

Verifiable quantum secret sharing scheme based on orthogonal product states

Chen-Ming Bai(白晨明), Lu Liu(刘璐), and Sujuan Zhang(张素娟)

Citation: Chin. Phys. B, 2024, 33 (**7**): 070302. DOI: 10.1088/1674-1056/ad342a
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Cryptanalysis of efficient semi-quantum secret sharing protocol using single particles

Gan Gao(高甘)
Chin. Phys. B, 2024, 33 (**4**): 040301. DOI: 10.1088/1674-1056/ad2bee

An efficient multiparty quantum secret sharing scheme using a single qudit

Wenwen Hu(胡文文), Bangshu Xiong(熊邦书), and Rigui Zhou(周日贵)
Chin. Phys. B, 2023, 32 (**8**): 080303. DOI: 10.1088/1674-1056/aca391

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)
Chin. Phys. B, 2023, 32 (**7**): 070308. DOI: 10.1088/1674-1056/ace159

Measurement-device-independent quantum secret sharing with hyper-encoding

Xing-Xing Ju(居星星), Wei Zhong(钟伟), Yu-Bo Sheng(盛宇波), and Lan Zhou(周澜)
Chin. Phys. B, 2022, 31 (**10**): 100302. DOI: 10.1088/1674-1056/ac70bb

Dynamic quantum secret sharing protocol based on two-particle transform of Bell states

Yu-Tao Du(杜宇韬), Wan-Su Bao(鲍皖苏)
Chin. Phys. B, 2018, 27 (**8**): 080304. DOI: 10.1088/1674-1056/27/8/080304

Verifiable quantum secret sharing scheme based on orthogonal product states

Chen-Ming Bai(白晨明)[†], Lu Liu(刘璐), and Sujuan Zhang(张素娟)

Department of Mathematics and Physics, Shijiazhuang Tiedao University, Shijiazhuang 050043, *China*

(Received 21 December 2023; revised manuscript received 4 March 2024; accepted manuscript online 15 March 2024)

In the domain of quantum cryptography, the implementation of quantum secret sharing stands as a pivotal element. In this paper, we propose a novel verifiable quantum secret sharing protocol using the d-dimensional product state and Lagrange interpolation techniques. This protocol is initiated by the dealer Alice, who initially prepares a quantum product state, selected from a predefined set of orthogonal product states within the $\mathbb{C}^d \otimes \mathbb{C}^d$ framework. Subsequently, the participants execute unitary operations on this product state to recover the underlying secret. Furthermore, we subject the protocol to a rigorous security analysis, considering both eavesdropping attacks and potential dishonesty from the participants. Finally, we conduct a comparative analysis of our protocol against existing schemes. Our scheme exhibits economies of scale by exclusively employing quantum product states, thereby realizing significant cost-efficiency advantages. In terms of access structure, we adopt a (t,n)-threshold architecture, a strategic choice that augments the protocol's practicality and suitability for diverse applications. Furthermore, our protocol includes a rigorous integrity verification mechanism to ensure the honesty and reliability of the participants throughout the execution of the protocol.

Keywords: quantum secret sharing, quantum product state, threshold scheme, unitary operations

PACS: 03.67.–a, 03.65.Ud **DOI:** 10.1088/1674-1056/ad342a

1. Introduction

Secret sharing is an important branch of cryptography and it provides new ideas for solving key management problems.[1,2] In 1979, Shamir[1] and Blakley[2] constructed (t,n)-threshold secret sharing schemes, respectively. In the realm of secret sharing algorithms, the Shamir system is grounded in the principles of polynomial interpolation, whereas the Blakley system is rooted in the framework of finite geometry. Within the (t,n)-threshold model, the dealer partitions the confidentiality asset into n discrete shares, which are then allocated to a collective of participants. This scheme ensures that the veracity of the secret may be accurately reconstructed through the collaborative efforts of any t participants; conversely, the reconstruction becomes infeasible with fewer than t participants.

