A novel semiquantum key distribution protocol with Bell states

Zhenying Sun (sun_zzut@163.com)
Zhengzhou University of Technology

Research Article

Keywords: Semiquantum key distribution, Bell state, reflecting operation

Posted Date: December 21st, 2023

DOI: https://doi.org/10.21203/rs.3.rs-3758182/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License

Additional Declarations: No competing interests reported.
A novel semiquantum key distribution protocol with
Bell states

Zhenying Sun*

College of Information and Engineering, Zhengzhou University of Technology, Zhengzhou, Henan, China, 450044
E-mail: sun_zzut@163.com

Abstract: In this paper, a novel semiquantum key distribution (SQKD) protocol is proposed by using Bell state, where quantum Alice can share $N$ secret bits with classical Bob via quantum channel. Classical Bob is required to measure particles with the $Z$ basis, produce fresh particles within the $Z$ basis and send particles via quantum channel. Security analysis turns out that this protocol is immune to various attacks launched by the outside eavesdropper. Compared with present SQKD protocols using Bell states without a third party, on one hand, this protocol has the highest qubit efficiency; and on the other hand, the reflecting operations of the classical user in this protocol contribute to the generation of final shared key.

Keywords: Semiquantum key distribution; Bell state; reflecting operation

1 Introduction

Quantum key distribution (QKD), which was first proposed by Bennett and Brassard [1] in 1984, is devoted to creating a private key shared between two remote users. In a quantum key distribution scheme [1,2], two remote users are always required to full quantum capabilities. Later, Boyer et al. [3,4] put forward the novel concept of semiquantum key distribution (SQKD), which releases a part of user from possessing full quantum capabilities. In Boyer et al.’s SQKD schemes [3,4], the classical user is restricted for the following actions: measuring particles with the $Z$ basis (i.e., $\{0,1\}$), producing fresh particles with the $Z$ basis, sending particles and scrambling particles via delay lines. In 2016, Krawec [5] put forward a novel SQKD scheme where the reflection operations (i.e., the receiver sending particles back to the sender without disturbance) of the classical user contribute to the generation of secret key. Subsequently, Ye et al. [6,7] utilized single photons in both polarization and spatial-mode degrees of freedom to design two novel SQKD schemes. Besides single photons based SQKD [1-7], numerous Bell states based SQKD schemes [8-11] have also been designed. However, in Bell states based SQKD schemes [8-11], the reflection operations of the classical user cannot contribute to the generation of secret key, which may decrease the qubit efficiency of communication.

In this paper, a novel Bell states based SQKD scheme is designed, where the reflection operations of the classical user contribute to the generation of secret key. Compared with present SQKD protocols using Bell states without a third party [8,9,11], this protocol has the highest qubit efficiency.

2 The proposed protocol

Alice can establish a private key of length $N$ together with Bob through the following protocol.

Step 1: Alice produces a random bit sequence of length $2N$ (i.e., $C_a$) with a random number generator. In the meanwhile, Bob produces a random bit sequence of length $2N$ (i.e., $C_b$) with another random number generator.
Step 2: Alice produces $2N$ Bell states randomly in the four states $\{\phi^+\}, \{\phi^-\}, \{\psi^+\}, \{\psi^-\}$, and splits these Bell states into two particle sequences, $S_A$ and $S_B$. Here, $|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, $|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$, and $S_A$ is composed by all first particles of these Bell states, while $S_B$ is composed by all second particles of these Bell states. Then, Alice keeps $S_A$ in her hand and sends the particles of $S_B$ to Bob one by one. Except the first particle, Alice sends out the next particle only after receiving the previous one.

