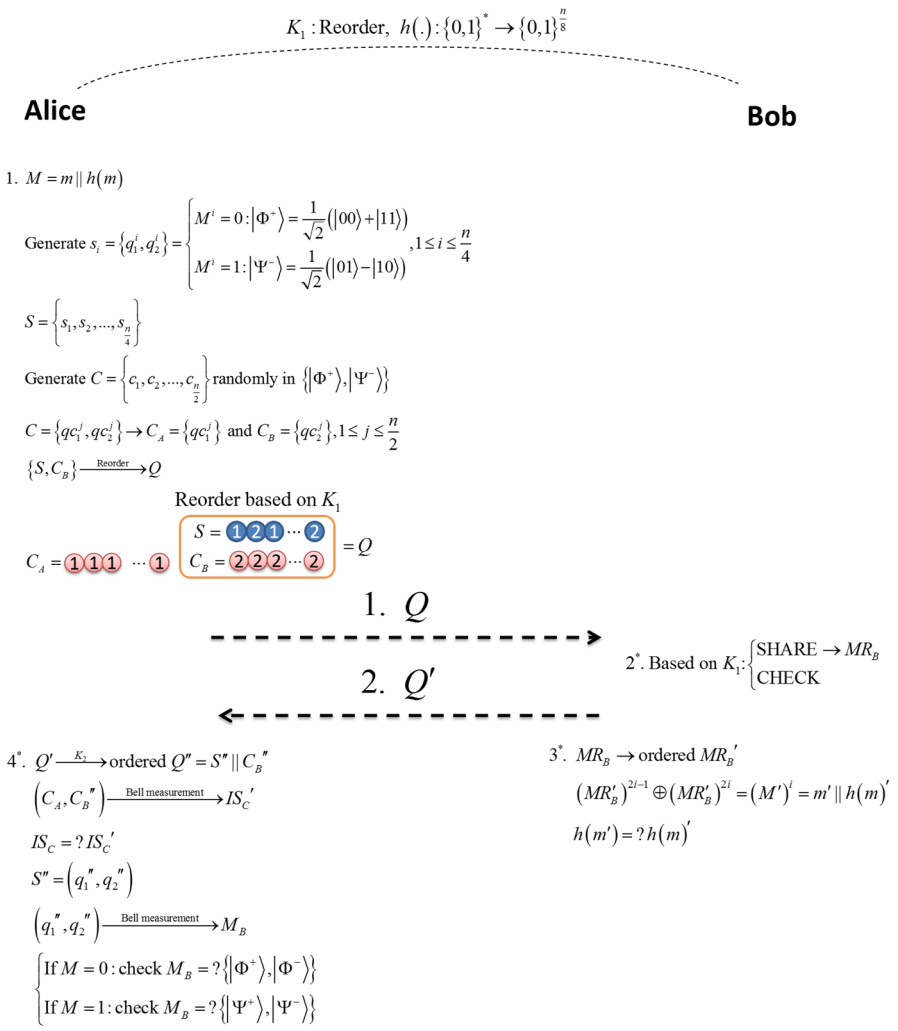

Fig. 2 The proposed measure-resend ASQDC protocol

it with the received $h(m)'$. If $h(m') = h(m)'$, Bob believes that the message m' is indeed sent from Alice without any disturbance. Otherwise, Alice and Bob will terminate the protocol and start it again.

Step 4* Upon receiving Q', Alice can recover Q' based on K_1 to obtain the ordered sequence $Q'' = S''||C_B''$. After that, Alice performs Bell measurement on $\{qc_1^j, (qc_2'')^j\}$ for $j = 1, 2, \ldots, \frac{n}{2}$ to check whether each corresponding set of two qubits is consistent with the states she generated in Step 1. If there is no eavesdropper, Alice performs Bell measurement on $s_i'' = \{(q_1'')^i, (q_2'')^i\}$ for $i = 1, 2, \ldots, \frac{n}{4}$. If the message is 0 (1), i.e., the initial state is $|\Phi^+\rangle$ ($|\Psi^-\rangle$), then the measurement result, M_B, is one of $\{|\Phi^+\rangle, |\Phi^-\rangle\}$ ($\{|\Psi^+\rangle, |\Psi^-\rangle\}$). If

the measurement results are all in the same as their initial states (i.e., $|\Phi^+\rangle$ or $|\Psi^-\rangle$), then it indicates a reflecting attack, and hence, Alice and Bob will terminate the protocol and start it again.

