

Efficient semi-quantum secret sharing protocol using single particles

Ding Xing(邢丁), Yifei Wang(王艺霏), Zhao Dou(窦钊), Jian Li(李剑), Xiubo Chen(陈秀波), and Lixiang Li(李丽香)
Citation: Chin. Phys. B, 2023, 32 (**7**): 070308. DOI: 10.1088/1674-1056/ace159
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Faithful and efficient hyperentanglement purification for spatial-polarization-time-bin photon system

Fang-Fang Du(杜芳芳), Gang Fan(樊钢), Yi-Ming Wu(吴一鸣), and Bao-Cang Ren(任宝藏)
Chin. Phys. B, 2023, 32 (**6**): 060304. DOI: 10.1088/1674-1056/aca395

Rigorous solution to second harmonic generation considering transmission and reflection of light at air-crystal interface

Ya-Ting Qiu(邱雅婷), Li-Hong Hong(洪丽红), and Zhi-Yuan Li(李志远)
Chin. Phys. B, 2023, 32 (**5**): 050301. DOI: 10.1088/1674-1056/ac9fc5

Realization of the iSWAP-like gate among the superconducting qutrits

Peng Xu(许鹏), Ran Zhang(张然), and Sheng-Mei Zhao(赵生妹)
Chin. Phys. B, 2023, 32 (**2**): 020306. DOI: 10.1088/1674-1056/ac89e7

Novel traveling quantum anonymous voting scheme via GHZ states

Wenhao Zhao(赵文浩) and Min Jiang(姜敏)
Chin. Phys. B, 2023, 32 (**2**): 020303. DOI: 10.1088/1674-1056/ac9b2e

Enhancement of charging performance of quantum battery via quantum coherence of bath

Wen-Li Yu(于文莉), Yun Zhang(张允), Hai Li(李海), Guang-Fen Wei(魏广芬), Li-Ping Han(韩丽萍), Feng Tian(田峰), and Jian Zou(邹建)
Chin. Phys. B, 2023, 32 (**1**): 010302. DOI: 10.1088/1674-1056/ac728b

---

Efficient semi-quantum secret sharing protocol using single particles

Ding Xing(邢丁)[1], Yifei Wang(王艺霏)[1], Zhao Dou(窦钊)[1,†], Jian Li(李剑)[2], Xiubo Chen(陈秀波)[1], and Lixiang Li(李丽香)[1]

[1] *Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*

[2] *Information Security Center, School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*

(Received 2 April 2023; revised manuscript received 21 June 2023; accepted manuscript online 25 June 2023)

Semi-quantum secret sharing (SQSS) is a branch of quantum cryptography which only requires the dealer to have quantum capabilities, reducing the difficulty of protocol implementation. However, the efficiency of the SQSS protocol still needs to be further studied. In this paper, we propose a semi-quantum secret sharing protocol, whose efficiency can approach 100% as the length of message increases. The protocol is based on single particles to reduce the difficulty of resource preparation. Particle reordering, a simple but effective operation, is used in the protocol to improve efficiency and ensure security. Furthermore, our protocol can share specific secrets while most SQSS protocols could not. We also prove that the protocol is secure against common attacks.

Keywords: semi-quantum secret sharing, efficiency, single particles, specific secret, particle reordering

PACS: 03.67.Dd, 03.67.Ac, 03.67.Hk **DOI:** 10.1088/1674-1056/ace159

1. Introduction

Secret sharing (SS)[1] is a widely used and efficient privacy protection protocol. It allows a dealer to share a secret among many agents, but only if they cooperate can the agents recover the dealer's secret or they obtain nothing alone.[2–4] However, classical secret sharing (CSS) is unable to address the problem of eavesdropping if it is not combined with other technologies such as encryption, and the introduction of quantum algorithms brings a huge potential threat to classical encryption algorithms.[5,6] Fortunately, quantum cryptography can solve these security problems. By determining whether an eavesdropper has attempted to gain information about the secret, quantum secret sharing (QSS) can provide for secure secret transmission.

In 1999, Hillery *et al.*[7] proposed the first QSS protocol based on the three-particle entangled GHZ states, attracting extensive attention. Since then, many researchers have studied the field of quantum secret sharing, and kinds of QSS protocols have been put forward.[8–15] However, those QSS protocols require all participants (both the dealer and the agents) to possess full quantum capabilities (e.g., quantum measurement, quantum states preparation, and so on) while in general quantum resources are valuable and quantum operations are not easy to implement.

