Efficient and Secure Authenticated Quantum Dialogue with Single Photons

Wenjun Luo and Guang Liu

ABSTRACT

A new quantum dialogue (QD) protocol with single photons is proposed. In the proposed protocol, two participants perform different operations according to their own secret information. A key previously shared by the two communicants through a secure QKD protocol is used to control not only the encoding operation of the dialogue initiator but also security detection. The analysis on efficiency demonstrates the proposed protocol is more efficient.

INTRODUCTION

Quantum cryptography has developed rapidly since the first quantum key distribution (QKD) protocol was proposed by Bennett and Brassard[1] in 1984 (usually called BB84). Quantum secure direct communication (QSDC) is another significant discovery of Quantum cryptography and allows the secret messages to be transmitted directly without pre-shared secret key[2]. So far, many QSDC protocols based on different types of quantum states have been designed, such as single photons[3] and Einstein-Podolsky-Rosen (EPR)[4] etc.. In 2004, another novel kind of quantum secure communication, called Quantum dialogue (QD), was put forward by Nguyen et al.[5] and it permits the two participants to exchange their respective secret messages simultaneously. Up to now, various QD protocols have been proposed based on single photons[6-13] or entanglement states[5,14]. The security, efficiency and practicability are the focus of quantum communication protocols. Obviously, the protocol with single photon is easier to implement under current experimental techniques. The single-photon QD protocols[6-8] originally designed suffer from information leakage risk[15]. That is, the eavesdropping can deduce useful information about secret message of the two communicants from public information that they announce. After that, different QD protocols without information leakage began to appear[9-13].
Dialogue with Single Photons

In the proposed protocol, three unitary operations, $I, i\sigma_y$ and $H$ are used to design the operations performed by Alice and Bob. Alice’s encoding operation set is $\{I, H\}$ and then she makes operation $I$ or $i\sigma_y$ under the control of the pre-shared key. Bob’s encoding operation set is $\{I, i\sigma_y\}$. Compared with previous schemes[9-13] with single photons, the proposed protocol has enhanced the efficiency.

The rest of the paper is organized as follows. Section 2 presents the new QD protocol. Section 3 discusses the security analyses of the proposed QD protocol and the comparison with previous protocols. Finally, a conclusion is drawn in Section 4.

THE PROPOSED QD PROTOCOL

Assume that the two communicants, Alice and Bob, have a secret message sequence $M_A = \{m_A^1, m_A^2, \ldots, m_A^n\}$ and $M_B = \{m_B^1, m_B^2, \ldots, m_B^n\}$, respectively, where $m_A^i, m_B^i \in \{0,1\}$, $i=1,2,\ldots,n$. The three unitary operations $I, i\sigma_y$ and $H$ to encode secret message are $I = |0\rangle\langle 0| + |1\rangle\langle 1|$, $\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$ and $H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 1|)$. Table 1 shows the result states of a photon in the four different states $\{|0\rangle, |1\rangle, |+\rangle, |\rangle\rangle$ after performing the above three operations.

Table 1. Results after performing unitary operations on single-photons.

| operation | $|0\rangle$ | $|1\rangle$ | $|+\rangle$ | $|\rangle\rangle$ |
|-----------|-----------|-----------|-----------|-----------|
| $I$       | $|0\rangle$ | $|1\rangle$ | $|+\rangle$ | $|\rangle\rangle$ |
| $i\sigma_y$ | $-|1\rangle$ | $|0\rangle$ | $|\rangle\rangle$ | $-|+\rangle$ |
| $H$       | $|+\rangle$ | $|\rangle\rangle$ | $|0\rangle$ | $|1\rangle$ |

Our QD protocol can proceed in the following steps (also see Figure 1):

1. Authentication key distribution: $K_{ab} = \{K_{ab}^1, K_{ab}^2, \ldots, K_{ab}^n\}$

2. Information transmission from Alice to Bob:
   a) prepares $S_a \in \{|0\rangle, |1\rangle\}$; encodes $M_a$ by making $I / H$ on $S_a$ and gets $S_a$
   b) implements $I / i\sigma_y$ on $S_a$ based on $K_{ab}^n$ and gets $S_a$
   c) prepares $S_B \in \{|0\rangle, |+\rangle, |\rangle\rangle\}$ and mixes $S_a$ and $S_B$ based on $K_{ab}^n$