Both ASQDC protocols use the entanglement correlation of the Bell state to detect the presence of eavesdroppers. The only difference between these two protocols (the randomization-based ASQDC and the measure-resend ASQDC) is in the type of operations that Bob is allowed to perform in Step 2 and Step 2*. Besides, in the proposed ASQDC protocols, the pre-shared secret keys are used for user authentication and message authentication. However, the secret keys can be reused if no eavesdropper is detected. Consequently, the communicants do not have to renew the secret keys, which is a tedious work, after completing a protocol execution. Only when a failure occurs in the eavesdropping check or when the secret keys are used for a long period of time does, the new secret keys have to be shared again between Alice and Bob.

Now, it should be noted that both of our proposed protocols can support the features like resistance to noises and resistance to Trojan horse attacks. In order to do that, we need to perform little modifications in our proposed protocols in the following way. Here, we show the modifications of the randomization-based ASQDC protocol. The same modifications can also be applied to the measure-resend one.

2.2.1 Resistance to noises

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. However, in our randomization-based ASQDC protocol, these changes of the transmitted qubits caused by noises will be detected as an eavesdropping in Step 2 through the use of the one-way hash function. Now, in order to combat with the noises in the quantum channel, we combine the linear error correction code (ECC) [7] with the semi-quantum environment. In this case, small errors can be corrected by the introduced error correction code and the majority errors due to malicious users can be detected by the one-way hash function.

Here, we show the detailed protocol as follows. We conceive that a $[\frac{n}{4},s]$ error correction code $\boldsymbol{ECC}$, which uses $\frac{n}{4}$-bit codeword to encode s-bit information using generator matrix $\boldsymbol{G}(x^s)$ and can correct t codeword error bits with the error-correcting function $\boldsymbol{D}(y^{\frac{n}{4}})$ [8–10], is used in the proposed protocol. In this case, a quantum sender, Alice, can send a $\frac{t}{2}$-bit secret message m to a classical receiver, Bob. The modified steps ($\bigstar$) are listed in detail, as follows. The others are the same as those described in Sect. 2.1.

Step 1$\bigstar$ Alice generates $M_A = m||h(m)$ and calculates the codeword of M_A under **ECC**, denoted as M. After that, Alice follows the same way in Step 1 of Sect. 2.1 to generate the Bell states S. Then, Alice generates the checking value IS randomly in the bit of 0 and 1 and calculates the codeword of IS under **ECC**, denoted as IS_C. Subsequently, Alice generates the checking state $C = \{c_1, c_2, \ldots, c_{\frac{n}{2}}\}$ based on IS_C, where $c_j = \{qc_1^j, qc_2^j\}$ for $j = 1, 2, \ldots, \frac{n}{2}$. That is, if the jth bit of IS_C is zero, i.e., $IS_C^i = 0$, Alice

generates c_j in $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Otherwise, $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ is generated. After that, she divides these $\frac{n}{2}$ Bell states into two ordered sequences, $C_A = \{qc_1^j\}$ and $C_B = \{qc_2^j\}$. Alice reorders the quantum sequences S and C_B together according to the secret key K_1 to obtain the new quantum sequence Q. After the above preparation, Alice retains the sequence C_A and sends the sequence Q to Bob.

Step 2★ When Bob receives the qubits in Q, he performs the same procedures as Step 2 to obtain the measurement result MR_B. Then, Bob calculates $MR_B^{2i-1} \oplus MR_B^{2i}$ to derive $(M')^i$. After that, Bob decodes M' and obtains $M'_A = m'||h(m)'$ under **ECC**. Bob calculates $h(m')$ and compares it with the received $h(m)'$. If $h(m') = h(m)'$, Bob believes that the message m' is indeed sent from Alice without any disturbance. Otherwise, Alice and Bob will terminate the protocol and start it again.

Step 3★ This step is the same as Step 3.