In 2007, Boyer *et al.*[16] first presented the notion of semi-quantum by presenting a protocol where one participant (Bob) is classical. In the definition of semi-quantum, two kinds of participants, quantum participant and classical participant are proposed. The quantum participant has full quantum capabilities and can perform all quantum operations while a classical participant can only perform the following operations when he accesses a segment of quantum channel: (a) generating qubits in the fixed computational basis (Z basis) $\{|0\rangle, |1\rangle\}$; (b) measuring qubits in the fixed Z basis $\{|0\rangle, |1\rangle\}$; (c) reflecting qubits without disturbance; (d) reordering qubits (via different delay lines). Since semi-quantum cryptography protocol only requires one participant to have the full quantum capability, it simplifies the execution difficulty of the protocols and has been widely applied to various quantum cryptography fields, such as semi-quantum key distribution,[17–19] semi-quantum secure direct communication,[20–22] semi-quantum private comparison[23–25] and semi-quantum secret sharing.[26–32]

In 2010, Li *et al.*[26] proposed the first semi-quantum secret sharing (SQSS) protocol using the maximally entangled GHZ states. Two years later, Wang *et al.*[27] considered an SQSS protocol using the two-particle entangled states. In 2013, Li *et al.*[28] utilized easier two-particle product states to implement an SQSS protocol. After that, Xie *et al.*[29] designed a new SQSS protocol with GHZ-like states, which can share a specific bit string compared with the previous protocols. In 2018, Li *et al.*[30] proposed an SQSS protocol where classical participants can realize secret sharing without making any measurements and quantum Alice does not need quantum registers, which improves the relative efficiency. In the same year, Ye *et al.*[31] proposed two circular SQSS protocols using single particles where the second one releases the classical parties from the measurement capability. A more practical and flexible SQSS protocol based on the Bell states was proposed by Tian *et al.*[32] in 2021, which can share specific secrets with classical parties. However, inefficiency is still a major problem of SQSS protocols.

In this paper, an SQSS protocol based on single particles is presented. An encoding method is used to make quantum

†Corresponding author. E-mail: dou@bupt.edu.cn

© 2023 Chinese Physical Society and IOP Publishing Ltd

Alice has the right to decide the shared secret message. After this, we use particle reordering to maximally utilize particles while ensuring security, so that there is no particle discarded or wasted in our protocol, improving the efficiency to nearly 100%. The resources used in the proposed protocol are simple single particles and are prepared only by the quantum party, reducing the difficulty of the resource preparation. Besides, the particles in our protocol are transmitted in a circular way, which makes the role of the agents equal, so this protocol is easy to be extended to multi-party secret sharing. And then, we analyze the security of the protocol to prove that our protocol is secure and can resist common attacks, such as intercept-resend attack and measure-resend attack.

The remaining parts of the paper are organized as follows. In Section 2, a novel SQSS protocol is described in detail. Next, the security analysis is in Section 3 while the comparison of the SQSS protocol with previous protocols is analyzed in Section 4. In Section 5, a conclusion is given.

2. The proposed SQSS protocol

In this section, we first present an encoding method. Secondly, we propose a three-party SQSS protocol based on single particles. Then, such SQSS protocol is generalized to the multiparty case. After that, we use an example to show the process of the protocol in detail.

2.1. Encoding method

To encode any integer as a bit string with equal numbers of 0 and 1, we try to present an encoding method, which can be applied in the protocol proposed thereafter.

First, let us look at the properties of this bit string. If a bit string has N 0 and N 1, it can express C_{2N}^{N} integers. From the combined number formula $C_{2N}^{N} = C_{2N-1}^{N-1} + C_{2N-1}^{N}$, we can derive a recursive formula $C_{2N}^{N} = C_{2N-1}^{N-1} + C_{2N-2}^{N-1} + \cdots + C_{N-1}^{N-1}$.

Inspired by this, based on the location where the first 1 appears, a $2N$-bit string can be divided into $N+1$ groups. If the first 1 appears in the i-th position, the remaining $N-1$ 1 can only appear in the later $2N-i$ position, so this group has C_{2N-i}^{N-1} combinations. Then every group can be further divided into sub-groups based on the location where the next 1 appears and so on. Once the N-th 1 is located, all 1 are well positioned and the remaining positions will be filled with 0. According to this idea, we can propose an encoding method which is suitable for any number N.