3. The first security checking

4. Information transmission from Bob to Alice:
   a) encodes $M_b$ by making $I / i\sigma_y$ on $S_a$ and gets $S_a$
   b) prepares $S_a \in \{|0\rangle, |+\rangle, |\rangle\rangle\}$ and mixes $S_a$ and $S_B$ based on $K_{ba}^n$

5. The second security checking

6. Information decoding:
   a) measures $S_a$ based on $M_a$ and generates $M$
   b) publishes $M$
   c) $M = M_a \oplus M_a \oplus K_{ab}^\prime$
   d) $M = M_a \oplus M_a \oplus K_{ab}^\prime$

Figure 1. The QD protocol.
(1) Alice and Bob previously share secret keys $K_{ab} = (k_{ab}^1, k_{ab}^2, ..., k_{ab}^{2n})$ with 2n bits through a secure QKD protocol[1]. For simplicity, we use the symbols $K_{ab}^{(1)}$ and $K_{ab}^{(2)}$ to denote the first and second n bits of $K_{ab}$, respectively.

(2) a) Alice prepares a sequence $S_1 = \{s_1^1, s_1^2, ..., s_1^n\}$ composed of n single photons randomly in one of the two states $\{|0\rangle, |1\rangle\}$. Then she encodes her secret message on each particle in $S_1$ by performing operations $I$ or $H$. That is, if $m_i^1$ is 0, she performs unitary operation $I$ on $s_i^1$; otherwise, unitary operation $H$ is selected. The encoded sequence is denoted as $S_2 = \{s_2^1, s_2^2, ..., s_2^n\}$; b) Alice implements operation $I$ or $i\sigma_y$ on each particle in the sequence $S_2$ based on the per-shared $K_{ab}^{(1)}$. If $k_{ab}^i$ is 0(or 1), she performs $I$ (or $i\sigma_y$) on $s_i^1$. Then $S_2$ will be transformed into a new sequence, called $S_3 = \{s_3^1, s_3^2, ..., s_3^n\}$; c) According to $K_{ab}^{(1)}$, Alice prepares detection sequence $D = \{d_1, d_2, ..., d_n\}$. Concretely, if $k_{ab}^i$ is 0, $d_i$ is randomly in the state $|0\rangle$ or $|+\rangle$ and the position of insertion will be before $s_i^1$; otherwise, the state of $d_i$ is $|1\rangle$ or $|\rangle$ and will be inserted behind $s_i^1$. Subsequently, Alice sends the new sequence to Bob and keeps the initial states of $S_1$ secret.

(3) Once confirming Bob has received the sequence, Alice publishes the original bases of the detection particles to Bob in order. Then Bob extracts detection sequence $S_0$ from the received sequence according to $K_{ab}^{(1)}$ and measures the detection particles. Finally, he can recover $K_{ab}^{(1)'}$ and compare $K_{ab}^{(1)'}$ with $K_{ab}^{(1)}$. If $K_{ab}^{(1)'}$ equals $K_{ab}^{(1)}$, Bob believes the channel has not been interfered and the sender is Alice, he continues the next step; otherwise he halts the communication and informs Alice.

(4) Bob recovers the sequence $S_3$ and implements the following procedures: a) Bob executes encoding operations on the photons in $S_3$ according to his secret message. That is, if $m_i^2$ is 0 (or 1), he performs $I$ (or $i\sigma_y$) on $s_i^2$. Consequently, he gets a new sequence $S_4 = \{s_4^1, s_4^2, ..., s_4^n\}$; b) As what Alice has done in Step 2, Bob also prepares detection sequence and inserts the detection photons into the sequence $S_4$ based on $K_{ab}^{(2)}$, then sends the new sequence to Alice.

(5) After receiving the sequence from Bob, Alice and Bob use the same method as that described in Step 3 to check whether the quantum channel is safe. Once Alice confirms Bob is legal, she continues the communication; otherwise she terminates the communication.