Step 4★ Upon receiving C''_B, Alice performs the same procedure as Step 4 to recover C''_B to $C'_B = \{(qc'_2)^j\}$ based on K_2. Then Alice performs Bell measurement on $\{qc_1^j, (qc'_2)^j\}$ for $j = 1, 2, \ldots, \frac{n}{2}$ to obtain IS'_C, i.e., $|\Phi^+\rangle$ represents a bit 0 and $|\Psi^-\rangle$ represents a bit 1. If the measurement result is $|\Phi^-\rangle$ or $|\Psi^+\rangle$, then Alice randomly decides a value 0 or 1 of IS'_C. After that, Alice decodes IS'_C to obtain IS' then checks whether IS' is consistent with the value she generated in Step 1★, IS. If the transmission between Alice and Bob is secure, then it means Alice has successfully transmitted the secret message to Bob.

2.2.2 Resistance to Trojan horse attacks

Trojan horse attacks [11–13] can be divided into the delay-photon Trojan horse attack and the invisible photon Trojan horse attack. In the proposed ASQDC protocols, since there are two transmissions of the same quantum signals, i.e., first from Alice to Bob, and then from Bob to Alice, a malicious party, Eve, therefore is able to obtain the useful information of the secret keys without being detected by performing the Trojan horse attacks. In detail, for the type of the delay-photon Trojan horse attack, Eve intercepts the signal transmitted from Alice to Bob in Step 1 and then inserts the eavesdropping photon in the signal with a delay time, shorter than the time windows. In this way, Bob cannot detect this fake photon since it does not click Bob's detector. After the operation done by Bob, Eve intercepts the signal again and separates the eavesdropping photon. She can get the information about Bob's operation with measurement. On the other hand, for the type of the invisible photon Trojan horse attack, Eve inserts an invisible photon in each signal prepared by Alice and sends it to Bob. As Bob's detector cannot click this photon and then he performs the operation (reorder) on each signal, Eve can steal the information about Bob's operation by means that she intercepts the signal operated and separates the invisible photon from each signal. With the measurement on the invisible photon, Eve can read out Bob's information. Its implement may be resort to the delay-photon attack strategy as it is necessary for Eve to separate the invisible photon from the signal without destroying the original photon.

To prevent the invisible photon Trojan horse attack, Bob only needs to add a wavelength filter [14–17] on each signal to filter out the illegal photons before he deals with it (i.e., measuring or reordering it). For the delay-photon Trojan horse attack, Bob should use a photon number splitter (PNS) (or a photon beam splitter (PBS): 50/50 [18]) to do the multi-photon detection [8]. In this case, the utilization of the PNS (or PBS) will consume the photons. Therefore, in order to prevent this kind of attack, in our randomization-based ASQDC protocol, the length of the secret key K_1 is assumed to be $\frac{3n}{2}$ bits, i.e., $K_1 \in \{0, 1\}^{\frac{3n}{2}}$. Besides, we show the modifications of the randomization-based ASQDC protocol as follows. The modified steps (▲) are listed in detail, as follows. The others are the same as those described in Sect. 2.1.

Step 1▲ Alice follows the Step 1 to generate the quantum sequences S, C_A, and C_B. After that, Alice prepares the Trojan horse detecting photons T randomly in the states of $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Then, she reorders the quantum sequences S, C_B, and T together according to the secret key K_1 to obtain the new quantum sequence Q. After the above preparation, Alice retains the sequence C_A and sends the sequence Q to Bob.

Step 2▲ When Bob receives the qubits in Q, Bob puts the qubit in T to the PNS to detect Trojan horse attacks and put other qubits into the delay line based on K_1. If there are no Trojan horse attacks, then Bob executes the Step 2. Otherwise, Bob will terminate the protocol and start it again.

3 Security analyses

In this section, three well-known attacks, i.e., the impersonation attack, the intercept-and-resend attack, and the modification attack, are analyzed, respectively. It should be noted that only the security of the randomization-based ASQDC protocol is analyzed in detail. As for the security of the measure-resend ASQDC protocol, the same analysis can be performed.

