Cryptanalysis and improvement of a quantum communication-based online shopping mechanism

Wei Huang · Ying-Hui Yang · Heng-Yue Jia

Received: 19 October 2014 / Accepted: 23 February 2015 / Published online: 5 March 2015
© Springer Science+Business Media New York 2015

Abstract Recently, Chou et al. (Electron Commer Res 14:349–367, 2014) presented a novel controlled quantum secure direct communication protocol which can be used for online shopping. The authors claimed that their protocol was immune to the attacks from both external eavesdropper and internal betrayer. However, we find that this protocol is vulnerable to the attack from internal betrayer. In this paper, we analyze the security of this protocol to show that the controller in this protocol is able to eavesdrop the secret information of the sender (i.e., the customer’s shopping information), which indicates that it cannot be used for secure online shopping as the authors expected. Accordingly, an improvement of this protocol, which could resist the controller’s attack, is proposed. In addition, we present another protocol which is more appropriate for online shopping. Finally, a discussion about the difference in detail of the quantum secure direct communication process between regular quantum communications and online shopping is given.

Keywords Quantum cryptography · Quantum secure direct communication · Cryptanalysis · E-commerce · Online shopping
1 Introduction

With the rapid development of the internet and related technologies, E-commerce, which is one of the most significant scientific accomplishments brought by internet, is playing an increasingly important role in modern life. As a key component of E-commerce, online shopping has become one of the most important shopping ways in people’s everyday life. In 2013, the average daily transaction volume of online shopping in the world reaches billions of dollars. Therefore, security and privacy have naturally become an essential requirement for online shopping.

So far, the security and privacy of E-commerce has been guaranteed by the classical cryptosystems whose security is based on the assumptions of computation complexity. Nevertheless, with the development of quantum algorithms and quantum computer [1–3], these classical cryptosystems are facing more and more challenges. To address the potential threat posed by quantum computation to classical cryptosystems, people begin to research new cryptographic technology, such as quantum cryptography. Quantum cryptography, whose security is relied on the quantum mechanics principles rather than the assumptions of computation complexity, has become a hotspot of cryptography. Since the pioneering work of Bennett and Brassard in 1984 [4], much attention has been focused on quantum cryptography, which includes quantum key distribution (QKD) [4–9], quantum secret sharing (QSS) [10–14], quantum secret direct communication (QSDC) [15–22], quantum watermark (QW) [23–25] and quantum secure multiparty computation (QSMC) [26–35], etc.

Quantum cryptography has also been utilized to assure the security and privacy in E-commerce. In 2010, Wen presented an E-payment protocol by utilizing quantum group signature, in which a trusted third party is required [36]. To enhance the robustness of the system, Wen and Nie [37] presented another E-payment protocol by employing quantum blind and group signature, where two trusted third parties are needed. Nevertheless, both the two protocols can only be applied to the cases where business transactions happen within the same bank. In real life, many business transactions occur between different banks. In addition, an E-payment system, which supports secure inter-bank transactions, should be desired from the view of practical application. In order to settle this problem and support unconditionally secure E-payment between two different banks, Wen et al. [38] presented an inter-bank E-payment protocol based on quantum proxy blind signature in 2013. Unfortunately, Cai and Wei [39] found that this protocol is susceptible to denial-of-service attack. Moreover, they also show that the dishonest merchant can succeed to change the purchase information of the customer in this protocol.

It is known that design and cryptanalysis have always been important branches of cryptography. Both of them drive the development of this field. In fact, cryptanalysis is an important and interesting work in quantum cryptography [40,41]. It estimates the security level of a protocol, finds potential loopholes, and tries to address security issues. As pointed out by Lo and Ko [42], breaking cryptographic systems was as important as building them. To date, many kinds of attacks strategies have been presented, such as entanglement swapping attack [43], intercept-resend attack [44], correlation-extractability attack [45,46], Trojan horse attack [47], and participant attack [48–50].
Recently, Chou et al. [51] presented a novel controlled QSDC protocol which can be used for online shopping. By utilizing this protocol, the online shopping mall could control the shopping process, hence shopping information of the customer could be more secure. For the sake of simplicity, we call it CLZ protocol hereafter. The authors of Ref. [51] made a simple security analysis of the CLZ protocol to show its immunity to the attacks from both external eavesdropper and internal betrayer. Unfortunately, we find that this protocol is susceptible to the attack from the internal betrayer. In this paper, we make an analysis to illustrate that this protocol cannot provide unconditional security for online shopping, since the controller of this protocol is able eavesdrop the secret information of the sender (i.e., the customer’s shopping information). After that, we first propose an improvement of the CLZ protocol to close this security loophole with classical XOR operation. Then, we also propose another protocol which is more suitable for online shopping, inspired by the ideas of Refs. [8,28]. Finally, we make a discussion about the difference in detail of the QSDC process between regular quantum communications and online shopping.

This paper is organized as follows. In next section, we make a brief introduction of the CLZ protocol. Section 3 first gives an analysis of the CLZ protocol to show its vulnerability to the internal attack from a dishonest controller. Then, the corresponding improvement is presented. In Sect. 4, we propose a new protocol which is more suitable for online shopping. Finally, a discussion about the factor that should be considered when QSDC is applied to online shopping, as well as a short conclusion is given in Sect. 5.

2 Brief review of the CLZ protocol and its application

Herein, we make a brief description of the CLZ protocol [51]. Then, we introduce how this protocol can be applied to online shopping.