An integer x within the range of $\left[1, C_{2N}^{N}\right]$ can be expressed as $x = C_{2N}^{N} - b_1 - b_2 - \cdots - b_N$, where

$$b_i = \begin{cases} 0, & P_{i-1} = x, \\ \max\left\{C_{a_i}^{N-i+1} \left| P_{i-1} - C_{a_i}^{N-i+1} \geq x \right.\right\}, & P_{i-1} \neq x, \end{cases} \tag{1}$$

$1 \leq i \leq N$, $a_i \in N^+$. The a_i is a parameter to build parameter b_i and indicates encoding positions. The P_i is an intermediate value

$$P_0 = C_{2N}^{N}, \ \ P_i = P_{i-1} - b_i. \tag{2}$$

If each $b_i \neq 0$, the positions from the first 1 to the N-th 1 will be $2N - a_1, 2N - a_2, \ldots, 2N - a_N$, or they will be $2N - a_1, 2N - a_2, \ldots, 2N - a_{k-1}, N + k, N + k + 1, \ldots, 2N$, $(k = \min\{i | b_i = 0\})$.

Table 1. Encoding method and encoded results for $N = 3$.

The location (in the i-th place) where the first 1 appears			The location (in the i-th place) where the second 1 appears			The location (in the i-th place) where the last 1 appears		The integer which will be encoded
i	The string determined by this location	Number of remaining combinations	i	The string determined by this location	Number of remaining combinations	i	The string determined by this location	
1	1	C_5^2	2	1	C_4^1	3	111000	1
						4	110100	2
						5	110010	3
						6	110001	4
			3	01	C_3^1	4	101100	5
						5	101010	6
						6	101001	7
			4	001	C_2^1	5	100110	8
						6	100101	9
			5	0001	C_1^1	6	100011	10
2	01	C_4^2	3	1	C_3^1	4	011100	11
						5	011010	12
						6	011001	13
			4	01	C_2^1	5	010110	14
						6	010101	15
			5	001	C_1^1	6	010011	16
3	001	C_3^2	4	1	C_2^1	5	001110	17
						6	001101	18
			5	01	C_1^1	6	001011	19
4	0001	C_2^2	5	1	C_1^1	6	000111	20

Here take $N = 3$ for example, following the rule, the 6-bit string can express $C_6^3 = 20$ integers and there will be three 1 in the string. The integer 8 can be expressed as $8 = C_6^3 - C_5^3 - C_2^2 - C_1^1$, so $b_1 = C_5^3,\ b_2 = C_2^2,\ b_3 = C_1^1,\ a_1 = 5,\ a_2 = 2,\ a_3 = 1$, integer 8 can be encoded into 100110. The integer 16 can be seen as $16 = C_6^3 - C_4^3 - 0 - 0$ with $b_1 = C_4^3,\ b_2 = 0,\ b_3 = 0,\ a_1 = 4,\ k = 2$, so it can be encoded into 010011. Based on the locations where the three 1 appear, we can encode the integer 1–20 and write out all the encoded results in Table 1.

2.2. Three-party SQSS protocol

Suppose Alice has quantum capabilities while the others two participants Bob and Charlie are classical. Alice wants to share a secret with Bob and Charlie securely. The proposed three-party SQSS protocol is composed of the following steps.

Step 1 Alice decides the content of the shared secret at will and encodes the secret into a bit string with equal numbers of 0 and 1 by using the encoding method in Subsection 2.1. Suppose the length of this bit string is $2a$.

Step 2 Alice first randomly selects one basis from Z basis $\{|0\rangle, |1\rangle\}$ and X basis $\{|+\rangle, |-\rangle\}$. Using the particles $|0\rangle$ and $|+\rangle$ to stand for the classical bit and particles $|1\rangle$ and $|-\rangle$ to stand for the classical bit 1, based on the encoded string, Alice prepares all $2a$ single particles from the selected one basis. After that, Alice reorders these particles. Note that the rearrangement order of particles is only known to Alice.

Step 3 Alice prepares m decoy photons, each of which is randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, inserts decoy photons to the reordered particles in random positions, and sends them to Bob.

Step 4 After confirming that Bob has received the particles, Alice publishes the insertion positions of a fraction of decoy photons. Before she publishes the states of these decoy photons, Bob must measure those photons in Z basis. For those photons in $|0\rangle$ or $|1\rangle$, Bob checks the error rate, and for those in $|+\rangle$ or $|-\rangle$, Bob checks whether the measurements are evenly distributed. He aborts the protocol if the error or deviation rate exceeds a preset threshold. After the check, he disturbs the order of the remaining particles. Only Bob himself knows the rearrangement order of them. Finally, Bob sends all particles to Charlie.

