entropy

MDPI

Article

A Semi-Quantum Secret-Sharing Protocol with a High Channel Capacity

Yuan Tian [1,*], Genqing Bian [1], Jinyong Chang [1], Ying Tang [1], Jian Li [2] and Chongqiang Ye [2]

[1] College of Information and Control Engineering, Xi'an University of Architecture and Technology, Xi'an 710055, China
[2] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
* Correspondence: tinyuen@xauat.edu.cn; Tel.: +86-18810281508

Abstract: Semi-quantum cryptography communication stipulates that the quantum user has complete quantum capabilities, and the classical user has limited quantum capabilities, only being able to perform the following operations: (1) measuring and preparing qubits with a Z basis and (2) returning qubits without any processing. Secret sharing requires participants to work together to obtain complete secret information, which ensures the security of the secret information. In the semi-quantum secret sharing (SQSS) protocol, the quantum user Alice divides the secret information into two parts and gives them to two classical participants. Only when they cooperate can they obtain Alice's original secret information. The quantum states with multiple degrees of freedom (DoFs) are defined as hyper-entangled states. Based on the hyper-entangled single-photon states, an efficient SQSS protocol is proposed. The security analysis proves that the protocol can effectively resist well-known attacks. Compared with the existing protocols, this protocol uses hyper-entangled states to expand the channel capacity. The transmission efficiency is 100% higher than that of single-degree-of-freedom (DoF) single-photon states, providing an innovative scheme for the design of the SQSS protocol in quantum communication networks. This research also provides a theoretical basis for the practical application of semi-quantum cryptography communication.

Keywords: quantum cryptography; semi-quantum secret sharing; hyper-entangled states; degree of freedom; eavesdropping detection

Citation: Tian, Y.; Bian, G.; Chang, J.; Tang, Y.; Li, J.; Ye, C. A Semi-Quantum Secret-Sharing Protocol with a High Channel Capacity. *Entropy* **2023**, *25*, 742. https://doi.org/10.3390/e25050742

Academic Editor: Giuliano Benenti

Received: 9 March 2023
Revised: 16 April 2023
Accepted: 25 April 2023
Published: 30 April 2023

1. Introduction

The core idea of secret sharing is that the secret holder appropriately divides a piece of complete secret information into several parts, leaving these parts of the secret information to different participants for safekeeping [1]. A single participant or part cannot obtain adequate secret information. Only when all participants cooperate can complete secret information be recovered. Secret sharing achieves decentralized management of secret information and plays a role in reducing the risk of eavesdropping and tolerating some attacks and errors [2]. Moreover, the secret sharing protocol is vital in practical applications such as key agreement, secure multi-party computing, and voting systems [3,4]. Based on the excellent characteristics of quantum mechanics, such as non-cloning, quantum cryptography theoretically provides a scheme for designing protocols with unconditional security [5,6]. It can also detect whether there is eavesdropping in the communication process. The concept of quantum cryptography was proposed in 1984 [7], when Bennett and Brassard designed the first quantum key distribution (QKD) protocol using non-orthogonal quantum states and the uncertainty principle. The protocol only needs to use a single particle state, which is easy to implement, and its security has been strictly proven. As a popular cryptography technology, quantum cryptography has received extensive attention and in-depth research [8–10]. The quantum secret sharing (QSS) protocol is an essential branch of the quantum cryptography protocol, which can be used to share confidential

information between multiple participants. In 1999, Hilllery et al. studied the QSS protocol based on the Greenberger–Horne–Zeiligner (GHZ) states for the first time [11] and proposed a protocol for sharing classical secret and quantum secret information. Later, many scholars joined the research of QSS [12–14].

However, people's research on quantum information technology is still in its infancy. Quantum communication, quantum computing, and other technologies are more complex and challenging to apply in current science and technology, work, and life [15,16]. Moreover, quantum devices have high prices and complex operations, and quantum state preparation, storage, and transmission are also extremely complex. The proposal of semi-quantum cryptography effectively alleviates the bottleneck in the development of quantum cryptography. This is relatively easier to realize while ensuring security. The semi-quantum key distribution (SQKD) protocol allows one party to have the full quantum capability, while the other party's quantum capability is limited to achieve secure communication between a quantum user and a "classical user" [17]. Semi-quantum cryptography has attracted the attention of many scholars and is one of the emerging research hotspots in quantum cryptography [18–26]. In semi-quantum cryptography, some users can only hold simple quantum devices, saving the high cost of purchasing quantum devices. Some users can prepare quantum states without the need to prepare quantum states or by only using the computational basis (Z basis), which reduces the complexity of preparing quantum states. Especially in case of equipment failure in the quantum cryptography communication process, users can choose to switch the quantum cryptography communication mode to a semi-quantum cryptography communication mode to ensure the completion of the whole communication process.