2.1 The CLZ protocol

Different from the BB84 [4] protocol in which only one photon is transmitted at a time, the photons in CLZ protocol are transmitted by utilizing the technique of block transmission which has been proposed firstly by Long et al. [15]. In this protocol, Alice, Bob, and Charlie are supposed to be the information sender, receiver, and controller, respectively. If Alice wants to transmit a secret message of $N$ bits directly to Bob under the control of Charlie, they could execute this protocol as the following steps.

1. **Controller prepares for the quantum information carriers** Charlie prepares a sequence of $N+δ$ single qubits, each of which is randomly in one of following four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle \}$, where $|0\rangle$ and $|1\rangle$ are, respectively, the eigenstates corresponding to the eigenvalue 0 and 1 of $\sigma_z$,

$$
|+\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle), \quad |\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle),
$$

and the sequence is denoted as $S_0$. After that, he sends $S_0$ to Alice.
(2) **Eavesdropping check for the first transmission** After the reception of $S_0$, Alice begins to check eavesdropping with Charlie as follows. Alice randomly selects $\delta$ single qubits from $S_0$ and randomly chooses a measuring basis $Z$-basis or $X$-basis, measuring the selected qubits for checking eavesdropping, where $Z$-basis=$\{|0\rangle, |1\rangle\}$ and $X$-basis=$\{|+\rangle, |−\rangle\}$. Afterward, Alice informs Charlie of the information including which bases she uses, the positions of selected qubits, and the corresponding measurement outcomes. With the information from Alice, Charlie could determine whether there exists eavesdropping in the first transmission. If there exists eavesdropping, they abort the protocol; otherwise, Alice throws away the qubits used for checking eavesdropping and continue to the next step.

(3) **Sender encodes the secret information** Alice encodes her secret message $M$ on the remaining $N$ qubits as follows. If the $i$-th bit of $M$ is 0/1, Alice performs operation $I$/$i\sigma_y$ on the $i$-th one of the remaining qubits, where
\[ I = |0\rangle\langle 0| + |1\rangle\langle 1|, \quad i\sigma_y = |0\rangle\langle 1| − |1\rangle\langle 0|. \]

After that, she generates $\delta$ decoy qubits which are randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |−\rangle\}$ and inserts them randomly into the sequence $S_0$. Then, Alice send the new sequence (denoted as $S_1$) to Bob.

(4) **Eavesdropping checking for the second transmission** After Bob receives $S_1$ from Alice, Alice informs Bob of the positions of the decoy qubits, Bob measures each of the decoy qubits randomly in $Z$-basis or $X$-basis. After that, Bob tells Alice which bases he uses and the corresponding measurement outcomes. According to the information announced by Bob, Alice could determine whether there exists eavesdropping during the transmission of $S_1$. If there exists eavesdropping, they stop the protocol; otherwise, Bob could get the secret message with the help of Charlie as follows.

(5) **Receiver deduces the secret message with the controller’s help** Bob discards the $\delta$ qubits used for checking eavesdropping and now only remains $N$ single qubits. Without Charlie’s permission, Bob is unable to obtain Alices secret message. Only after Charlie publishes the initial states of the $N$ single qubits, can Bob recover Alice’s secret message $M$ by comparing with the initial states. Concretely, if the initial state of a qubit is $|0\rangle$ or $|1\rangle$ ($|+\rangle$ or $|−\rangle$), Bob measure it in $Z$-basis ($X$-basis). And the corresponding bit of $M$ is 0 (1) provided the measurement outcome is the same as (different with) the initial state.

This protocol could also be extended to a multiparty controllers version. Take the two controllers version as an example. Suppose the two controllers, Charlie and Dave, both have the ability to control Alice and Bob’s communication. Some modifications are required in steps (1) and (5). In step (1), after Charlie prepares the qubit sequence, he sends it to Dave instead of Alice. Once Dave receives these photons, he make an eavesdropping check as Alice does in step (2). To change the states of qubits, Dave performs randomly operation $I$ or $i\sigma_y$ on each of the remaining qubits, then he sends these qubits to Alice like the original step (1) does. In the new step (5), Bob need ask Charlie to reveal the initial states he prepared and Dave to publish the operations he had performed. After Bob gets all the information, he is able to deduce $M$. 
2.2 The application of the CLZ protocol on online shopping

Herein, we introduce how the CLZ protocol can complete the online shopping process [51]. In this example, eBay is considered as the online shopping mall, and the detail steps can be described as follows.

(a) Both merchant and consumer register as eBay members.
(b) eBay authenticates the identities of merchant and consumer.
(c) Once the consumer decides to buy items from the merchant, he/she asks eBay to transmit a sequence of single qubits randomly in \{|0\rangle, |1\rangle, |+\rangle, |−\rangle\} via quantum channel, but without knowing its initial states.
(d) After checking the security of the transmitted qubits, customer encodes his/her shopping information on those photons by performing the corresponding unitary operations as described in steps (2) and (3). The shopping information includes customer ID, item number, etc. Once the encoding is finished, those encoded photons will be sent to the merchant.
(e) Again, the security checking on these transmitted qubits is needed. If the transmission is secure, merchant will ask eBay for the initial states of these photons. With the encoded qubits and their initial states, merchant could deduce the shopping information of the customer.

3 Security analysis and improvement of the CLZ protocol

In this section, we analyze the security of the CLZ protocol to show that it is susceptible to the attack from a dishonest controller. Specifically, we first explain how a dishonest controller could eavesdrop the secret information of the sender in the CLZ protocol. That is to say, a dishonest online shopping mall can eavesdrop the customer’s shopping information when the CLZ protocol is applied to online shopping. Then, we present an improvement which could close the corresponding security loophole of the CLZ protocol by employing classical XOR operation.