Step 5 After Charlie announces the receipt of all particles from Bob, Alice publishes the insertion positions of another fraction of decoy photons. Then Bob publishes the transposition order of those photons, so Charlie can accurately measure those decoy photons in Z basis. She checks the measurements just like Bob based on the states published by Alice. After that, she does not need to do anything else but reorder the remaining particles secretly and send them back to Alice.

Step 6 After receiving particles from Charlie, Alice publishes the original positions of the rest of decoy photons. Bob and Charlie publish in turn their transposition order of these photons so Alice could get the final positions of the decoy photons in the existing particle sequence. Alice performs measurements in the corresponding basis of the decoy photons at these positions. By comparing the measurement results to the originally prepared photon states, Alice can calculate an error rate. If the error rate exceeds a preset threshold, they will abort this communication and restart the protocol. Otherwise, they continue to the next step.

Step 7 Alice measures all the remaining particles with the basis selected in step 2 and publishes the measurement results, that is, the encoded string that has been reordered by Alice, Bob, and Charlie. After that, Alice announces her rearrangement order. Only Bob and Charlie have cooperated, can they recover the original encoded string by sharing their own rearrangement order. Finally, they can get Alice's secret by decoding the encoded string.

2.3. Multi-party SQSS protocol

The three-party SQSS protocol is easily generalized to multi-party SQSS protocol.

Steps 1–5 are roughly the same as our three-party SQSS protocol, but at the end of step 5, Charlie sends the particles to the next classical participant, David, instead of Alice.

Step 6 After David announces the receipt of all particles, Alice publishes the insertion positions of a fraction of decoy photons and previous classical participants publish their transposition order of those decoy photons. Subsequently, David measures decoy photons and checks the measurements just like the Bob in step 4 based on the states published by Alice. After the check, he disturbs the order of remaining particles and sends the particles to the next classical participant. The remaining participants also operate as above, except that the last participant Zach sends the particles back to Alice.

Step 7 After receiving particles from Zach, Alice could get the final positions of the decoy photons with the help of all classical participants. The same as in step 6 in Subsection 2.2, Alice can make the corresponding measurements and calculate an error rate to detect eavesdropping.

Step 8 Alice publishes her rearrangement order and the measurement results of all the remaining particles measured in the basis selected in step 2. Classical participants can recover the encoded string only by cooperating. Finally, they can decode the encoded string to get Alice's secret.

The proposed multi-party SQSS protocol is implemented as above.

2.4. Example

Now, an example of our proposed SQSS protocol will be given in this part.

Suppose Alice wants to share an integer 40 which can be encoded into 01101100. She first selects the Z basis to prepare the sequence of $\{|0\rangle, |1\rangle, |1\rangle, |0\rangle, |1\rangle, |1\rangle, |0\rangle, |0\rangle\}$ and reorders it to $\{|1\rangle, |1\rangle, |0\rangle, |0\rangle, |1\rangle, |0\rangle, |1\rangle, |0\rangle\}$ by the order

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 7 & 3 & 2 & 1 & 8 & 4 \end{pmatrix}$. After being inserted decoy photons (in positions 3, 6, 9, 12, 13, 14), the sequence of particles turns into $\{|1\rangle_1, |1\rangle_2, |+\rangle_3, |0\rangle_4, |0\rangle_5, |0\rangle_6, |1\rangle_7, |0\rangle_8, |1\rangle_9, |1\rangle_{10}, |0\rangle_{11}, |-\rangle_{12}, |0\rangle_{13}, |1\rangle_{14}\}$. Alice then sends these particles to Bob.

After measuring and checking the particle $|1\rangle_{14}$ based on the information Alice published, Bob changes the order into $\{|-\rangle_{12},|0\rangle_{11},|1\rangle_{10},|1\rangle_9,|0\rangle_8,|1\rangle_7,|0\rangle_6,|0\rangle_5,|0\rangle_4, |+\rangle_3, |1\rangle_2,|1\rangle_1, |0\rangle_{13}\}$ by the order $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 13 \end{pmatrix}$ and sends it to Charlie.