In 2010, using the concept of "semi-quantum", Li et al. proposed two SQSS protocols for the first time [27]. Subsequently, this attracted a large number of scholars to study SQSS. In 2013, Li et al. considered it difficult to prepare entangled states in practice and designed a more realistic SQSS protocol based on the product states [28]. Xie et al. used two entangled states to encode messages for SQSS [29] and realized the direct sharing of secret information in 2015. Based on the Bell states, efficient SQSS was proposed by Yin et al. in 2017 [30]. The next year, Li et al. proposed an SQSS protocol which enables the sharing of secret information without the participants making any measurement operations [31]. In 2019, Xiang et al. presented a new SQSS scheme based on multi-level quantum systems which can share a large amount of information of the third and fourth levels with the same security [32]. Tsai et al., based on the W state, proposed a three-party SQSS protocol [33]. In 2021, Tian et al. constructed a new SQSS protocol which can share specific secret information and is more efficient than similar protocols [34]. An SQSS protocol for high-dimensional quantum systems based on product states was proposed in the context of the qualifications of Hu et al. in 2022 [35]. It is easy to find that the existing SQSS protocols focus on using the characteristics of different qubits to design different protocols, and all SQSS protocol quantum carriers are only in one DoF. Therefore, this paper, based on hyper-entangled states, implements a new SQSS protocol for the first time: the transmission particles in polarization and spatial mode DoFs.

As a carrier of quantum information, photons can not only become entangled in a single DoF, such as polarization, path, or spatial mode, but also realize entanglement in multiple DoFs at the same time, which is called hyper-entanglement [36,37]. Compared with a single DoF, photons in multiple DoFs have many advantages: they can achieve more effective state measurements, build an asymmetric optical quantum network, improve the channel capacity of the quantum network, and also contribute to the physical realization of quantum purification and quantum computation. In recent years, research on hyper-entangled states has become a hot topic in the field of quantum information, and many significant advances have been made, such as the preparation of hyper-entangled states and multi-DoF teleportation based on hyper-entangled states.

In this paper, we employ the unique advantages of hyper-entangled states to construct a novel SQSS protocol based on hyper-entangled single-photon states. The hyper-entangled

state improves the communication capacity, and the amount of information that the proposed protocol can share in one communication process is twice that of the single-DoF protocols. In addition, we analyze three attack strategies—intercept-resend attack, measure-resend attack, and entangle-measure attack—and prove that the proposed protocol can effectively resist well-known attacks. Table 1 lists all explanations of acronyms and symbols used in the paper.

Table 1. Explanations of acronyms and symbols.

Case	Bob's Operation
QSS	Quantum secret sharing
SQSS	Semi-quantum secret sharing
DoF	Degree of freedom
DoFs	Degrees of freedom
QKD	Quantum key distribution
SQKD	Semi-quantum key distribution
SIFT	Measure and prepare the qubits with Z basis
CTRL	Reflect the qubits without disturbance
X_P(X_S)	X basis under polarization DoF (spatial mode DoF)
Z_P(Z_S)	Z basis under polarization DoF (spatial mode DoF)
K_A	Alice's secret bit
K_B	Bob's secret bit
K_C	Charlie's secret bit
η	Qubit efficency

The structure of this paper is as follows: Section 2 describes the proposed SQSS protocol, Section 3 analyzes the security of three attacks, and Section 4 discusses and concludes this paper.

2. Protocol

Generally, the N hyper-entangled single-photon states in polarization and spatial mode DoFs can be represented by

$$|\Pi\rangle_{PS} = |\delta_P\rangle_{AB\ldots Z} \otimes |\delta_S\rangle_{AB\ldots Z}, \tag{1}$$

where the subscript $AB\ldots Z$ denotes the N photons, P denotes the polarization DoF, and S denotes the spatial-mode DoF. There are two non-orthogonal measure bases in the polarization DoF: the basis $Z_P = \{|H\rangle, |V\rangle\}$ and $X_P = \{|R\rangle, |A\rangle\}$. Here, we have

$$|R\rangle_P = \frac{|H\rangle + |V\rangle}{\sqrt{2}}, \tag{2}$$

$$|A\rangle_P = \frac{|H\rangle - |V\rangle}{\sqrt{2}}, \tag{3}$$

where $|H\rangle$ and $|V\rangle$ indicate the horizontal and vertical polarizations. There are two non-orthogonal measure bases in the spatial mode DoF: the basis $Z_S = \{|x_1\rangle, |x_2\rangle\}$ and $X_S = \{|a\rangle, |b\rangle\}$. Here, we have

$$|a\rangle_S = \frac{|x_1\rangle + |x_2\rangle}{\sqrt{2}}, \tag{4}$$

$$|b\rangle_S = \frac{|x_1\rangle - |x_2\rangle}{\sqrt{2}}, \tag{5}$$

where $|x_1\rangle$ and $|x_2\rangle$ indicate the upper and the lower spatial modes, respectively.