3.1 Security analysis

In Ref. [51], the authors make a simple analysis to show that the CLZ protocol is secure against the attacks from both external eavesdropper and internal betrayer. However, the Trojan horse attack and invisible photon attack [52,53], which are usually utilized to attack two-way quantum communication, have been neglected by the authors. Obviously, if the attackers utilize these attacks, he/she can obtain the secret message $M$ without being noticed. Fortunately, these two attacks can be easily prevented by employing the strategies in Refs. [52,53]. In the rest of our analysis, we assume that Alice employs the strategies in Refs. [52,53] to resist these two kinds of attacks. Now, we show that the controller Charlie can still get $M$ under this assumption.

In each transmission of the quantum information carriers in the CLZ protocol, there are $\delta$ decoy qubits, which are randomly in the four states \{\ket{0}, \ket{1}, \ket{+}, \ket{-}\} and randomly inserted in the qubit sequence. After receiving the qubit sequence, the
receiver measures each of the decoy qubits randomly in $Z$-basis or $X$-basis. Whatever kind of attack an external eavesdropper utilizes, his/her eavesdropping action will introduce errors into the eavesdropping check with a certain probability. The reason is that the process for eavesdropping check done in this protocol, in essence, is the same as that in the BB84 QKD protocol [4], which has been proved unconditional secure. Hence, the CLZ is indeed secure against the external attacks.

However, an internal betrayer of a multiparty quantum cryptographic protocol may have more power to attack the protocol than an external eavesdropper. First, he/she can know partial information legally. Second, he/she can tell a lie in the process of eavesdropping check to avoid introducing errors. Therefore, the attacks from dishonest participants are generally more powerful and should be paid more attention to [48–50]. The authors of the CLZ protocols said that this protocol could resist the attacks from both the information receiver and the controller. That is, the receiver Bob could not get the secret message $M$ without the help of the controller Charlie. Also, Charlie is unable to get $M$ without leaving a trace in the eavesdropping check.

We admit that, no matter what kind of attack Charlie employs in the CLZ protocol, once he could get any useful information of $M$, her action will introduce errors into the eavesdropping check and hence make the protocol aborted. In fact, this condition is sufficient to ensure the security of a QKD protocol, but it is not enough to guarantee the security of the CLZ protocol since it is a QSDC protocol. Different from QKD, the purpose of which is to establish a random key, the purpose of QSDC is to directly transmit a secret message [15–22]. In a QKD protocol, if the eavesdropper’s action is detected in the eavesdropping check, the transmitted information carriers can be abandoned as they do not carry any information about the secret message. On the contrary, in a QSDC protocol, the secret message is directly encoded on the transmitted information carriers. Hence, QSDC has higher security requirements than QKD. On the one hand, the eavesdropping check in a secure QSDC protocol should detect the eavesdropper’s attack. On the other hand, a secure QSDC protocol should leak none useful information of the secret message to the eavesdropper. In other words, once the eavesdropper has already got any useful information of the secret message, the QSDC protocol is insecure even if the eavesdropper’s attack has been detected in the eavesdropping check.

Unfortunately, the CLZ protocol could not simultaneously satisfy both the two security requirements. In this protocol, if Charlie wants to eavesdrop the secret message $M$, he could execute the following strategy. In step (3), when Alice sends out the sequence $S_1$, Charlie intercepts the traveling sequence $S_1$ and stores it. Instead, he prepares another sequence $S'_1$ of $N+\delta$ qubits to replace $S_1$ and sends it Bob. After Bob receives the sequence $S'_1$, Alice will announce the positions of the $\delta$ decoy qubits. Once Charlie gets this information, he discards the corresponding decoy qubits in $S_1$. Then, he could easily deduce $M$ with the remaining $N$ qubits and the information of their initial states. It should be pointed out this attacking strategy will inevitably introduce errors into the eavesdropping check. Thus, the protocol will be aborted by Alice and Bob according to step (4). Even so, Alice and Bob could only determine that there exists eavesdropping in the transmission. That is to say, they will not suspect Charlie as the eavesdropper. So far, we have shown that the controller Charlie in the CLZ protocol could easily get the whole secret message $M$ beyond suspicion.
Accordingly, the application of the CLZ protocol given above, i.e., online shopping, also has the same security loophole. Specifically, the online shopping mall (i.e., eBay) could utilize this strategy to get the customer’s shopping information in the process of online shopping.

3.2 The improvement of the CLZ protocol

Herein, we give an improvement of the CLZ protocol in order to close the security loophole introduced above. To close the corresponding loophole, we only need to, respectively, substitute the steps (3)–(5) of the CLZ protocol with the steps (3′)–(5′) given below.

(3′) *Sender encodes the secret information* Before encoding her secret information, Alice first generates an $N$-bit random string $K$. Then, she encodes $K \oplus M$ on the remaining $N$ qubits as follows (here $\oplus$ represents XOR operation). If the $i$-th bit of $K \oplus M$ is 0/1, Alice performs operation $I/i\sigma_z$ on the $i$-th one of the remaining qubits. After that, she generates $\delta$ decoy qubits which are randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |−\rangle\}$ and inserts them randomly into the encoded $N$ qubits. Finally, Alice sends the new sequence (denoted as $S_1$) to Bob.