Quantum secret sharing (QSS) serves as the quantum analog to its classical counterpart, occupying a paramount position within the sphere of quantum cryptography research. By harmoniously integrating tenets from both quantum theory and classical secret sharing, QSS schemes have emerged as a robust means to securely distribute information in the quantum domain. With the burgeoning field of quantum information, which is continuously growing, the domain of secret sharing has accordingly undergone a paradigm shift, transcending classical confines to embrace the quantum realm. This evolution is epitomized by the emergence of QSS protocols.[3–5] These protocols hold the unique distinction of facilitating not only the sharing of classical information but also enabling the dissemination of unknown quantum states among authorized parties. The historical milestone of the first QSS scheme was achieved in 1999, with Hillery *et al.*[3] paving the way through the utilization of three-particle or four-particle GHZ states. In the same year, Cleve *et al.*[4] proposed the threshold QSS scheme based on the theory of quantum error correction codes. Subsequently, Xiao *et al.*[6] generalized the QSS of Hillery *et al.* into arbitrary multiparty. Since then, numerous QSS schemes based on different theoretical frameworks have been put forward.[7–15] For instance, Wang *et al.*[16] presented a QSS scheme that relies on the local distinguishability of orthogonal multiqudit entangled states, enabling the realization of a (t,n)-threshold access structure. Tavakoli *et al.*[17] constructed the QSS scheme through the mutual unbiased basis and d-dimensional single-particle quantum states, where d is restricted to odd prime number. In addition, Qin *et at.*[18] gave a verifiable (t,n)-threshold QSS using d-dimensional Bell state. Bai *et al.*[19] proposed a verifiable QSS scheme using d-dimensional GHZ state. Furthermore, significant experimental progress has been made in the domain of QSS schemes, underscoring the feasibility of quantum-based approaches to secure information dissemination.[20–23]

The majority of QSS schemes employ either quantum entanglement or single-particle quantum states as their foundation. Although quantum entanglement does occupy a critical position within the realm of QSS, its presence is not imperative for the functioning of QSS protocols. In 2003, Guo *et al.*[24] proposed a QSS protocol without entanglement based

[†]Corresponding author. E-mail: baichm@stdu.edu.cn

© 2024 Chinese Physical Society and IOP Publishing Ltd

on a modified BB84 QKD protocol and the efficiency is improved to approach 100%, with the use of quantum data storage. Hsu *et al.*[25] constructed a class of QSS schemes based on product states. Yang *et al.*[26] presented an efficient QSS protocol with orthogonal product states in the $\mathbb{C}^3\otimes\mathbb{C}^3$ Hilbert space. Hu *et al.*[27] proposed a novel semi-QSS protocol in high-dimensional quantum system using product states. Accordingly, this evidence substantiates the efficacy of employing quantum product states as a cornerstone in the construction of QSS protocols. Concurrently, the local distinguishability of orthogonal product states has emerged as a prominent research trajectory within the quantum information landscape, yielding a wealth of theories and properties that continue to illuminate this subject.[28–31] From the above analysis, it is not difficult to see that the QSS protocol, established via a quantum entangled state and unitary transformations, facilitates the realization of a more complex threshold structure. Conversely, the scheme predicated on the quantum product state is confined to a simple threshold structure. However, the preparation of quantum product states is significantly more accessible compared to that of quantum entangled states. Hence, we consider the adoption of quantum product states combined with unitary transformations as a means to accomplish the threshold structure. This approach not only successfully achieves the threshold structure but also simplifies the preparation of quantum states and saves quantum resources.

In this paper, we will use the orthogonal product states within the $\mathbb{C}^d\otimes\mathbb{C}^d$ Hilbert space and harness the power of Lagrange interpolation to unveil a verifiable (t,n)-threshold QSS scheme. In our scheme, the dealer prepares a quantum product state that is randomly selected from an ensemble of orthogonal product states on $\mathbb{C}^d\otimes\mathbb{C}^d$. Subsequently, we integrate the data block transmission technique[32] and capitalize on the decoy-photon technique[33] to reinforce the security of the transmission. Then, these participants perform the unitary operations on the product state to reconstruct the secret. Finally, we analyze the security of the scheme against both eavesdropping and dishonest participants.

The organization of this paper is as follows. In Section 2, we give some preliminaries. In Section 3, we propose the verifiable QSS scheme based on product states. In Section 4, we analyze the correctness and security of our schemes. Section 5 compares our scheme with the existing schemes. Finally, the conclusion is given in Section 6.