There are N single photons in the polarization DoF, which can be described as

$$|\delta_P\rangle_{AB\ldots Z} = (\frac{|H\rangle \pm |V\rangle}{\sqrt{2}})_A(\frac{|H\rangle \pm |V\rangle}{\sqrt{2}})_B \ldots (\frac{|H\rangle \pm |V\rangle}{\sqrt{2}})_Z. \tag{6}$$

There are N single photons in the spatial mode DoF, which can be described as

$$|\delta_S\rangle_{AB\ldots Z} = (\frac{|x_1\rangle \pm |x_2\rangle}{\sqrt{2}})_A(\frac{|x_1\rangle \pm |x_2\rangle}{\sqrt{2}})_B \ldots (\frac{|x_1\rangle \pm |x_2\rangle}{\sqrt{2}})_Z. \tag{7}$$

We set $N = 2$, and the hyper-entangled single-photon states are

$$\begin{aligned} |\Gamma\rangle_{PS} &= |\gamma\rangle_P \otimes |\gamma\rangle_S \\ &= |R\rangle_P|R\rangle_P \otimes |a\rangle_S|a\rangle_S \\ &= \frac{|H\rangle + |V\rangle}{\sqrt{2}}\frac{|H\rangle + |V\rangle}{\sqrt{2}} \otimes \frac{|x_1\rangle + |x_2\rangle}{\sqrt{2}}\frac{|x_1\rangle + |x_2\rangle}{\sqrt{2}}. \end{aligned} \tag{8}$$

The three-party SQSS protocol based on hyper-entangled single-photon states is presented in detail. Alice, as the holder of the secret information, plans to share the secret with two classical participants: Bob and Charlie. Here, Alice is a quantum user who has full quantum capabilities. She can generate and measure qubits with any basis. Bob (Charlie) is a classical user whose quantum capabilities are restricted. He can only use the Z basis to generate and measure qubits. The processing of the proposed protocol is as follows:

Step 1: Carrier preparation and transmission. Alice generates n two-qubit product hyper-entangled states $|\Gamma\rangle_{PS}$:

$$\begin{aligned} |\Gamma\rangle_{PS} &= |\gamma\rangle_P^{BC} \otimes |\gamma\rangle_S^{BC} \\ &= |R\rangle_P^B|R\rangle_P^C \otimes |a\rangle_S^B|a\rangle_S^C \\ &= \frac{|H\rangle^B + |V\rangle^B}{\sqrt{2}}\frac{|H\rangle^C + |V\rangle^C}{\sqrt{2}} \otimes \frac{|x_1\rangle^B + |x_2\rangle^B}{\sqrt{2}}\frac{|x_1\rangle^C + |x_2\rangle^C}{\sqrt{2}}, \end{aligned} \tag{9}$$

where B and C denote the system of the two participants: Bob and Charlie, respectively. Alice forms a quantum sequence S using $|\Gamma\rangle_{PS}$:

$$\begin{aligned} S = \{&[|R\rangle_P \otimes |a\rangle_S(B), |R\rangle_P \otimes |a\rangle_S(C)]_1, [|R\rangle_P \otimes |a\rangle_S(B), |R\rangle_P \otimes |a\rangle_S(C)]_2, \\ &\ldots, [|R\rangle_P \otimes |a\rangle_S(B), |R\rangle_P \otimes |a\rangle_S(C)]_n\}. \end{aligned} \tag{10}$$

Then, Alice divides the sequence S into sequences S_B and S_C:

$$S_B = \{[|R\rangle_P \otimes |a\rangle_S(B)]_1, [|R\rangle_P \otimes |a\rangle_S(B)]_2, \ldots, [|R\rangle_P \otimes |a\rangle_S(B)]_n\}, \tag{11}$$

$$S_C = \{[|R\rangle_P \otimes |a\rangle_S(C)]_1, [|R\rangle_P \otimes |a\rangle_S(C)]_2, \ldots, [|R\rangle_P \otimes |a\rangle_S(C)]_n\}, \tag{12}$$

Alice then sends S_B to Bob and S_C to Charlie.

Step 2: Bob and Charlie's operations. When Bob (Charlie) receives the sequence S_B (S_C), Bob (Charlie) randomly chooses the SIFT or CTRL operation. The SIFT operation means the participant measures the qubits with the Z basis, prepares fresh qubits with the same measurements with the Z basis, and sends them to Alice. The CTRL operation means the participant reflects the qubits to Alice without disturbance.

Step 3: Alice, Bob, and Charlie's publication. For the last qubits arriving from Bob and Charlie, Alice broadcasts that the sequences S_B and S_C have been received. After acknowledgment, Bob and Charlie announce the certain operation, SIFT or CTRL, which has been chosen for each qubit.

Step 4: Alice's operations. According to Bob's (Charlie's) choice, Alice divides the corresponding qubits into the following four cases. The four cases as illustrated in Table 2

and depend on the different operations which Bob and Charlie performed. In case 1, Bob and Charlie chose SIFT, and Alice measured the qubits B and C with $Z_P \otimes Z_S$. In case 2, Bob chose SIFT and Charlie chose CTRL, while Alice measured the qubits B with $Z_P \otimes Z_S$ and the qubits C with $X_P \otimes X_S$. In case 3, Bob chose CTRL and Charlie chose SIFT, while Alice measured the qubits B with $X_P \otimes X_S$ and the qubits C with $Z_P \otimes Z_S$. In case 4, Bob and Charlie chose CTRL, and Alice measured the qubits B and C with $X_P \otimes X_S$. Case 1 was used for generating the raw keys and checking for eavesdropping, while cases 2, 3, and 4 were used for checking for eavesdropping.