(4′) *Eavesdropping checking for the second transmission* After Bob receives $S_1$ from Alice, Alice informs Bob of the positions of the decoy qubits in $S_1$, Bob measures each of the decoy qubits randomly in $Z$-basis or $X$-basis. After that, Bob tells Alice which bases he uses and the corresponding measurement outcomes. According to the information announced by Bob, Alice could determine whether there exists eavesdropping during the transmission of $S_1$. If there exists eavesdropping, they stop the protocol; otherwise, Alice publishes the binary string $K$. Then, Bob could get $M$ with the help of Charlie in the next step.

(5′) *Receiver deduces the secret message with the controller’s help* Bob discards the $\delta$ qubits used for checking eavesdropping and now only remains $N$ qubits. Without Charlie’s permission, Bob is unable to obtain $M$. Only after Charlie publishes the initial states of the $N$ qubits, can Bob recover the binary string $K \oplus M$ by comparing with the initial states. Concretely, if the initial state of a qubit is $|0\rangle$ or $|1\rangle$ ($|+\rangle$ or $|−\rangle$), Bob measures it in $Z$-basis ($X$-basis). And the corresponding bit of $K \oplus M$ is 0 (1) provided the measurement outcome is the same as (opposite to) the initial state. Once obtaining $K \oplus M$, Bob could deduce $M$ with the string $K$ announced by Alice.

By employing this improved version, Alice could securely send secret message to Bob under the control of Charlie. Besides, Alice should make use of the strategies in Refs. [52,53] to prevent the Trojan horse attack and invisible photon attack.

Now we explain why this improvement can close the security loophole given in Sect. 3.1. As analyzed in Sect. 3.1, the process for eavesdropping check done in this improved version, in essence, is the same as that in the BB84 QKD protocol [4]. Therefore, no matter what kind of attack the eavesdropper (both the external eavesdropper and internal betrayer) utilizes, once he/she has obtained any useful information about $K \oplus M$, his/her attacking action will unavoidably leave a trace in (i.e., introduce errors into) the check. Then, the protocol will be stopped before Alice publishes the
binary string \( K \). Since \( K \) is a random binary string known only by Alice, even if the eavesdropper gets some useful information about \( K \oplus M \), he/she knows nothing about \( M \) since \( K \) will not be published anymore. Till now, we have shown that the improved version is secure against all the present attack, since whatever kind of attack the eavesdropper uses, he/she could get none useful information about \( M \) but be noticed in the eavesdropping check. Accordingly, by utilizing the improved version, the corresponding process of online shopping could also be immune to all the present attack.

4 The new protocol which could be used for online shopping

To close the security loophole introduced in Sect. 3.1, Sect. 3.2 has given an improvement of the CLZ with minor modifications. Herein, we present a new protocol which could also be used in the online shopping process described in Sect. 2.2. In this protocol, all the qubits are prepared by the controller Charlie, and the sender Alice utilizes a tilt-adjustable phase plate to process the traveling qubits. The specific steps of this protocol can be described as follows.

(1) Charlie prepares a sequence of \( N+2\delta \) single qubits, each of which is randomly in one of the four states \( \{|+\rangle, |-\rangle, |r\rangle, |l\rangle\} \), where

\[
|r\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \quad |l\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle), \quad (3)
\]

and the sequence is denoted as \( S_0 \). Afterward, he sends \( S_0 \) to Alice.

(2) Upon receiving \( S_0 \), Alice starts to check eavesdropping with Charlie. Specifically, Alice randomly chooses \( \delta \) qubits from \( S_0 \) for checking eavesdropping. For each of the chosen qubits, Alice measures it by choosing randomly one of the two bases, \( X \)-basis and \( Y \)-basis, where \( Y \)-basis = \( \{|r\rangle, |l\rangle\} \). After that, Alice informs Charlie of the information including which bases she uses, the positions of the chosen qubits and the corresponding measurement outcomes. Based on the information from Alice, Charlie could judge whether there exists eavesdropping in the transmission of \( S_0 \). If there exists eavesdropping, Charlie informs the other two participants to abort the protocol; otherwise, Alice discards the qubits used for checking eavesdropping and continue to the next step.

(3) Before encoding her secret message \( M \), Alice randomly chooses \( \delta \) single qubits of the remaining \( N+\delta \) ones as decoy qubits. For each of the decoy qubits, Alice makes use of a tilt-adjustable phase plate to apply a phase shift, which is randomly chosen in \( \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\} \), on it. It is easy to verify that applying a phase shift of \( 0, \frac{\pi}{2}, \pi \) and \( \frac{3\pi}{2} \) can be identical to performing the operation \( I, S, Z, \) and \( ZS \), respectively, where

\[
I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (4)
\]
Afterward, Alice encodes $K \oplus M$ on the remaining $N$ qubits as follows, where $K$ is an $N$-bit random string generated by herself. If the $i$-th bit of $K \oplus M$ is 0/1, Alice applies a phase shift of $0/\pi$ (i.e., performs operation $I/Z$) on the $i$-th one of the remaining $N$ qubits. Once finishing processing all the $N+\delta$ qubits, Alice sends the new sequence (denoted as $S_1$) to Bob.