Alice announces that the original position of the decoy photon for this detection is the 13-th position, while Bob publishes his rearrangement order of this photon as $13 \to 13$. After measuring and checking the particle $|0\rangle_{13}$ based on these information, Charlie reorders it again into $\{|0\rangle_4, |0\rangle_8, |0\rangle_{11}, |+\rangle_3, |1\rangle_9, |-\rangle_{12}, |1\rangle_1, |0\rangle_6, |1\rangle_{10}, |0\rangle_5, |1\rangle_2, |1\rangle_7\}$ by the order $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 3 & 9 & 5 & 2 & 12 & 8 & 10 & 1 & 4 & 11 & 7 \end{pmatrix}$ and sends it back to Alice.

Alice first announces the original position of the decoy photons $(3,6,9,12)$, Bob and Charlie then publish their transposition order of photons at the corresponding locations $(3 \to 10,\ 6 \to 7,\ 9 \to 4,\ 12 \to 1)$ and $(10 \to 4,\ 7 \to 8,\ 4 \to 5,\ 1 \to 6)$. So, Alice uses Z basis measurements for positions 8 and 5 and uses X basis to measure particles in positions 4 and 6. If there is no eavesdropping, then the measurement result should be $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. After the eavesdropping detection passes, Alice measures the remaining particles using Z basis, and publishes the results 00011011 and the initial rearrangement order $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 7 & 3 & 2 & 1 & 8 & 4 \end{pmatrix}$. By sharing their own rearrangement order, Bob and Charlie can get the encoded 01101100. By decoding the encoded string, they can get the shared integer 40.

3. Security analysis

In general, in the QSS protocol, internal attackers are more powerful than external eavesdroppers because they know more information about the secret. Therefore, we will focus on the security of the proposed SQSS protocol for dishonest internal participants below.

3.1. Intercept-resend attack

If Bob is a dishonest internal attacker, to obtain Alice's shared secret, Bob can try to launch an intercept-resend attack as follows: he uses Alice's particles as usual to perform the step 4. Then, he prepares a string of fake single particles and sends it to Charlie. After Charlie finishes his operation, Bob intercepts the particles that Charlie sends to Alice. By measuring this string of particles, Bob tries to obtain Charlie's rearrangement order of the particles.

However, Bob cannot determine the transposition order for particles in the same state $|0\rangle$ or $|1\rangle$. For example, if the sequence $\{|0\rangle, |1\rangle, |1\rangle, |0\rangle\}$ is reordered to $\{|0\rangle, |1\rangle, |0\rangle, |1\rangle\}$, the $|1\rangle$ on the second position may be unchanged or may be reordered to the fourth position. Consequently, Bob can not get exactly how Charlie disturbs the particles. Even if Bob can get Charlie's rearrangement order, since he does not know the positions and states of decoy photons when he sends the fake particle sequence, his attack will introduce errors when Alice and Charlie detect eavesdropping.

Therefore, Bob can obtain almost no information by launching intercept-resend attack without being detected. As a result, the intercept-resend attack fails.

3.2. Measure-resend attack

Without loss of generality, supposing Bob is a dishonest internal attacker, to obtain Alice's shared secret, he can take two strategies below to perform measure-resend attack.

(i) Bob intercepts the string of particles transmitted from Alice and measures all particles using the same basis (Z or X basis). Based on the measurements, Bob generates a new quantum sequence with the same measurement results and resends it to Charlie. If Bob's attack is not detected, Bob has a $1/2$ chance of choosing the right basis Alice selects and obtaining access to the secrets Alice wants to share. However, his attack will introduce errors and be detected before he obtains any useful information. Suppose Charlie checks μ decoy photons in Z basis and Alice measures η decoy photons. If Bob chooses to measure all particles in Z basis, the probability that Bob will not be detected is $(1/2)^{\eta/2}$, and if Bob chooses to measure all particles in X basis, the probability that Bob will not be detected is $(1/2)^{(\eta/2)+\mu}$. Therefore, the average probability that the attack will not be detected is $1-(1/2)^{(\eta/2)+1} \times \left[1+(1/2)^{\mu}\right]$, and when η is large enough, Bob's attack cannot be successfully implemented.

(ii) Bob intercepts the particles sent to Alice and measures all particles using the same basis (Z or X basis). As the rearrangement order of the particles is only known by the operator himself, Bob cannot accurately obtain Alice's shared secret without the help of Charlie, and this operation will be detected by eavesdropping detection.

Stated thus, the proposed protocol is secure against measure-resend attack.

3.3. Entanglement-measure attack

Suppose a malicious internal attacker Bob attempts to steal the secret shared by Alice through the entangle-measure attack. As this protocol only uses decoy photons to detect eavesdropping, we only consider the effect on decoy photons for entangle-measure attacks. The entangle-measure attack from Bob can be described as follows: the unitary operations U_{F} attacking particles as they go from Bob to Charlie and the unitary operations U_{R} attacking particles as they go back from

Charlie to Alice, where $U_{\rm F}$ and $U_{\rm R}$ share a common probe space with the state $|\varepsilon\rangle$.