2. Preliminaries

In this section, we introduce some preliminaries that are employed in the subsequent discussion.

2.1. Orthogonal product states

To start with, we define a set of orthogonal states to be locally indistinguishable if they cannot be perfectly distinguished via local operations and classical communication (LOCC).[25,34] Here, we consider a set of orthogonal product states on $\mathbb{C}^d\otimes\mathbb{C}^d$ as follows:

$$
\begin{aligned}
&|\psi_{2i-1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |i\rangle)|i\rangle,\\
&|\psi_{2j+2(d-1)}\rangle = \frac{1}{\sqrt{2}}|j+1\rangle(|0\rangle + |j\rangle),\\
&|\psi_{2i}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |i\rangle)|i\rangle,\\
&|\psi_{2j-1+2(d-1)}\rangle = \frac{1}{\sqrt{2}}|j+1\rangle(|0\rangle - |j\rangle),\\
&|\psi_{4d-5}\rangle = \frac{1}{\sqrt{2}}|1\rangle(|0\rangle - |d-1\rangle),\\
&|\psi_{4d-4}\rangle = \frac{1}{\sqrt{2}}|1\rangle(|0\rangle + |d-1\rangle),
\end{aligned}
\tag{1}
$$

where $i = 1,2,\ldots,d-1$ and $j = 1,2,\ldots,d-2$.

Theorem 1 The following orthogonal product states in Eq. (1) cannot be perfectly distinguished by LOCC, no matter who goes first.

Proof Suppose that the first party performs a general measurement with a set of $d\times d$ positive operator-valued measure (POVM) elements $\{M_k^\dagger M_k : k = 1,2\}$, where

$$
M_k^\dagger M_k = \begin{bmatrix}
m_{0,0}^k & m_{0,1}^k & m_{0,2}^k & \cdots & m_{0,d-1}^k\\
m_{1,0}^k & m_{1,1}^k & m_{1,2}^k & \cdots & m_{1,d-1}^k\\
m_{2,0}^k & m_{2,1}^k & m_{2,2}^k & \cdots & m_{2,d-1}^k\\
\vdots & \vdots & \vdots & & \vdots\\
m_{d-1,0}^k & m_{d-1,1}^k & m_{d-1,2}^k & \cdots & m_{d-1,d-1}^k
\end{bmatrix}
\tag{2}
$$

under the basis $\{|0\rangle,|1\rangle,\ldots,|d-1\rangle\}$.

It is noted that the post-measurement states must be pairwise orthogonal to make further discrimination feasible. That is, the states that are orthogonal on the first side should maintain the orthogonality on the first side after the measurement.

For the sake of convenience, let us consider the example of quantum states $|\psi_1\rangle$, $|\psi_2\rangle$ and $|\psi_{2d}\rangle$ as an example. Therefore, we have

$$\langle\psi_1|M_k^\dagger M_k\otimes I_d^\dagger I_d|\psi_{2d}\rangle = \frac{1}{2}(m_{0,2}^k - m_{1,2}^k) = 0, \tag{3}$$

$$\langle\psi_2|M_k^\dagger M_k\otimes I_d^\dagger I_d|\psi_{2d}\rangle = \frac{1}{2}(m_{0,2}^k + m_{1,2}^k) = 0, \tag{4}$$

$$\langle\psi_{2d}|M_k^\dagger M_k\otimes I_d^\dagger I_d|\psi_1\rangle = \frac{1}{2}(m_{2,0}^k - m_{2,1}^k) = 0, \tag{5}$$

$$\langle\psi_{2d}|M_k^\dagger M_k\otimes I_d^\dagger I_d|\psi_2\rangle = \frac{1}{2}(m_{2,0}^k + m_{2,1}^k) = 0. \tag{6}$$

Hence, by Eqs. (3)–(6), we can get

$$m_{0,2}^k = m_{1,2}^k = 0, \quad m_{2,0}^k = m_{2,1}^k = 0.$$

Using the same method to analyze the quantum states in Eq. (1), we can obtain

$$m^k_{v,w} = m^k_{w,v} = 0, \tag{7}$$

where $v \neq w$ and $v, w = 0, 1, \ldots, d-1$.