(6) Alice gets the sequences $S_4$ after she removes detection sequence. Then the decoding procedures are as follows: a) Alice measures the photons in $S_4$ with correct basis based on her secret message $M_A$. That is, she uses Z-basis $\{|0\rangle, |1\rangle\}$ to measure $s_i^1$ if $m_i^1$ is 0; otherwise, X-basis $\{|+, -\rangle\}$ will be used. Subsequently, Alice generates classical bits $M = \{m_i^1 | m_i^1 \in \{0, 1\}, i = \{1, 2, ..., n\}\}$ according to the initial states of $S_4$ and measurement results of $S_4$. The rule is shown in Table 2; b) Alice publishes the outcome M to Bob; c) According to M and $K_{ab}^{(1)}$, Alice can obtain Bob’s secret messages

$$M_B = M \oplus M_A \oplus K_{ab}^{(1)}$$

(1)
d) Similarly, Bob can also infer Alice’s secret messages

\[ M_a = M \oplus M_b \oplus K_{i_a}^{(i)} \]  

(2)

**Table 2.** The rule to generate M.

<table>
<thead>
<tr>
<th>Initial state</th>
<th>Measurement result</th>
<th>Classical bit ( m' )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(</td>
<td>0\rangle )</td>
<td>(</td>
</tr>
<tr>
<td>(</td>
<td>1\rangle )</td>
<td>(</td>
</tr>
<tr>
<td>(</td>
<td>0\rangle )</td>
<td>(</td>
</tr>
<tr>
<td>(</td>
<td>1\rangle )</td>
<td>(</td>
</tr>
</tbody>
</table>

**SECURITY ANALYSES AND COMPARISONS**

**Information Leakage**

Information leakage indicates that a malicious eavesdropper, Eve, can deduce partial or entire secret message only from the public announcement without taking any active attacks. In the proposed QD protocol, Eve can only obtain the public information M announced by Alice in Step 6. According to Eq.(1) and (2), Eve can only infer the secret message \( M_i \oplus M_{i'} \oplus k_{i_{ba}}^{(i)} \) since she has no knowledge of the key \( k_{i_{ba}}^{(i)} \). Thus, the quantum channel contains \( - \sum p_i \log_2 p_i = -4 \cdot \frac{1}{4} \log_2 \frac{1}{4} = 2 \) bit information for Eve. This amount of information is just equal to the number of classical bits encoded on a qubit. Namely, the proposed protocol can be free from information leakage.

**Comparisons**

The formula \( \eta = \frac{c}{q} \) is usually applied to analyze the efficiency of QD protocols[12,13], where \( c \) is the total number of secret classical bits exchanged between two communicants, \( q \) denotes the total number of particles used in the quantum channel. In the QD protocol, Alice and Bob totally exchange \( 2n \) classical bits, and the total particles used for this protocol is \( 3n \) (\( n \) particles for carrying secret messages and \( 2n \) particles for eavesdropping detection). Thus, the efficiency is \( \eta = \frac{2n}{n + 2n} = 66.7\% \). As we can see from Table 2, our proposed protocol owns the obvious superiority in the efficiency.

**Table 4.** Efficiencies of QD protocols.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>( c )</td>
<td>2n</td>
<td>2n</td>
<td>2n</td>
<td>2n</td>
<td>2n</td>
<td>2n</td>
</tr>
<tr>
<td>( q )</td>
<td>6n</td>
<td>6n</td>
<td>4n</td>
<td>4n</td>
<td>4n</td>
<td>3n</td>
</tr>
<tr>
<td>( \eta )</td>
<td>33.3%</td>
<td>33.3%</td>
<td>50%</td>
<td>50%</td>
<td>50%</td>
<td>66.7%</td>
</tr>
</tbody>
</table>
CONCLUSION

In this paper, a secure authenticated QD protocol without information leakage based on single photons is proposed. The proposed QD protocol not only can fix the defect of information leakage, but also has a higher efficiency than the existing similar QD schemes.

REFERENCES