After confirming that Bob has received $S_1$, Alice announces the positions of the decoy qubits in $S_1$. Then, Bob requires Charlie to publishes the initial state of each of the decoy qubits. After Charlie finishes publishing the corresponding information, Alice tells Bob which phase shift she has applied on each of the decoy qubits. For each of the decoy qubits, according to the information provided by Alice and Charlie, Bob deduces its expected state and measures it in the corresponding basis. For example, if the initial state of a decoy qubit is $|+\rangle$, the expected state of it should be $|+\rangle/|r\rangle/|−\rangle/|l\rangle$, provided the phase shift Alice applied on it is $0/\pi/3\pi/\pi$. And if the expected state of a decoy qubit is $|+\rangle$ or $|−\rangle$ ($|r\rangle$ or $|l\rangle$), Bob will measure it with $X$-basis ($Y$-basis). If there exists no eavesdropping in the transmission of $S_1$, the measurement outcome of each decoy qubit should be identical to its expected state. With the measurement outcomes of all the decoy qubits, Bob could judge whether there exists eavesdropping during the transmission of $S_1$ in this way. If there exists eavesdropping, Bob informs the other two participants to stop the protocol; otherwise, Alice publishes the binary string $K$, then Bob could extract $M$ with the help of Charlie as follows.

Bob throws away the $\delta$ qubits used for checking eavesdropping and now only retains $N$ qubits. Without Charlie’s help, Bob is unable to get $M$. Only after Charlie publishes the initial states of the $N$ qubits, can Bob extract the binary string $K \oplus M$ by comparing the measurement outcomes with the corresponding initial states. Concretely, if the initial state of a qubit is $|+\rangle$ or $|−\rangle$ ($|r\rangle$ or $|l\rangle$), Bob measure it in $X$-basis ($Y$-basis). And the corresponding bit of $K \oplus M$ is 0 (1) provided the measurement outcome is the same as (opposite to) the initial state. Once obtaining $K \oplus M$, Bob could deduce $M$ with the string $K$ announced by Alice.

Compared with the CLZ protocol and the improved version, the sender Alice in this protocol no longer needs to be capable of preparing qubits. That is to say, this protocol reduces the quantum hardware requirement for Alice. Similar to the CLZ protocol and the improved version, Alice should also take the measures in Refs. [52,53] to prevent the Trojan horse attack and invisible photon attack.

Now, we make a security analysis of this protocol to show that it can resist the attacks from both external eavesdropper and internal betrayer. The attacks from internal betrayer can be divided into two cases. On one hand, the controller Charlie may want to obtain the secret information $M$. On the other hand, the receiver Bob may want to get $M$ without the help of Charlie. Obviously in this protocol, the attacks from internal betrayer are much more threatening than those from external eavesdroppers. Firstly, all the qubits utilized in this protocol are prepared by Charlie, which indicates that he could replace the legal qubits with any kind of states he likes. Secondly, in the second eavesdropping check, Charlie could tell lies when he is required to announce the initial states of the decoy qubits. Thirdly, Bob could tell a lie for the result of
the second eavesdropping check. In consequence, if this protocol is secure against
the attacks from internal betrayer, it is also immune to the attacks from any external
eavesdropper. Now, we focus on showing that this version could resist the attacks from
Charlie and Bob, respectively.

In this protocol, the sender Alice’s secret message $M$ is first encrypted with the
binary string $K$. Then, Alice encodes the string $K \oplus M$ into the corresponding qubits.
Only when Alice and Bob have confirmed that there exists no eavesdropping in the
second transmission can Bob extract $K \oplus M$ with Charlies’s help and the string $K$
which is announced by Alice thereafter. In other words, if Charlie wants to get $M$, he
has to obtain $K \oplus M$ with out introduce errors into the second eavesdropping check.
However, it is an impossible task for him.

In fact, the decoy qubits in $S_1$ is randomly chosen by Alice from the $N + \delta$ qubits.
Alice will announce the positions of these decoy qubits only after Bob receives $S_1$.
That is to say, Charlie is unable to know which qubits in $S_1$ are decoy particles before
Bob receives $S_1$. When he knows the positions of the decoy qubits, he has had no
access to the qubits in $S_1$ since they have already been possessed by Bob. Under
this situation, Charlie has to treat each of the qubits in $S_1$ equally. Actually in this
protocol, for each of the decoy qubits in $S_1$, Alice randomly chooses one operation
from $\{I, S, Z, ZS\}$ to perform on it. If Charlie dose not want to disturb the state of this
decoy qubit, he should find out that which one of the four operations that Alice has
performed on the decoy qubit with only one opportunity. That is, if he wants to get any
useful information of $K \oplus M$ without introduce errors into the second eavesdropping
check, he must be able to unambiguously discriminate the four operations that Alice
performs on the decoy qubits. Before illustrating that Charlie is unable to fulfill this
task, we first introduce a theorem on quantum operation discrimination.

**Theorem 1** [54] Under the condition that the device can be accessed only once, the
minimum error probability to discriminate the two operations $U_1$ and $U_2$ is

$$P_E = \frac{1}{2} \left[ 1 - \sqrt{1 - 4p_1p_2r(U_1^\dagger U_2)^2} \right],$$  \hspace{1cm} (5)

where $r(U_1^\dagger U_2)$ stands for the distance between the origin of the complex plane and
the polygon whose vertices are the eigenvalues of the unitary operator $U_1^\dagger U_2$. Here,
$U^\dagger$ represents the adjoint matrix of $U$, and if the operations $U_1$ and $U_2$ are operations
on single qubits, $r(U_1^\dagger U_2)$ represents the distance between the origin of the complex
plane and the line segment whose vertices are the eigenvalues of the unitary operator $U_1^\dagger U_2$.