Table 2. Participants' operations on the qubits in each position.

Case	Bob's Operation	Charlie's Operation	Alice's Operation	Usage
1	SIFT	SIFT	Measure the qubits B and C with $Z_P \otimes Z_S$	Generate raw key, check for eavesdropping
2	SIFT	CTRL	Measure the qubits B with $Z_P \otimes Z_S$ and measure the qubits C with $X_P \otimes X_S$	Check for eavesdropping
3	CTRL	SIFT	Measure the qubits B with $X_P \otimes X_S$ and Measure the qubits C with $Z_P \otimes Z_S$	Check for eavesdropping
4	CTRL	CTRL	Measure the qubits B and C with $X_P \otimes X_S$	Check for eavesdropping

Step 5: First eavesdropping detection. Alice conducted eavesdropping detection in cases 2, 3, abd 4. Alice measured the measured qubits with $Z_P \otimes Z_S$ and measured the reflected qubits with $X_P \otimes X_S$. For example, in case 2, Alice would measure the qubits C with $X_P \otimes X_S$, which were reflected by Charlie. If there was no eavesdropper, then the measurement results should be same as in the initial state which she prepared. Alice would measure the qubits B with $Z_P \otimes Z_S$, which were measured by Bob, and she would inform Bob to publish his measurement results. If there was no eavesdropper, then the measurement results should be the same between Alice and Bob. Similarly, Alice would have the same operations for eavesdropping as in case 3. In case 4, Alice would measure the qubits B and C with $X_P \otimes X_S$, and the measurement results should be same as the initial state which was prepared by her; otherwise, there was an eavesdropper present. If the error rate is higher than the predefined threshold values, then Alice terminates the protocol. The details of the security analysis will be provided in the next section.

Step 6: Second eavesdropping detection. Alice randomly selects a few qubits which belong to case 1 to be TEST bits and announces the states and corresponding positions. Bob and Charlie compare the states with their qubits. Alice and Bob (Charlie) should have the same measurement results. If the error rates exceed the threshold values, then the protocol aborts.

Step 7: Secret sharing. The remaining qubits in case 1 are INFO bits. Because of the hyper-entangled states in polarization and spatial mode DoFs, one participant's operations on one qubit position can share two keys. Secret information 1 and 2 are encoded by Alice as given in Table 3. K_A, K_B, and K_C are the results measured by Alice, Bob, and Charlie in case 1, respectively. Presume that K_A is the secret bits, and Alice encodes K_A as

$$K_A \equiv K_B \oplus K_C. \tag{13}$$

Only Bob and Charlie's colleagues can obtain the secret information.

Table 3. The shared secret information between two participants from Alice.

Secret Information 1 and 2	Bob's Results	Charlie's Results	Alice's Results
0 and 0	$\|0\rangle_P \otimes \|0\rangle_S$	$\|0\rangle_P \otimes \|0\rangle_S$	$\|00\rangle_P \otimes \|00\rangle_S$
0 and 1	$\|0\rangle_P \otimes \|0\rangle_S$	$\|0\rangle_P \otimes \|1\rangle_S$	$\|00\rangle_P \otimes \|01\rangle_S$
1 and 0	$\|0\rangle_P \otimes \|0\rangle_S$	$\|1\rangle_P \otimes \|0\rangle_S$	$\|01\rangle_P \otimes \|00\rangle_S$
1 and 1	$\|0\rangle_P \otimes \|0\rangle_S$	$\|1\rangle_P \otimes \|1\rangle_S$	$\|01\rangle_P \otimes \|01\rangle_S$
0 and 1	$\|0\rangle_P \otimes \|1\rangle_S$	$\|0\rangle_P \otimes \|0\rangle_S$	$\|00\rangle_P \otimes \|10\rangle_S$
0 and 0	$\|0\rangle_P \otimes \|1\rangle_S$	$\|0\rangle_P \otimes \|1\rangle_S$	$\|00\rangle_P \otimes \|11\rangle_S$
1 and 1	$\|0\rangle_P \otimes \|1\rangle_S$	$\|1\rangle_P \otimes \|0\rangle_S$	$\|01\rangle_P \otimes \|10\rangle_S$
1 and 0	$\|0\rangle_P \otimes \|1\rangle_S$	$\|1\rangle_P \otimes \|1\rangle_S$	$\|01\rangle_P \otimes \|11\rangle_S$
1 and 0	$\|1\rangle_P \otimes \|0\rangle_S$	$\|0\rangle_P \otimes \|0\rangle_S$	$\|10\rangle_P \otimes \|00\rangle_S$
1 and 1	$\|1\rangle_P \otimes \|0\rangle_S$	$\|0\rangle_P \otimes \|1\rangle_S$	$\|10\rangle_P \otimes \|01\rangle_S$
0 and 0	$\|1\rangle_P \otimes \|0\rangle_S$	$\|1\rangle_P \otimes \|0\rangle_S$	$\|11\rangle_P \otimes \|00\rangle_S$
0 and 1	$\|1\rangle_P \otimes \|0\rangle_S$	$\|1\rangle_P \otimes \|1\rangle_S$	$\|11\rangle_P \otimes \|01\rangle_S$
1 and 1	$\|1\rangle_P \otimes \|1\rangle_S$	$\|0\rangle_P \otimes \|0\rangle_S$	$\|10\rangle_P \otimes \|10\rangle_S$
1 and 0	$\|1\rangle_P \otimes \|1\rangle_S$	$\|0\rangle_P \otimes \|1\rangle_S$	$\|10\rangle_P \otimes \|11\rangle_S$
0 and 1	$\|1\rangle_P \otimes \|1\rangle_S$	$\|1\rangle_P \otimes \|0\rangle_S$	$\|11\rangle_P \otimes \|10\rangle_S$
0 and 0	$\|1\rangle_P \otimes \|1\rangle_S$	$\|1\rangle_P \otimes \|1\rangle_S$	$\|11\rangle_P \otimes \|11\rangle_S$