3.1 Security against impersonation attack

An attacker, Eve, may try to impersonate Alice to send a forged message to Bob. Without knowing the pre-shared key K_1, however, Eve will be caught by Bob with a very high probability. In the randomization-based ASQDC protocol, suppose Eve generates a sequence of qubits, Q_E, and sends them to Bob in Step 1. If Eve can pass the eavesdropping check in Step 2, then she is able to successfully impersonate Alice to send a forged message to Bob. However, without knowing the pre-shared key K_1, Eve cannot perform the correct reorder operation on Q_E and eventually the comparison in Step 2 will be failed. Since one-bit error in the input (i.e., a transmitted message) will cause significant changes in the output (i.e., a hashed value), the probability for Eve to be detected in the randomization-based ASQDC protocol is close to 1.

On the other hand, Eve may try to impersonate Bob to communicate with Alice. In the randomization-based ASQDC protocol, Eve may intercept the sequence Q sent from Alice to Bob in Step 1. Since Eve does not know the secret key K_1 and K_2, she

does not know how to choose the reflecting qubits in Q and does not know how to perform the reorder operation on the chosen qubits, respectively. In this case, she will randomly choose some qubits in Q and randomly reorders the chosen qubits and sends them to Alice in Step 3. If, however, Eve reflects the wrong qubits with the wrong order back to Alice, then Eve can successfully pass the verification process of Alice with a probability of $\frac{1}{4}$ for each qubit. For example, if the initial state is $|\Phi^+\rangle$ ($|\Psi^-\rangle$), then Alice performs the Bell measurement on the wrong qubit to obtain the measurement result $|\Phi^+\rangle$ ($|\Psi^-\rangle$) with a probability of $\frac{1}{4}$ because she will randomly obtain one of the four measurement results from $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$. As a result, Eve has a probability of $\frac{5}{8}$ ($= \frac{1}{2} + \frac{1}{2} \times \frac{1}{4}$) to pass the verification for each qubit. Hence, the probability for Eve to be detected in the randomization-based ASQDC protocol is $1 - (\frac{5}{8})^{\frac{n}{2}}$. The detection probability would converge to 1 when n is large enough.

3.2 Security against intercept-and-resend attack

Eve may launch the intercept-and-resend attack in hope that she can get the useful information about the secret message M without being detected. In this attack, Eve intercepts the sequence Q in Step 1 and measures it with Z basis ($\{|0\rangle, |1\rangle\}$). After that, she generates the same states based on her measurement results and sends them to Bob. However, each secret message in M is encoded into a Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (if $M^i = 0$) or $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ (if $M^i = 1$) and then reordered with the checking states C_B based on K_1. Without knowing the secret key K_1, Eve cannot identify which qubit belongs to S and which qubit belongs to C_B. Therefore, Eve cannot recover the measurement results to the correct order and hence cannot calculate the secret message of Alice.

Besides, any arbitrary measurement on C_B would destroy the entanglement of a Bell state and eventually will be detected by Alice in Step 4 with a probability of $\frac{1}{2}$ for each Bell state in C_B. For example, if the initial state of the Bell state is $|\Phi^+\rangle$, after Eve performs the intercept-and-resend attack, the state of the Bell state will collapse to $|00\rangle/|11\rangle$ (since $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$). In Step 4, Alice will perform the Bell measurement on $|00\rangle/|11\rangle$ and she will obtain the measurement result $|\Phi^+\rangle$ with a probability of $\frac{1}{2}$, since $|00\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle)$ and $|11\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Phi^-\rangle)$. As a result, Eve has a probability of $\frac{1}{2}$ to pass the verification for each Bell state. The probability for Eve to be detected in the randomization-based ASQDC protocol is $1 - (\frac{1}{2})^{\frac{n}{2}}$. The detection probability would converge to 1 when n is large enough.

3.3 Security against modification attack

In the modification attack, Eve may try to modify one-bit message of the transmitted qubits, Q, by using the unitary operation $i\sigma_y$ and make the receiver to obtain a wrong message without being detected. The following two cases show that Eve will be detected by using the checksum $h(m')$ of the hash function or the entanglement correlation of a Bell state as the integrity verification mechanism.