Taking the operations $I$ and $S$ as an example, we can calculate that the eigenvalues
of the operation $I^\dagger S$ is 1 and $i$. According to Theorem 1, $r(Z^\dagger S) = \frac{1}{\sqrt{2}}$, and the
minimum error probability to discriminate $I$ and $S$ is

$$p = \frac{1}{2} \left[ 1 - \sqrt{1 - \left( \frac{1}{\sqrt{2}} \right)^2} \right] \approx 0.15.$$  \hspace{1cm} (6)
Analogously, we can find that the minimum error probability to discriminate the operations $S$ and $Z$ ($I$ and $ZS$, $Z$ and $ZS$) is also $p$. That is to say, the operations $I$, $S$, $Z$ and $ZS$ cannot be unambiguously discriminated with only one opportunity. Hence, no matter what kind of attacking strategy Charlie utilizes, once he could acquire any useful information about $K \oplus M$, he will unavoidably introduce errors into the second eavesdropping check and make the protocol stopped. In this circumstance, Alice will not publish $K$, hence Charlie could get no useful information of $M$.

Next, we illustrate that Bob is unable to get $M$ without the help of Charlie. Apparently, if Bob could replace (or acquire the states of) the qubits sent from Charlie to Alice without being detected by the first eavesdropping check, he can then succeed in getting $M$ without the help of Charlie. Nevertheless, as analyzed in Sect. 3.1, the transmission of $S_0$ is secure against any attack from Bob since the process for the first eavesdropping check in step (2), in essence, is the same as that in the BB84 QKD protocol [4], which has been proved unconditional secure. That is to say, whatever kind of attack Bob employs, once he obtains any useful information of the qubits received by Alice, his eavesdropping action will introduces errors into the first eavesdropping check with a certain probability and hence make the protocol aborted. Therefore, this protocol is secure against the the attacks from Bob.

Thus far, we have showed that the proposed protocol can resist the attacks from internal betrayer, which also indicates that it is immune to the attacks from outside eavesdroppers. In a word, this protocol is secure against the attacks from both external eavesdropper and internal betrayer.

5 Discussion and conclusion

As the main purpose of presenting the CLZ protocol in Ref. [51] is the use of QSDC in online shopping, in this section, we first make a discussion about the difference in detail of the QSDC process between regular quantum communications and online shopping. Then, a simple discussion of the differences among the CLZ protocol, the improved version and the proposed protocol is also made. Finally, we end the paper with a short conclusion.

5.1 Discussion

Herein, we discuss about the difference of the QSDC process between regular communications and online shopping. It is known that QSDC is presented for directly transmitting secret message between two legitimate users based on the laws of quantum mechanics. So far, many kinds of quantum techniques, such as quantum teleportation, quantum dense coding, quantum entanglement swapping, and quantum multiparticle/single-particle measurements have been utilized to design QSDC protocols. And various kinds of quantum states, such as single photons, EPR pairs, GHZ states, and W states have been used as information carriers in different QSDC protocols. From the perspective of the number of participants, QSDC protocols could be classified into two-party ones and three-party ones. The three-party QSDC protocols, such
as the protocol in Ref. [22] and the CLZ protocol, refer to the ones where exists a third party for helping or controlling the communication between the two legitimate users.

Based on the existing technical conditions, the quantum devices are still expensive since the constructions of them are difficult. Hence, what quantum abilities the participants should have (i.e., what quantum devices the participants should be equipped with) is an important factor that should be considered when designing a QSDC protocol. Obviously, if two legitimate users want to make use of a QSDC protocol to transmit secret messages between each other, they should have the same quantum ability (i.e., be equipped with the same quantum devices). Taking the QSDC protocol in Ref. [16] as an example, if two users, Alice and Bob, want to transmit secret messages between each other with this protocol (i.e., by utilizing the protocol, Alice wants send messages to Bob, and also Bob wants to send secret messages to Alice), both of them should be capable of generating single qubits, measuring single qubits, performing certain unitary operations, etc. However, when QSDC is applied to a specific scenario, the quantum hardware requirement for each of the involved participants may be different.

In the online shopping process described in Sect. 2.2, three participants, an online shopping mall, a merchant who opens an online shop in the mall and a consumer, are involved. Evidently, to complete such a online shopping process, only the consumer needs to send secret information to the merchant with QSDC. In other words, to complete the online shopping process, the three participants need not to have the same quantum ability. Actually, these three participants have different status and economic conditions in real life. Concretely, the online shopping mall, which acts as a server in the online shopping process, is usually a large corporation which has strong economic power, such as Alibaba and eBay. Hence, the online shopping mall could afford to have various kinds of quantum devices. Also, the merchant is a participant who will benefit from each of the corresponding online transactions. Therefore, it is reasonable to require the merchant to be equipped with enough quantum devices. Nevertheless, the consumer of the online shopping is usually an ordinary people. When a consumer wants to buy a product from an online shop of the mall, if he/she is required to be equipped many quantum devices, he/she is likely to give up shopping here, and then try to buy the product from another online shopping mall or even in a physical store. Therefore, when considering employing a QSDC process to guarantee the security of the online shopping, it is better to utilize a QSDC protocol which requires the message sender to be equipped with as less quantum devices as possible. That is to say, if a quantum communication-based online shopping mechanism wants to be widely applied in real life, the convenience and implement cost for the consumers must be carefully considered. Apparently, according to this principle, the protocol proposed by us in Sect. 4 is more suitable for online shopping than the CLZ protocols and the improved version.