Theorem 1 For the entangle-measure attack $(U_{\rm F}, U_{\rm R})$ performed by Bob inducing no error in eavesdropping detection, the final state of Bob's probe should be independent of Alice's measurement result. As a result, Bob gets no information on Alice's shared secret.

Proof After Bob has performed $U_{\rm F}$, the following relations should be established:

$$U_{\rm F}(|0\rangle|\varepsilon\rangle) = |0\rangle|\varepsilon_{00}\rangle + |1\rangle|\varepsilon_{01}\rangle, \tag{3}$$

$$U_{\rm F}(|1\rangle|\varepsilon\rangle) = |0\rangle|\varepsilon_{10}\rangle + |1\rangle|\varepsilon_{11}\rangle, \tag{4}$$

$$\begin{aligned} U_{\rm F}(|+\rangle|\varepsilon\rangle) = {} & \frac{1}{\sqrt{2}}(|0\rangle|\varepsilon_{00}\rangle + |1\rangle|\varepsilon_{01}\rangle) \\ & + \frac{1}{\sqrt{2}}(|0\rangle|\varepsilon_{10}\rangle + |1\rangle|\varepsilon_{11}\rangle), \end{aligned} \tag{5}$$

$$\begin{aligned} U_{\rm F}(|-\rangle|\varepsilon\rangle) = {} & \frac{1}{\sqrt{2}}(|0\rangle|\varepsilon_{00}\rangle + |1\rangle|\varepsilon_{01}\rangle) \\ & - \frac{1}{\sqrt{2}}(|0\rangle|\varepsilon_{10}\rangle + |1\rangle|\varepsilon_{11}\rangle), \end{aligned} \tag{6}$$

where $|\varepsilon_{00}\rangle$, $|\varepsilon_{01}\rangle$, $|\varepsilon_{10}\rangle$ and $|\varepsilon_{11}\rangle$ represent the un-normalized states of Bob's probe.

For particles of any order, Bob needs the final state of the first register to be the same as the original state to pass the eavesdropping detection, so $U_{\rm R}$ must satisfy the following conditions:

$$U_{\rm R}(U_{\rm F}(|0\rangle|\varepsilon\rangle)) = U_{\rm R}(|0\rangle|\varepsilon_{00}\rangle + |1\rangle|\varepsilon_{01}\rangle) = |0\rangle|F_0\rangle, \tag{7}$$

$$U_{\rm R}(U_{\rm F}(|1\rangle|\varepsilon\rangle)) = U_{\rm R}(|0\rangle|\varepsilon_{10}\rangle + |1\rangle|\varepsilon_{11}\rangle) = |1\rangle|F_1\rangle, \tag{8}$$

$$\begin{aligned} & U_{\rm R}(U_{\rm F}(|+\rangle|\varepsilon\rangle)) \\ = {} & \frac{1}{\sqrt{2}}U_{\rm R}(|0\rangle|\varepsilon_{00}\rangle + |0\rangle|\varepsilon_{10}\rangle + |1\rangle|\varepsilon_{01}\rangle + |1\rangle|\varepsilon_{11}\rangle) \\ = {} & \frac{1}{\sqrt{2}}(|0\rangle|F_0\rangle + |1\rangle|F_1\rangle) \\ = {} & \frac{1}{2}[|+\rangle(|F_0\rangle + |F_1\rangle) + |-\rangle(|F_0\rangle - |F_1\rangle)] \\ = {} & \frac{1}{2}(|+\rangle(|F_0\rangle + |F_1\rangle)), \end{aligned} \tag{9}$$

$$\begin{aligned} & U_{\rm R}(U_{\rm F}(|-\rangle|\varepsilon\rangle)) \\ = {} & \frac{1}{\sqrt{2}}U_{\rm R}(|0\rangle|\varepsilon_{00}\rangle - |0\rangle|\varepsilon_{10}\rangle + |1\rangle|\varepsilon_{01}\rangle - |1\rangle|\varepsilon_{11}\rangle) \\ = {} & \frac{1}{\sqrt{2}}(|0\rangle|F_0\rangle - |1\rangle|F_1\rangle) \\ = {} & \frac{1}{2}[|+\rangle(|F_0\rangle - |F_1\rangle) + |-\rangle(|F_0\rangle + |F_1\rangle)] \\ = {} & \frac{1}{2}(|-\rangle(|F_0\rangle + |F_1\rangle)). \end{aligned} \tag{10}$$