3. Security Analysis

Suppose that an eavesdropper wants to obtain Alice's secret information through illegal means. He will take specific means to eavesdrop on the participants' keys. Generally, when analyzing the security of the SQSS protocol, a dishonest participant (Bob or Charlie) causes more serious harm than external eavesdroppers because they have already obtained one part of the secret information and only need to steal the secret information of another participant. They can obtain Alice's secret information alone. Therefore, the security analysis of the proposed protocol mainly focuses on malicious participants. Assuming that Bob is a malicious participant, he uses the following attack strategies to steal Charlie's keys and finally obtains Alice's secret information.

Measure-resend attack. To obtain Charlie's secret keys, Bob uses the measure-resend attack strategy. When Alice sends S_C to Charlie, Bob first intercepts the sequence, measures the qubits using the $Z_P \otimes Z_S$ basis, and stores the measurement results. Then, Bob prepares a new sequence S_E with $Z_P \otimes Z_S$, which is the same state as the previous sequence measured by him. If Alice and Charlie do not detect Bob's attack, then Bob will obtain the corresponding Charlie secret keys according to his measurement results. Unfortunately, Bob's eavesdropping can be detected through eavesdropping detection in cases 2 and 4 under step 5 because Bob cannot distinguish which operation Charlie will choose for the specific qubits. When Bob measured $[|R\rangle_P \otimes |a\rangle_S(C)]_i$, where Charlie chose the SIFT operation on $[|R\rangle_P \otimes |a\rangle_S(C)]_i$, he could successfully obtain Charlie's secret keys and combine his secret keys to calculate Alice's secret information. Although such behavior will not introduce any errors, once Charlie selects the CTRL operation, Alice will have a chance of half to detect the errors introduced by Bob when performing eavesdropping detection. Specifically, with Alice using the $X_P \otimes X_S$ basis to measure the qubits prepared by Bob, the measurement results may occur as one of four results: $\{[|R\rangle_P \otimes |a\rangle_S(C)]_i, [|R\rangle_P \otimes |b\rangle_S(C)]_i, [|A\rangle_P \otimes |a\rangle_S(C)]_i$, and $[|A\rangle_P \otimes |b\rangle_S(C)]_i\}$. Thus, the error rate introduced by Bob can be calculated as $r_1 = \frac{1}{2} \times \frac{3}{4} = \frac{3}{8}$, and he can eavesdrop the probability of $\frac{5}{8}$. The detection probability for the presented SQSS protocol is $p_1 = 1 - (\frac{5}{8})^t$. If t is large enough, then the detection probability will be toward one.

Intercept-resend attack. Bob employs the intercept-resend attack strategy to steal Charlie's secret keys. First, Bob intercepts the sequence S_C and sends a fake sequence S'_E with $Z_P \otimes Z_S$ or $X_P \otimes X_S$ to Charlie. Then, Charlie sends back S''_E to Alice. Bob intercepts S''_E and sends S_C to Alice. Unfortunately, Bob will inevitably be detected. When Charlie chose the CTRL operation, there was no error introduced by Bob. However, there was a possibility of a half that Charlie chose the SIFT operation. In the case where Charlie chose SIFT, Bob would be detected in cases 1 and 3 under step 5. Specifically, Alice used

the $Z_P \otimes Z_S$ basis to measure the qubits returned by Bob. The measurement results may occur as one of four results: $\{[|x_1\rangle_P \otimes |x_1\rangle_S(C)]_i, [|x_1\rangle_P \otimes |x_2\rangle_S(C)]_i, [|x_2\rangle_P \otimes |x_1\rangle_S(C)]_i$, and $[|x_2\rangle_P \otimes |x_2\rangle_S(C)]_i\}$. Thus, the error rate introduced by Bob can be calculated as $r_2 = \frac{1}{2} \times \frac{3}{4} = \frac{3}{8}$. He can eavesdrop with a probability of $\frac{5}{8}$. When t is large enough, the detection probability of $p_2 = 1 - (\frac{5}{8})^t$ will approximately be one for the presented SQSS protocol.

Entangle-measure attack. Bob's most general attack is the measure-entangle attack, which is composed of two unitary operations: $\bar{U}_E$ attacking qubits when Alice sends information to Charlie and $\bar{U}_F$ attacking qubits when Charlie sends information to Alice.