Step 3: On receiving the $j$th particle of $S_B$, when $C'_b = 0$, Bob enters into the REFLECT_B mode; and when $C'_b = 1$, Bob enters into the FLIP_B mode. Here, $C'_b$ is the $j$th bit of $C_B$ and $j = 1, 2, \ldots, 2N$. Concretely, in the REFLECT_B mode, Bob returns the $j$th particle of $S_b$ to Alice directly; and in the FLIP_B mode, Bob measures the $j$th particle of $S_b$ with the $Z$ basis, produces a fresh particle in the state opposite to his corresponding measurement result and sends this fresh one back to Alice. Note that the opposite state of $|0\rangle$ is $|1\rangle$, vice versa. The new particle sequence after Bob’s operations is called as $S'_b$.

Step 4: After receiving all particles of $S_b$ from Bob, Alice performs her operations on the particles of $S_A$. That is, for the $j$th particle of $S_A$, when $C'_a = 0$, Alice enters into the REFLECT_A mode; and when $C'_a = 1$, Alice enters into the FLIP_A mode. Here, $C'_a$ is the $j$th bit of $C_A$ and $j = 1, 2, \ldots, 2N$. Concretely, in the REFLECT_A mode, Alice does nothing on the $j$th particle of $S_a$; and in the FLIP_A mode, Alice measures the $j$th particle of $S_a$ with the $Z$ basis, produces a fresh particle in the state opposite to her corresponding measurement result and keeps this fresh one in her hand. The new particle sequence after Alice’s operations is called as $S'_a$.

Step 5: In order to check the security of quantum channel, Alice randomly chooses half particles of $S'_b$ and requires Bob to publish his operation modes for the corresponding particles of $S_b$.

When Alice entered into the REFLECT_A mode for the corresponding particle of $S_a$ and Bob entered into the REFLECT_B mode for the corresponding particle of $S_b$, Alice performs Bell basis measurement on the corresponding particles of $S_a$ and $S_b$. When there is no eavesdropper, Alice’s Bell basis measurement result should be same to the initial prepared state.

When Alice entered into the REFLECT_A mode for the corresponding particle of $S_a$ and Bob entered into the FLIP_B mode for the corresponding particle of $S_b$, Alice measures the corresponding particles of $S_a$ and $S_b$ with the $Z$ basis and requires Bob to publish his $Z$ basis measurement result on the corresponding particle of $S_b$. When there is no eavesdropper, Alice’s $Z$ basis measurement results on the corresponding particles of $S_a$ and $S_b$ and Bob’s $Z$ basis measurement result on the corresponding particle of $S_b$ should be correctly related.

When Alice entered into the FLIP_A mode for the corresponding particle of $S_a$ and Bob entered into the REFLECT_B mode for the corresponding particle of $S_b$, Alice measures the corresponding particles of $S_a$ and $S_b$ with the $Z$ basis. When there is no eavesdropper, Alice’s $Z$
basis measurement results on the corresponding particles of $S'_A$ and $S'_B$ should be correctly related.

When Alice entered into the FLIP_A mode for the corresponding particle of $S_A$, and Bob entered into the FLIP_B mode for the corresponding particle of $S_B$, Alice measures the corresponding particles of $S'_A$ and $S'_B$ with the Z basis and requires Bob to publish his Z basis measurement result on the corresponding particle of $S_B$. When there is no eavesdropper, Alice’s Z basis measurement results on the corresponding particles of $S'_A$ and $S'_B$ and Bob’s Z basis measurement result on the corresponding particle of $S_B$ should be correctly related.

If the error rate of either of the above four Cases is abnormally high, Alice and Bob will stop the protocol; otherwise, the next Step will be implemented.