Now we discuss about the differences among the CLZ protocol, the improved version and the proposed protocol. Firstly, in the scenario of online shopping, if the CLZ protocol/improved version is employed, the consumer Alice should be capable of generating single qubits, measuring single qubits and performing certain unitary operations. While by utilizing the proposed protocol, Alice no longer needs to be equipped with the devices for generating single qubits. Secondly, to enhance the security of the protocol against a dishonest controller, the improved version/proposed protocol makes
use of classical XOR operation and the basic idea of QSS. Therefore, there exists a clear difference between the CLZ protocol and the improved version/proposed protocol. That is, once confirming there is no eavesdropping in the whole procedure of transmission, the sender of the CLZ protocol could directly get Alice’s secret message with the help of Charlie. However, in the improved version/proposed protocol, to obtain Alice’s secret message, Bob should not only obtain the information of the initial states from Charlie, but also get the information of $K$ from Alice. Thirdly, it should be pointed out that the improved version/proposed protocol also has a important difference with the traditional QSS. In a three-party QSS protocol which involves a boss and two agents, the two agents need cooperate and both of them are able to get the boss’s secret message. While in the improved version/proposed protocol, although Bob and Charlie need to cooperate to extract Alice’s secret message, Charlie is not permitted to get the content of the secret message.

5.2 Conclusion

In this paper, we make a cryptanalysis of the CLZ protocol, which can be used for online shopping, to show that it has a security loophole. Concretely, we show that the controller of the CLZ protocol is able to obtain the whole secret message of the sender. Then, we improve this protocol to be secure against all the present attacks with classical XOR operation. After that, we propose a new protocol where the quantum devices that should be equipped by the message sender are less than those of the CLZ protocol/improved version. Hence, it is more suitable for online shopping. Finally, a discussion about the difference in detail of the QSDC process between regular quantum communications and online shopping is made.

Acknowledgments This work is supported by NSFC (Grant Nos. 61272057, 61170270, 61309029), Beijing Higher Education Young Elite Teacher Project (Grant Nos. YETP0475, YETP0477), BUPT Excellent Ph.D. Students Foundation (Grant No. CX201441).