Theorem 1. *Suppose that Bob uses an attack ($\bar{U}_E$,$\bar{U}_F$) on the qubits from Alice to Charlie and from Charlie back to Alice. Furthermore, the final probes should be independent of Charlie's measurement results to not induce any error. Hence, Bob cannot obtain any information on the secret keys.*

Proof. Before Bob's attack, the qubits are $|R\rangle_P \otimes |a\rangle_S$, and the ancillary qubit is $|e\rangle$. After $\bar{U}_E$, the state evolves into

$$\bar{U}_E(|R\rangle_P \otimes |a\rangle_S)|e\rangle = |Hx_1\rangle|e_{Hx_1}\rangle + |Hx_2\rangle|e_{Hx_2}\rangle + |Vx_1\rangle|e_{Vx_1}\rangle + |Vx_2\rangle|e_{Vx_2}\rangle, \quad (14)$$

where $|e_{Hx_1}\rangle$, $|e_{Hx_2}\rangle$, $|e_{Vx_1}\rangle$, and $|e_{Vx_2}\rangle$ are the unnormalized states of Eve's probes. □

When Charlie receives the qubits, he selects the SIFT operation or CTRL operation. Subsequently, Bob performs $\bar{U}_F$ on the state.

Charlie selects the SIFT operation. The global state is collapsed into one of four states: $|Hx_1\rangle|e_{Hx_1}\rangle$, $|Hx_2\rangle|e_{Hx_2}\rangle$, $|Vx_1\rangle|e_{Vx_1}\rangle$, and $|Vx_2\rangle|e_{Vx_2}\rangle$. If Bob wants no error to be introduced, then after $\bar{U}_F$, there are

$$\bar{U}_F(|Hx_1\rangle|e_{Hx_1}\rangle) = |Hx_1\rangle|f_{Hx_1}\rangle, \quad (15)$$

$$\bar{U}_F(|Hx_2\rangle|e_{Hx_2}\rangle) = |Hx_2\rangle|f_{Hx_2}\rangle, \quad (16)$$

$$\bar{U}_F(|Vx_1\rangle|e_{Vx_1}\rangle) = |Vx_1\rangle|f_{Vx_1}\rangle, \quad (17)$$

$$\bar{U}_F(|Vx_2\rangle|e_{Vx_2}\rangle) = |Vx_2\rangle|f_{Vx_2}\rangle. \quad (18)$$

Charlie selects the CTRL operation. The global state should be unchanged:

$$\begin{aligned} &\bar{U}_F(Hx_1\rangle|e_{Hx_1}\rangle + |Hx_2\rangle|e_{Hx_2}\rangle + |Vx_1\rangle|e_{Vx_1}\rangle + |Vx_2\rangle|e_{Vx_2}\rangle) \\ &= |Hx_1\rangle|f_{Hx_1}\rangle + |Hx_2\rangle|f_{Hx_2}\rangle + |Vx_1\rangle|f_{Vx_1}\rangle + |Vx_2\rangle|f_{Vx_2}\rangle, \end{aligned} \quad (19)$$

According to the protocol, if there is no error introduced, then from Equation (19), it must hold that

$$|f_{Hx_1}\rangle = |f_{Hx_2}\rangle = |f_{Vx_1}\rangle = |f_{Vx_2}\rangle = |f\rangle. \quad (20)$$

According to Equation (20), Equations (15)–(18) can be deduced:

$$\bar{U}_F(|Hx_1\rangle|e_{Hx_1}\rangle) = |Hx_1\rangle|f_{Hx_1}\rangle = |Hx_1\rangle|f\rangle, \quad (21)$$

$$\bar{U}_F(|Hx_2\rangle|e_{Hx_2}\rangle) = |Hx_2\rangle|f_{Hx_2}\rangle = |Hx_2\rangle|f\rangle, \quad (22)$$

$$\bar{U}_F(|Vx_1\rangle|e_{Vx_1}\rangle) = |Vx_1\rangle|f_{Vx_1}\rangle = |Vx_1\rangle|f\rangle, \quad (23)$$

$$\bar{U}_F(|Vx_2\rangle|e_{Vx_2}\rangle) = |Vx_2\rangle|f_{Vx_2}\rangle = |Vx_2\rangle|f\rangle. \quad (24)$$

To avoid introducing errors during Alice's eavesdropping detection, the final state of Bob's probes should be independent of Charlie's measurement results. Theorem 1 has been proven by the above methods.

4. Discussion and Conclusions

Now, we discuss the differences between our proposed protocol and the existing SQSS protocol. Obviously, compared with the previous SQSS protocol, the proposed protocol features the use of hyper-entangled states in two DoFs, which improves the communication capacity of the protocol. The qubit efficiency can be defined as $\eta = \frac{b}{q}$ [38], where b denotes the total number of shared classical bits and q denotes the total number of prepared qubits in the protocol. Specific comparisons are given in Table 4.

Table 4. SQSS protocol comparison.