From the equations above, it should hold that

$$|F_0\rangle = |F_1\rangle = |F\rangle. \tag{11}$$

After inserting Eq. (11) into Eqs. (7)–(10), we have

$$\begin{cases} U_{\rm R}(U_{\rm F}(|0\rangle|\varepsilon\rangle)) = |0\rangle|F\rangle, \\ U_{\rm R}(U_{\rm F}(|1\rangle|\varepsilon\rangle)) = |1\rangle|F\rangle, \\ U_{\rm R}(U_{\rm F}(|+\rangle|\varepsilon\rangle)) = |+\rangle|F\rangle, \\ U_{\rm R}(U_{\rm F}(|-\rangle|\varepsilon\rangle)) = |-\rangle|F\rangle. \end{cases} \tag{12}$$

According to Eq. (12), if Bob is not detectable in the security check, he can not distinguish his final probe states. As a result, Bob gets no information on Alice's shared secret QED.

3.4. Trojan horse attack

Here, Bob plans to use Trojan horse attack. After finishing his normal operation, he attaches the invisible photons or the spy photons to his particles and transmits all of them to Charlie for Trojan horse attack.[33] By analyzing spy photons in this string of particles sent to Alice by Charlie, Bob tries to obtain Charlie's order of the particles. Nevertheless, by applying a photon number splitter (PNS) and a wavelength filter device (WF), the malicious operations can be easily resisted.[34] Hence, the presented protocol is secure against Trojan horse attack.

3.5. Collusion attack

In collusion attack, some participants can collude together to get the shadow of the share of other participants.

In our protocol, to facilitate the description, we denote the classical participants of the $(n+1)$-party protocol as $P_1, P_2, \ldots, P_n$. Suppose participants P_{j-1} and P_{j+1} try to perform the protocol dishonestly to get the P_j's rearrangement order. Since particle reordering is an independent operation and the rearrangement order is known only to P_j himself, two dishonest participants can attack no more than the previous dishonest Bob did alone, they can not get this order by colluding together to perform attacks.

Moreover, even $(n-1)$ dishonest participants collude together, they do not know the positions and states of decoy photons before P_j receives particles, which means they are unable to escape P_j's eavesdropping detection by publishing fake transposition order of decoy photons. As a consequence, their collusion attack will introduce errors and the protocol will be aborted, so Alice's secrets will not be leaked.

Therefore, our protocol is secure against collusion attack.

4. Comparison

We analyze and compare the performance of the proposed protocol with existing SQSS protocols. Our protocol makes progress in the following three aspects: simplifying the quantum resources, improving the protocol efficiency, and transmitting specific secrets. In Table 2, we make a more detailed comparison with the typical SQSS protocols in Refs. [26,28,31,32].

Here, b represents the net number of secret information bits and c represents the amount of information that all particles used actually can express. According to the above definition, the b/c of our proposed protocol should be $\log_2 C_{2N}^{N}/\log_2 2^{2N} = \log_2\left(2N!/(N!)^2\right)/2N$. By Stirling's formula, it can be derived that b/c is $\left(2N - \log_2\sqrt{\pi N}\right)/2N$. Thus, the qubit efficiency is $2N/2N - o(2N)$ which approaches to 1 when the length of message $2N$ increases.

As shown in Table 2, our protocol is based on single particles rather than entangled states or product states, reducing the difficulty of resource preparation. Moreover, we can see that the qubit efficiency of the proposed protocol is higher than all of the compared protocols, because it can approach 100% as N increases (the decoy photons are ignored). Lastly, in most previous protocols, the shared secret is not specific, whereas in our protocol Alice can decide which secret message to share.

Table 2. Comparisons of the SQSS protocols.

Protocol	Quantum resource	Qubit efficiency (b/c)	Sharing secret
The protocol of Ref. [26]	GHZ state	0.125	unspecific
The protocol of Ref. [28]	product state	0.25	unspecific
The protocol B of Ref. [31]	single particles	0.333	unspecific
The protocol of Ref. [32]	Bell state	0.5	specific
Proposed protocol	single particles	~ 1	specific

Through the above comparison, the proposed protocol is more efficient and practical than existing ones.