References

1. Knill, E., Laflamme, R., Zurek, W.H.: Resilient quantum computation. Science 279, 342–345 (1998)
2. Knill, E., Laflamme, R., Milburn, G.J.: A scheme for efficient quantum computation with linear optics. Nature 409, 46–52 (2001)
3. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of 35th Annual Symposium on Foundations of Computer Science, pp. 124–134. Santa Fe (1994)
4. Bennett, C.H., Brassard, G.: In: Proceedings IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175–179. IEEE Press, New York (1984)
5. Deng, F.G., Long, G.L.: Controlled order rearrangement encryption for quantum key distribution. Phys. Rev. A 68, 042315 (2003)
6. Deng, F.G., Long, G.L.: Bidirectional quantum key distribution protocol with practical faint laser pulses. Phys. Rev. A 70, 012311 (2004)
7. Song, S.Y., Wang, C.: Recent development in quantum communication. Chin. Sci. Bull. 57, 4694–4700 (2012)
8. Liu, B., Gao, F., Wen, Q.Y.: Single-photon multiparty quantum cryptographic protocols with collective detection. IEEE J. Quantum Electron. 47, 1383–1390 (2011)
9. Lin, S., Guo, G.D., et al.: Quantum key distribution: defeating collective noise without reducing efficiency. Quantum Inf. Comput. 14, 845–856 (2014)
10. Hillery, M., Buzêk, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A. 59, 1829–1834 (1999)
11. Wang, T.Y., Wen, Q.Y., Chen, X.B., Guo, F.Z., Zhu, F.C.: An efficient and secure multiparty quantum secret sharing scheme based on single photons. Opt. Commun. 281, 6130–6134 (2008)
12. Yang, Y.G., Teng, Y.W., Chai, H.P., Wen, Q.Y.: Fault-tolerant quantum secret sharing against collective noise. Phys. Scr. 83, 025003 (2011)
13. Sun, Y., Deng, J.Z., Qin, S.J.: Quantum secret sharing with bidirectional authentication. Acta Phys. Sin. 57, 4689–4694 (2008)
14. Yan, F.L., Gao, T.: Quantum secret sharing between multiparty and multiparty without entanglement. Phys. Rev. A 72, 012304 (2005)
15. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A 65, 032302 (2002)
16. Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A 69, 052319 (2004)
17. 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)
18. Wang, C., Deng, F.G., Li, Y.S., Liu, X.S., Long, G.L.: Quantum secure direct communication with high-dimension quantum superdense coding. Phys. Rev. A 71, 044305 (2005)
19. Wang, C., Deng, F.G., Long, G.L.: Multi-step quantum secure direct communication using multi-particle Green–Horne–Zeilinger state. Opt. Commun. 253, 15–20 (2005)
20. Huang, W., Wen, Q.Y., Jia, H.Y., Qin, S.J., Gao, F.: Fault tolerant quantum secure direct communication with quantum encryption against collective noise. Chin. Phys. B 21, 100308 (2012)
21. Long, G.L., Deng, F.G., Wang, C., Li, X.H., et al.: Quantum secure direct communication and deterministic secure quantum communication. Front. Phys. China 2, 251 (2007)
22. Deng, F.G., Li, X.H., Li, C.Y., et al.: Quantum secure direct communication network with Einstein–Podolsky–Rosen pairs. Phys. Lett. A 359, 359–365 (2006)
23. Zhang, W.W., Gao, F., Liu, B., Wen, Q.Y., Chen, H.: A watermark strategy for quantum images based on quantum fourier transform. Quantum Inf. Process. 12, 793–803 (2013)
24. Zhang, W.W., Gao, F., Liu, B., Jia, H.Y.: A quantum watermark protocol. Int. J. Theor. Phys. 52, 504–513 (2013)
25. Yang, Y.G., Peng, X., Tian, J., Zhang, H.: Analysis and improvement of the dynamic watermarking scheme for quantum images using quantum wavelet transform. Quantum Inf. Process. 13, 1931–1936 (2014)
26. Gao, F., Qin, S.J., Guo, F.Z., Wen, Q.Y.: Cryptanalysis of the arbitrated quantum signature protocols. Phys. Rev. A 84, 022344 (2011)
27. Zhang, K.J., Song, T.T., Zuo, H.J., Zhang, W.W.: A secure quantum group signature scheme based on Bell states. Phys. Scr. 87, 045012 (2013)
28. Liu, B., Gao, F., Jia, H.Y., et al.: Efficient quantum private comparison employing single photons and collective detection. Quantum Inf. Process. 12, 887–897 (2012)
29. Wen, X.J., Liu, Y., Zhou, N.R.: Realizable quantum broadcasting multi-signature scheme. Int. J. Mod. Phys. B 22, 4251–4259 (2009)
30. Yang, Y.G., Wen, Q.Y.: An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. J. Phys. A Math. Theor. 42, 055305 (2009)
31. Tseng, H.Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf. Process. 11, 373–384 (2012)
32. Li, Y.B., Wen, Q.Y., Gao, F., et al.: Information leak in Liu et al.’s quantum private comparison and a new protocol. Eur. Phys. J. D 66, 110 (2012)
33. Zhang, W.W., Li, D., Zhang, K.J., Zuo, H.J.: A quantum protocol for millionaire problem with Bell states. Quantum Inf. Process. 12, 2241–2249 (2013)
34. Huang, W., Wen, Q.Y., Liu, B., Gao, F., Sun, Y.: Robust and efficient quantum private comparison of equality with collective detection over collective-noise channels. Sci. China Phys. Mech. Astron. 56, 1670–1678 (2013)
35. Huang, W., Wen, Q.Y., Liu, B., et al.: Quantum anonymous ranking. Phys. Rev. A 89, 032325 (2014)
36. Wen, X.J.: An E-payment system based on quantum group signature. Phys. Scr. 82, 065403–065407 (2010)
37. Wen, X.J., Nie, Z.: An E-payment system based on quantum blind and group signature. In: Proceedings of International Symposium on Data, Privacy, and E-Commerce, America (2010)
38. Wen, X.J., Chen, Y.Z., Fang, J.B.: An inter-bank E-payment protocol based on quantum proxy blind signature. Quantum Inf. Process. 12, 549–558 (2013)
39. Cai, X.Q., Wei, C.Y.: Cryptanalysis of an inter-bank E-payment protocol based on quantum proxy blind signature. Quantum Inf. Process. 12, 1651–1657 (2013)
40. Gao, F., Qin, S.J., Guo, F.Z., Wen, Q.Y.: Dense-coding attack on three-party quantum key distribution protocols. IEEE J. Quantum Electron. 47, 630–635 (2011)
41. Huang, W., Wen, Q.Y., Liu, B., Gao, F., Sun, Y.: Cryptanalysis of a multi-party quantum key agreement protocol with single particles. Quantum Inf. Process. 13, 1651–1657 (2013)
42. Lo, H.K., Ko, T.M.: Some attacks on quantum-based cryptographic protocols. Quantum Inf. Comput. 5, 40–47 (2005)
43. Liu, B., Gao, F., Wen, Q.Y.: Eavesdropping and improvement to multiparty quantum secret sharing with collective eavesdropping-check. Int. J. Theor. Phys. 51, 1211–1223 (2012)
44. Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.C.: Comment on “experimental demonstration of a quantum protocol for Byzantine agreement and liar detection”. Phys. Rev. Lett. 101, 208901 (2008)
45. Gao, F., Wen, Q.Y., Zhu, F.C.: Comment on: “Quantum exam”. Phys. Lett. A 360, 748 (2007)
46. Qin, S.J., Gao, F., Guo, F.Z., Wen, Q.Y.: Comment on “Two-way protocols for quantum cryptography with a nonmaximally entangled qubit pair”. Phys. Rev. A 82, 036301 (2010)
47. Gisin, N., Fasel, S., Kraus, B., Zbinden, H., Ribordy, G.: Trojan-horse attacks on quantum-key-distribution systems. Phys. Rev. A 73, 022320 (2006)
48. Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: A simple participant attack on the brádler-dušek protocol. Quantum Inf. Comput. 7, 329–334 (2007)
49. Wang, Q.L., Zhang, W.W., Su, Q.: Revisiting “The loophole of the improved secure quantum sealed-bid auction with post-confirmation and solution”. Int. J. Theor. Phys. 53, 3147–3153 (2014)
50. Wang, Q.L., Zhang, K.J.: Security analysis and improvement of the dining cryptographer problem-based anonymous quantum communication via non-maximally entanglement state analysis. Int. J. Theor. Phys. 54, 106–115 (2015)
51. Chou, Y.H., Lin, F.J., Zeng, G.J.: An efficient novel online shopping mechanism based on quantum communication. Electron. Commer. Res. 14, 349–367 (2014)
52. Cai, Q.Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A 351, 23 (2006)
53. 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, 054302 (2006)
54. D’Ariano, G.M., Lo Presti, P., Paris, M.G.A.: Using entanglement improves the precision of quantum measurements. Phys. Rev. Lett. 87, 270404 (2001)