Reference	Quantum Source	Measurement	Decoy Photons	DoF	Sharing Message	Qubit Effigency
[27]	GHZ-type states	Single qubit measurement, Bell measurement, three-qubit joint measurement	No	1	Unspecific	$\frac{1}{8}$
[28]	Two-qubit product states	Single qubit measurement	No	1	Unspecific	$\frac{1}{4}$
[29]	Two entangled states	Single qubit measurement, two-particle measurement, three-particle measurement	No	1	Specific	$\frac{1}{4}$
[30]	Bell states	Single qubit measurement, Bell measurement	No	1	Unspecific	-
[31]	Two-qubit product states	Single qubit measurement	No	1	Unspecific	$\frac{1}{4}$
[32]	Two-qubit product states	-	No	1	Unspecific	$\frac{1}{8}$
[33]	W states	Single qubit measurement, Bell measurement	No	1	Unspecific	$\frac{1}{8}$
[34]	Bell states	Single qubit measurement, Bell measurement	Yes	1	Specific	$<\frac{1}{2}$
[35]	Product states	Single qubit measurement	No	1	Unspecific	$\frac{1}{4}$
Proposed protocol	Two-qubit product hyper-entangled states	Single hyper-entangled qubit measurement	No	2	Unspecific	$\frac{1}{2}$

The application research on multi-DoF quantum information has just started. The multi-DoF approach may give people more colorful content which differs from manipulating a single DoF. In this paper, by using hyper-entangled states as quantum transmission carriers, we proposed a semi-quantum secret-sharing protocol with high efficiency which solves the problem of only the cooperation of different participants being able to recover the key. The analysis results show that the protocol can detect well-known attacks, such as an intercept-resend attack, measure-resend attack, and entangle-measure attack, and thus the security is asymptotically secure in theory. More in-depth security analysis is needed in practice. Applying hyper-entangled states in quantum communication can improve the channel capacity and communication security, serve practical quantum communication networks, and promote the practical process of semi-quantum cryptography communication.