**Step 6**: There are $N$ particles of $S'_A$ and $N$ particles of $S'_B$ left now. Alice performs Bell basis measurement on the $i$ th remaining particles of $S'_A$ and $S'_B$, where $i=1,2,...,N$. According to her measurement result on the $i$ th remaining particles of $S'_A$ and $S'_B$ and the corresponding initial prepared state, Alice obtains a classical bit $T'_i$ according to the following rule: when the corresponding initial prepared state is $|\Phi^+\rangle$ or $|\Phi^-\rangle$ and Alice’s measurement result is $|\Phi^+\rangle$ or $|\Phi^-\rangle$, Alice gets $T'_i=0$; when the corresponding initial prepared state is $|\Phi^+\rangle$ or $|\Phi^-\rangle$ and Alice’s measurement result is $|\Psi^+\rangle$ or $|\Psi^-\rangle$, Alice gets $T'_i=1$; when the corresponding initial prepared state is $|\Psi^+\rangle$ or $|\Psi^-\rangle$ and Alice’s measurement result is $|\Phi^+\rangle$ or $|\Phi^-\rangle$, Alice gets $T'_i=1$; when the corresponding initial prepared state is $|\Psi^+\rangle$ or $|\Psi^-\rangle$ and Alice’s measurement result is $|\Psi^-\rangle$ or $|\Psi^+\rangle$, Alice gets $T'_i=0$. The relationships among Alice’s measurement result on the $i$ th remaining particles of $S'_A$ and $S'_B$, the corresponding initial prepared state, $C'_A$ and $C'_B$ are summarized in Table 1. According to Table 1, it is easy to get that $T'_i = C'_A \oplus C'_B$. Alice can obtain $C'_B$ by calculating $T'_i \oplus C'_A$. Until now, Alice and Bob share the secret key bit $C'_B$, where $i=1,2,...,N$.

3 Security Analysis

(1) The intercept-resend attack

Eve intercepts the particle of $S_B$ sent from Alice and transmits the fake one she prepared within the Z basis in advance to Bob instead. When Alice enters into the REFLECT_A mode for the corresponding particle of $S_A$ and Bob enters into the REFLECT_B mode for the fake particle, the attack behavior of Eve can be detected with the probability of $\frac{3}{4}$; when Alice enters into the FLIP_A mode for the corresponding particle of $S_A$ and Bob enters into the REFLECT_B mode for the fake particle, the attack behavior of Eve can be detected with the probability of $\frac{1}{2}$; when Alice enters into the FLIP_A mode for the corresponding particle of $S_A$ and Bob enters into the REFLECT_B mode for the fake particle, the attack behavior of Eve can be detected with the probability of $\frac{1}{2}$; and when Alice enters into the FLIP_A mode for the corresponding particle of $S_A$ and Bob enters into the FLIP_B mode for the fake particle, the attack behavior of Eve can be detected with...
the probability of $\frac{1}{2}$. Because one particle of $S_a$ is chosen for security check with the probability of $\frac{1}{2}$, Eve’s intercept-resend attack on one particle of $S_a$ is detected with the probability of $\frac{1}{2} \left(\frac{1}{4} \times \frac{3}{4} + \frac{1}{4} \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{4} \times \frac{1}{2} \right) = \frac{9}{32}$. As there are $N$ particles of $S_a$ chosen for security check, Eve’s intercept-resend attack is detected with the probability of $1 - \left(1 - \frac{9}{32}\right)^N = 1 - \left(\frac{23}{32}\right)^N$.

Table 1  Relationships among Alice’s measurement result on the $i$th remaining particles of $S_i$ and $S_a$, the corresponding initial prepared state, $C_i$, $C_s$ and $T_i$