1. If Eve performs the unitary operation $i\sigma_y$ on a qubit belong to the sequence S and then sends it to Bob. However, arbitrary modification will lead to the wrong measurement result, and Bob can detect the modification with 100 % probability in Step 2. This is similar to the security analysis proposed in [19–21]: if the 1-bit message is modified, then the computed checksum $h(m')$ cannot be equal to the measured checksum, $h(m)'$, according to the feature of a collision-free hash function.
2. If Eve performs the unitary operation $i\sigma_y$ on a qubit belong to the sequence C_B and then sends it to Bob. Then the Bell state $|\Phi^+\rangle$ ($|\Psi^-\rangle$) will be changed to $|\Psi^-\rangle$ ($|\Phi^+\rangle$). An arbitrary modification to a qubit, however, could lead to the wrong measurement result and eventually would be detected by Alice. Hence, Eve cannot pass the verification process of Alice because the measurement result cannot be equal to the initial state.

Therefore, the proposed ASQDC protocol is secure against the modification attack to a single-qubit level because Eve cannot modify the sequence Q without being detected.

4 Conclusions

In this paper, we have proposed two authenticated semi-quantum direct communication (ASQDC) protocols without using classical channels. The first proposed protocol is the randomization-based ASQDC protocol, and the other protocol is based on the measure-resend ASQDC protocol. In both proposed ASQDC protocols, a sender with advanced quantum devices can transmit a secret message to a classical receiver, who can only perform classical operations, without information leakage through the pre-shared secret keys. Analyses show that the proposed protocols are resistant to the impersonation attack, the intercept-and-resend attack, the modification attack, and Trojan horse attacks. Nevertheless, with the introduction of a linear error correction code, both the ASQDC protocols can also be useful in a random noise environment.

Acknowledgments We would like to thank the Ministry of Science and Technology of Republic of China for financial support of this research under Contract No. MOST 104-2221-E-006-102-.

References

1. 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)
2. Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical Bob. Phys. Rev. Lett. **99**, 140501 (2007)
3. Boyer, M., Gelles, R., Kenigsberg, D., Mor, T.: Semiquantum key distribution. Phys. Rev. A **79**(3), 032341 (2009)
4. Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block. Phys. Rev. A **68**, 042317 (2003)
5. FIPS180-1: Secure hash standard. NIST, US Department of Commerce, Washington (1995)
6. Preneel, B., Dobbertin, H., Bosselaers, A.: The cryptographic hash function RIPEMD-160. Crypto Bytes **3**(2), 9–14 (1997)
7. MacWilliams, F.J., Sloane, N.J.A.: The theory of error correcting codes. Elsevier, Amsterdam (1977)
8. Li, Y.-B., Qin, S.-J., Yuan, Z., Huang, W., Sun, Y.: Quantum private comparison against decoherence noise. Quantum Inf. Process. **12**(6), 2191–2205 (2013)

9. Li, Y.-B., Wang, T.-Y., Chen, H.-Y., Li, M.-D., Yang, Y.-T.: Fault-tolerate quantum private comparison based on GHZ states and ECC. Int. J. Theor. Phys. **52**(8), 2818–2825 (2013)
10. Li, Y.-B., Wen, Q.-Y., Qin, S.-J., Guo, F.-Z., Sun, Y.: Practical quantum all-or-nothing oblivious transfer protocol. Quantum Inf. Process. **13**(1), 131–139 (2014)
11. Cai, Q.Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A **351**, 23–25 (2006)
12. Gisin, N., Fasel, S., Kraus, B., Zbinden, H., Ribordy, G.: Trojan-horse attacks on quantum-key-distribution systems. Phys. Rev. A **73**(2), 022320 (2006)
13. 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)
14. 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 (2005). arXiv:quant-ph/0508168v1
15. 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)
16. 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)
17. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Erratum: Improving the security of multiparty quantum secret sharing against Trojan horse attack [Phys. Rev. A 72, 044302 (2005)]. Phys. Rev. A **73**(4), 049901 (2006)
18. Yang, Y.-G., Sun, S.-J., Zhao, Q.-Q.: Trojan-horse attacks on quantum key distribution with classical Bob. Quantum Inf. Process. **14**(2), 681–686 (2015)
19. Yang, C.-W., Hwang, T.: Improved QSDC protocol over a collective-dephasing noise channel. Int. J. Theor. Phys. **51**(12), 3941–3950 (2012)
20. 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)
21. Hwang, T., Luo, Y.-P., Yang, C.-W., Lin, T.-H.: Quantum authencryption: one-step authenticated quantum secure direct communications for off-line communicants. Quantum Inf. Process. **13**(4), 925–933 (2014)