Author Contributions: This article was completed by six authors. The first author, Y.T. (Yuan Tian), was mainly responsible for the conceptualization and methodology and writing—original draft and editing. The second author, G.B., was mainly responsible for validation and writing—review. The third author, J.C., was mainly responsible for the investigation and formal analysis. The fourth author, Y.T. (Ying Tang), was mainly responsible for verification. The fifth author, J.L., was mainly responsible for supervision and funding acquisition. The sixth author, C.Y., was mainly responsible for visualization. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded the National Natural Science Foundation of China, grant numbers 61872284, 61671087, and 61962009.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We would like to thank the anonymous reviewers for their detailed review and valuable comments, which have enhanced the quality of this paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
2. Chandramouli, A.; Choudhury, A.; Patra, A. A Survey on Perfectly Secure Verifiable Secret-Sharing. *ACM Comput. Surv. CSUR* **2022**, *54*, 1–36. [CrossRef]
3. Blanton, M.; Kang, A.; Yuan, C. Improved building blocks for secure multi-party computation based on secret sharing with honest majority. In Proceedings of the Applied Cryptography and Network Securit: 18th International Conference, ACNS 2020, Rome, Italy, 19–22 October 2020.
4. Liu, Y.; Zhao, Q. E-voting scheme using secret sharing and K-anonymity. *World Wide Web* **2019**, *22*, 1657–1667. [CrossRef]
5. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145. [CrossRef]
6. Portmann, C.; Renner, R. Security in quantum cryptography. *Rev. Mod. Phys.* **2022**, *94*, 025008. [CrossRef]
7. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 10–12 December 1984.
8. Lo, H.K.; Curty, M.; Tamaki, K. Secure quantum key distribution. *Nat. Photonics* **2016**, *8*, 595–604. [CrossRef]
9. Sun, Z.; Song, L.; Huang, Q.; Yin, L.; Long, G.; Lu, J.; Hanzo, L. Toward practical quantum secure direct communication: A quantum-memory-free protocol and code design. *IEEE Trans. Commun.* **2020**, *68*, 5778–5792. [CrossRef]
10. Basso Basset, F.; Valeri, M.; Roccia, E.; Muredda, V.; Poderini, D.; Neuwirth, J.; Spagnolo, N.; Rota, M.B.; Carvacho, G.; Sciarrino, F.; et al. Quantum key distribution with entangled photons generated on demand by a quantum dot. *Sci. Adv.* **2021**, *7*, eabe6379. [CrossRef]
11. Hillery, M.; Bužek, V. Berthiaume, Quantum secret sharing. *Phys. Rev. A* **1999**, *59*, 1829. [CrossRef]
12. Williams, B.P.; Lukens, J.M.; Peters, N.A.; Qi, B.; Grice, W.P. Quantum secret sharing with polarization-entangled photon pairs. *Phys. Rev. A* **2019**, *99*, 062311. [CrossRef]
13. Sutradhar, K.; Om, H. Efficient quantum secret sharing without a trusted player. *Quantum Inf. Process.* **2020**, *19*, 73. [CrossRef]
14. Liao, Q.; Liu, H.; Zhu, L.; Guo, Y. Quantum secret sharing using discretely modulated coherent states. *Phys. Rev. A* **2021**, *103*, 032410. [CrossRef]
15. Bennett, C.H.; Wiesner, S.J. Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.* **1992**, *69*, 2881. [CrossRef]
16. Cirac, J.I. Quantum computing and simulation: Where we stand and what awaits US. *Nanophotonics* **2020**, *10*, 453-456. [CrossRef]
17. Boyer, M.; Kenigsberg, D.; Mor, T. Quantum key distribution with classical Bob. In Proceedings of the 2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07), Guadeloupe, France, 2–6 January 2007.
18. Iqbal, H.; Krawec, W.O. Semi-quantum cryptography. *Quantum Inf. Process.* **2020**, *19*, 97. [CrossRef]
19. Tian, Y.; Li, J.; Yuan, K.; Li, C.; Li, H.; Chen, X. An efficient semi-quantum key distribution protocol based on EPR and single-particle hybridization. *Quantum Inf. Comput.* **2021**, *21*, 563–576. [CrossRef]
20. Tian, Y.; Li, J.; Ye, C.; Li, C. Multi-party semi-quantum key distribution protocol based on hyperentangled Bell states. *Front. Phys.* **2022**, *10*, 966. [CrossRef]
21. Guskind, J.; Krawec, W.O. Mediated semi-quantum key distribution with improved efficiency. *Quantum Sci. Technol.* **2022**, *7*, 035019. [CrossRef]
22. Jiang, L.Z. Semi-quantum private comparison based on Bell states. *Quantum Inf. Process.* **2020**, *19*, 180. [CrossRef]
23. Lin, P.H.; Hwang, T.; Tsai, C.W. Efficient semi-quantum private comparison using single photons. *Quantum Inf. Process.* **2019**, *18*, 207. [CrossRef]
24. Tian, Y.; Li, J.; Chen, X.B.; Ye, C.Q.; Li, C.Y.; Hou, Y.Y. An efficient semi-quantum private comparison without pre-shared keys. *Quantum Inf. Process.* **2021**, *20*, 360. [CrossRef]
25. Zhou, N.R.; Zhu, K.N.; Bi, W.; Gong, L.H. Semi-quantum identification. *Quantum Inf. Process.* **2019**, *18*, 197. [CrossRef]
26. Rong, Z.; Qiu, D.; Mateus, P.; Zou, X. Mediated semi-quantum secure direct communication. *Quantum Inf. Process.* **2021**, *20*, 58. [CrossRef]
27. Li, Q.; Chan, W.H.; Long, D.Y. Semi-quantum secret sharing using entangled states. *Phys. Rev. A* **2010**, *82*, 022303. [CrossRef]
28. Li, L.; Qiu, D.; Mateus, P. Quantum secret sharing with classical Bobs. *J. Phys. Math. Theor.* **2013**, *46*, 045304. [CrossRef]
29. Xie, C.; Li, L.; Qiu, D. A novel semi-quantum secret sharing scheme of specific bits. *Int. J. Theor. Phys.* **2015**, *54*, 3819–3824. [CrossRef]
30. Yin, A.; Wang, Z.; Fu, F. A novel semi-quantum secret sharing scheme based on Bell states. *Mod. Phys. Lett. B* **2017**, *31*, 1750150. [CrossRef]
31. Li, Z.; Li, Q.; Liu, C.; Peng, Y.; Chan, W.H.; Li, L. Limited resource semiquantum secret sharing. *Quantum Inf. Process.* **2018**, *17*, 285. [CrossRef]
32. Xiang, Y.; Liu, J.; Bai, M.Q.; Yang, X.; Mo, Z.W. Limited resource semi-quantum secret sharing based on multi-level systems. *Int. J. Theor. Phys.* **2019**, *58*, 2883–2892. [CrossRef]
33. Tsai, C.W.; Yang, C.W.; Lee, N.Y. Semi-quantum secret sharing protocol using W-state. *Mod. Phys. Lett. A* **2019**, *34*, 1950213. [CrossRef]
34. Tian, Y.; Li, J.; Chen, X.B.; Ye, C.Q.; Li, H.J. An efficient semi-quantum secret sharing protocol of specific bits. *Quantum Inf. Process.* **2021**, *20*, 217. [CrossRef]

35. Hu, W.; Zhou, R.G.; Luo, J. Semi-quantum secret sharing in high-dimensional quantum system using product states. *Chin. J. Phys.* **2022**, *77*, 1701–1712. [CrossRef]
36. Wang, X.L.; Cai, X.D.; Su, Z.E.; Chen, M.C.; Wu, D.; Li, L.; Liu, N.L.; Lu, C.Y.; Pan, J.W. Quantum teleportation of multiple degrees of freedom of a single photon. *Nature* **2015**, *518*, 516–519. [CrossRef]
37. Ye, T.Y.; Li, H.K.; Hu, J.L. Semi-quantum key distribution with single photons in both polarization and spatial-mode degrees of freedom. *Int. J. Theor. Phys.* **2020**, *59*, 2807–2815. [CrossRef]
38. Cabello, A. Quantum key distribution in the Holevo limit. *Phys. Rev. Lett.* **2000**, *85*, 5635. [CrossRef]