<table>
<thead>
<tr>
<th>Initial prepared state</th>
<th>$C_i$</th>
<th>$C_s$</th>
<th>Alice’s measurement result on the $i$th remaining particles of $S_i$ and $S_a$</th>
<th>$T_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0</td>
<td>$</td>
<td>\phi^\prime\rangle$</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0 1</td>
<td>$</td>
<td>\phi^\prime\rangle$</td>
<td>0</td>
<td>$</td>
</tr>
<tr>
<td>1 0</td>
<td>$</td>
<td>\phi^\prime\rangle$</td>
<td>0</td>
<td>$</td>
</tr>
<tr>
<td>1 1</td>
<td>$</td>
<td>\phi^\prime\rangle$</td>
<td>0</td>
<td>$</td>
</tr>
<tr>
<td>0 0</td>
<td>$</td>
<td>\phi^\prime\rangle$</td>
<td>0</td>
<td>$</td>
</tr>
<tr>
<td>0 1</td>
<td>$</td>
<td>\phi^\prime\rangle$</td>
<td>0</td>
<td>$</td>
</tr>
<tr>
<td>1 0</td>
<td>$</td>
<td>\phi^\prime\rangle$</td>
<td>0</td>
<td>$</td>
</tr>
<tr>
<td>1 1</td>
<td>$</td>
<td>\phi^\prime\rangle$</td>
<td>0</td>
<td>$</td>
</tr>
<tr>
<td>0 0</td>
<td>$</td>
<td>\phi^\prime\rangle$</td>
<td>0</td>
<td>$</td>
</tr>
<tr>
<td>0 1</td>
<td>$</td>
<td>\phi^\prime\rangle$</td>
<td>0</td>
<td>$</td>
</tr>
<tr>
<td>1 0</td>
<td>$</td>
<td>\phi^\prime\rangle$</td>
<td>0</td>
<td>$</td>
</tr>
<tr>
<td>1 1</td>
<td>$</td>
<td>\phi^\prime\rangle$</td>
<td>0</td>
<td>$</td>
</tr>
<tr>
<td>0 0</td>
<td>$</td>
<td>\phi^\prime\rangle$</td>
<td>0</td>
<td>$</td>
</tr>
<tr>
<td>0 1</td>
<td>$</td>
<td>\phi^\prime\rangle$</td>
<td>0</td>
<td>$</td>
</tr>
<tr>
<td>1 0</td>
<td>$</td>
<td>\phi^\prime\rangle$</td>
<td>0</td>
<td>$</td>
</tr>
<tr>
<td>1 1</td>
<td>$</td>
<td>\phi^\prime\rangle$</td>
<td>0</td>
<td>$</td>
</tr>
</tbody>
</table>

(2) The measure-resend attack

Eve intercepts the particle of $S_b$ sent from Alice, measures it with the $Z$ basis and sends the obtained state to Bob instead. When Alice enters into the REFLECT_A mode for the corresponding particle of $S_a$ and Bob enters into the REFLECT_B mode for the received particle, the attack behavior of Eve can be detected with the probability of $\frac{1}{2}$; when Alice enters into the FLIP_A mode for the corresponding particle of $S_a$ and Bob enters into the REFLECT_B mode for the received particle, the attack behavior of Eve can be detected with the probability of 0; when Alice enters into the REFLECT_A mode for the corresponding particle of $S_a$ and Bob enters into the FLIP_B mode for the received particle, the attack behavior of Eve can be detected with the probability of 0; and when Alice enters into the FLIP_A mode for the corresponding particle of $S_a$ and Bob enters into the FLIP_B mode for the received particle, the attack behavior of Eve can be detected with the
probability of 0. Because one particle of $S_a$ is chosen for security check with the probability of $\frac{1}{2}$, Eve’s measure-resend attack on one particle of $S_a$ is detected with the probability of $\frac{1}{2} \times \left( \frac{1}{4} \times \frac{1}{2} + \frac{1}{4} \times 0 + \frac{1}{4} \times 0 + \frac{1}{4} \times 0 \right) = \frac{1}{16}$. As there are $N$ particles of $S_a$ chosen for security check, Eve’s measure-resend attack is detected with the probability of $1 - \left( 1 - \frac{1}{16} \right)^N = 1 - \left( \frac{15}{16} \right)^N$.

(3) The Trojan horse attack

Alice sends the particles of $S_a$ to Bob; after his operations, Bob sends the particles of $S'_b$ to Alice. The receiver can put a wavelength filter and a photon number splitter in front of her device to defeat Eve’s invisible photon eavesdropping attack and delay-photon Trojan horse attack, respectively [12,13].