5. Conclusion

We have presented a more efficient and practical SQSS protocol. The efficiency of protocol could approach 100% as the length of message increases. Our protocol is based on single particles, reducing the difficulty of resource preparation. In addition, the shared secret message can be determined by Alice herself which cannot be realized by some previous protocols. Finally, we analyze the security of the proposed protocol and fully prove that our protocol can resist common attacks. High efficiency is a big advantage of our protocol, and we will explore how to improve the efficiency of protocols in other semi-quantum cryptography fields in future work.

Acknowledgments

Project supported by the National Key Research and Development Program of China (Grant No. 2020YFB1805405), the 111 Project (Grant No. B21049), the National Natural Science Foundation of China (Grant No. 62272051), the Foundation of Guizhou Provincial Key Laboratory of Public Big Data (Grant No. 2019BDKFJJ014), and the Fundamental Research Funds for the Central Universities of China (Grant Nos. 2019XD-A02 and 2020RC38).

References

[1] Shamir A 1979 *Commun. ACM* **22** 612
[2] Blakley G R 1979 1979 *International Workshop on Managing Requirements Knowledge*, June 4–7, 1979, New York, USA, p. 313
[3] Brickell E F 1990 *Workshop on the Theory and Application of Cryptographic Techniques*, April 10–13, 1989, Houthalen, Belgium, p. 468
[4] Brickell E F and Davenport D M 1991 *J. Cryptol.* **4** 123
[5] Chuang I L and Yamamoto Y 1995 *Phys. Rev. A* **52** 3489
[6] Plenio M B and Knight P L 1996 *Phys. Rev. A* **53** 2986
[7] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[8] Gottesman D 2000 *Phys. Rev. A* **61** 042311
[9] Guo G P and Guo G C 2003 *Phys. Lett. A* **310** 247
[10] Xiao L, Long G L, Deng F G and Pan J W 2004 *Phys. Rev. A* **69** 052307
[11] Hsieh C R and Tzonelih H 2010 *Commun. Theor. Phys.* **54** 1019
[12] Liu Z H, Chen H W, Xu J, Liu W J and Li Z Q 2012 *Quantum Inf. Process.* **11** 1785
[13] Wang M M, Wang W, Chen J G and Farouk A 2015 *Quantum Inf. Process.* **14** 4211
[14] Qin H, Zhu X and Dai Y 2015 *Quantum Inf. Process.* **14** 2997
[15] Grice W P and Qi B 2019 *Phys. Rev. A* **100** 022339
[16] Boyer M, Kenigsberg D and Mor T 2007 2007 *First International Conference on Quantum, Nano, and Micro Technologies*, January 2–6, 2007, Guadeloupe, French Caribbean, p. 10
[17] Boyer M, Gelles R, Kenigsberg D and Mor T 2009 *Phys. Rev. A* **79** 032341
[18] Zou X, Qiu D, Li L, Wu L and Li L 2009 *Phys. Rev. A* **79** 052312
[19] Wang M M, Gong L M and Shao L H 2019 *Quantum Inf. Process.* **18** 260
[20] Shukla C, Thapliyal K and Pathak A 2017 *Quantum Inf. Process.* **16** 295
[21] Zou X F and Qiu D W 2014 *Sci. China Phys. Mech.* **57** 1696
[22] Yang C W and Tsai C W 2020 *Quantum Inf. Process.* **19** 126
[23] Lin P H, Hwang T and Tsai C W 2019 *Quantum Inf. Process.* **18** 207
[24] Jiang L Z 2020 *Quantum Inf. Process.* **19** 180
[25] Ye C Q, Li J, Chen X B and Tian Y 2021 *Quantum Inf. Process.* **20** 262
[26] Li Q, Chan W H and Long D Y 2010 *Phys. Rev. A* **82** 022303
[27] Wang J, Zhang S, Zhang Q and Tang C J 2012 *Int. J. Quantum Inf.* **10** 1250050
[28] Li L, Qiu D and Mateus P 2013 *J. Phys. A Math. Theor.* **46** 045304
[29] Xie C, Li L and Qiu D 2015 *Int. J. Theor. Phys.* **54** 3819
[30] Li Z, Li Q, Liu C, Peng Y, Chan W H and Li L 2018 *Quantum Inf. Process.* **17** 285
[31] Ye C Q and Ye T Y 2018 *Commun. Theor. Phys.* **70** 661
[32] Tian Y, Li J, Chen X B, Ye C Q and Li H J 2021 *Quantum Inf. Process.* **20** 217
[33] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 *Phys. Rev. A* **73** 022320
[34] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev. A* **72** 044302