4 Discussion and conclusion

The communication efficiency of this protocol is evaluated by the qubit efficiency, which is defined as [2]

$$\eta = \frac{\lambda_k}{\lambda_q + \lambda_c}. \quad (1)$$

Here, $\lambda_k$ is the number of secret bits established between Alice and Bob, $\lambda_q$ is the number of consumed qubits and $\lambda_c$ is the number of consumed classical bits via classical communication. Here disregards the classical resources consumed during security check processes. In this protocol, the number of secret bits established between Alice and Bob is $N$, so $\lambda_k = N$. Alice produces $2N$ Bell states randomly in the four states $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$, splits these Bell states into $S_a$ and $S_b$, and keeps $S_a$ in her hand and sends the particles of $S'_b$ to Bob one by one. When Alice entered into the FLIP_A mode for half particles of $S_a$, she needs to produce $N$ fresh qubits; and when Bob entered into the FLIP_B mode for half particles of $S_b$, he also needs to produce $N$ fresh qubits. Hence, $\lambda_q = 2N \times 2 + N + N = 6N$. No classical communication is required, except that of security check processes, so $\lambda_c = 0$. Therefore, this protocol has a qubit efficiency of $\eta = \frac{N}{6N} = \frac{1}{6}$.

In addition, the comparison of this protocol and present SQKD protocols using Bell states without a third party [8,9,11] are made. The comparison results are shown in Table 2 for clarity. It is apparent from Table 2 that compared with the SQKD protocols in Refs.[8,9,11], this protocol has the highest qubit efficiency and has the merit that the reflecting operations of the classical user contribute to the generation of final shared key.

In summary, a novel SQKD protocol based on Bell state is put forward, in order to realize that quantum Alice establishes $N$ secret bits together with classical Bob via quantum channel. Classical Bob needs to measure particles with the $Z$ basis, produce fresh particles within the $Z$ basis and send
particles via quantum channel. This protocol is proven to be secure against various attacks from Eve. Compared with present SQKD protocols using Bell states without a third party [8,9,11], this protocol has two merits: (1) it has the highest qubit efficiency; and (2) the reflecting operations of the classical user contribute to the generation of final shared key.

Table 2  Comparison results of this protocol and present SQKD protocols using Bell states without a third party

<table>
<thead>
<tr>
<th>Initial quantum resource</th>
<th>Existence of a third party</th>
<th>Quantum measurement of the classical user</th>
<th>Quantum state preparation of the classical user</th>
<th>Whether the reflecting operations of the classical user contribute to the generation of final shared key</th>
<th>Qubit efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>The protocol of Ref.[8]</td>
<td>Bell states No Z basis measurements states within the Z basis</td>
<td>No</td>
<td>No</td>
<td>$\frac{1}{10(1+\delta)}$</td>
<td></td>
</tr>
<tr>
<td>The measure-resend protocol of Ref.[9]</td>
<td>Bell states No Z basis measurements states within the Z basis</td>
<td>No</td>
<td></td>
<td>$\frac{1}{10}$</td>
<td></td>
</tr>
<tr>
<td>The protocol of Ref.[11]</td>
<td>Bell states No Z basis measurements states within the Z basis</td>
<td>No</td>
<td>No</td>
<td>$\frac{1}{12(1+\delta)}$</td>
<td></td>
</tr>
<tr>
<td>This protocol</td>
<td>Bell states No Z basis measurements states within the Z basis</td>
<td>No</td>
<td>Yes</td>
<td>$\frac{1}{6}$</td>
<td></td>
</tr>
</tbody>
</table>

Acknowledgments

This work is supported by the Henan province science and technology projects (No.222102210222).

References

polarization and spatial-mode degrees of freedom. Quantum Inf Process, 2022, 21:123