Second, we take the quantum states $|\psi_{2i-1}\rangle$ and $|\psi_{2i}\rangle$ as an example. Therefore, we have

$$\begin{aligned} &\langle\psi_{2i-1}|M_k^\dagger M_k \otimes I_d^\dagger I_d|\psi_{2i}\rangle \\ &= m^k_{0,0} + m^k_{0,i} - m^k_{i,0} - m^k_{i,i} = 0. \end{aligned} \tag{8}$$

Since $m^k_{i,0} = m^k_{0,i} = 0$, we obtain

$$m^k_{0,0} = m^k_{i,i},$$

where $i = 1, \ldots, d-1$.

This implies that any of POVM elements belonging to the first party should have the form

$$M_k^\dagger M_k = \begin{bmatrix} m^k_{0,0} & 0 & 0 & \ldots & 0 \\ 0 & m^k_{0,0} & 0 & \ldots & 0 \\ 0 & 0 & m^k_{0,0} & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & m^k_{0,0} \end{bmatrix} \propto I_d. \tag{9}$$

Through the above analysis, all of the first party's POVM elements must be proportional to the identity. Thus, the first party cannot go first and by the symmetry of states in Eq. (1), neither can the second party. Therefore, these states are locally indistinguishable. This completes the proof.

According to these quantum states described in Eq. (1), we proceed to construct a set of measurement operators as follows:

$$\begin{aligned} &M_{2i-1} = |\psi_{2i-1}\rangle\langle\psi_{2i-1}|, \\ &M_{2j-1+2(d-1)} = |\psi_{2j-1+2(d-1)}\rangle\langle\psi_{2j-1+2(d-1)}|, \\ &M_{2i} = |\psi_{2i}\rangle\langle\psi_{2i}|, \\ &M_{2j+2(d-1)} = |\psi_{2j+2(d-1)}\rangle\langle\psi_{2j+2(d-1)}|, \\ &M_{4d-5} = |\psi_{4d-5}\rangle\langle\psi_{4d-5}|, \\ &M_{4d-4} = |\psi_{4d-4}\rangle\langle\psi_{4d-4}|, \\ &\tilde{M} = I - \sum_{i=1}^{d-1}(M_{2i-1} + M_{2i}) \\ &\qquad - \sum_{j=1}^{d-1}(M_{2j-1+2(d-1)} + M_{2j+2(d-1)}), \end{aligned}$$

where $i = 1, 2, \ldots, d-1$ and $j = 1, 2, \ldots, d-2$.

Using the measurement operators described above, we can obtain the set $\mathcal{M}$ of measurement operators, denoted by

$$\mathcal{M} = \{M_1, M_2, \ldots, M_{4d-5}, M_{4d-4}, \tilde{M}\}. \tag{10}$$

Example 1 For $\mathbb{C}^6 \otimes \mathbb{C}^6$ system, we give a set of orthogonal product states

$$\begin{aligned} &|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|1\rangle, \quad |\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|1\rangle, \\ &|\psi_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |2\rangle)|2\rangle, \quad |\psi_4\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |2\rangle)|2\rangle, \\ &|\psi_5\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |3\rangle)|3\rangle, \quad |\psi_6\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |3\rangle)|3\rangle, \\ &|\psi_7\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |4\rangle)|4\rangle, \quad |\psi_8\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |4\rangle)|4\rangle, \\ &|\psi_9\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |5\rangle)|5\rangle, \quad |\psi_{10}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |5\rangle)|5\rangle, \\ &|\psi_{11}\rangle = \frac{1}{\sqrt{2}}|2\rangle(|0\rangle - |1\rangle), \quad |\psi_{12}\rangle = \frac{1}{\sqrt{2}}|2\rangle(|0\rangle + |1\rangle), \\ &|\psi_{13}\rangle = \frac{1}{\sqrt{2}}|3\rangle(|0\rangle - |2\rangle), \quad |\psi_{14}\rangle = \frac{1}{\sqrt{2}}|3\rangle(|0\rangle + |2\rangle), \\ &|\psi_{15}\rangle = \frac{1}{\sqrt{2}}|4\rangle(|0\rangle - |3\rangle), \quad |\psi_{16}\rangle = \frac{1}{\sqrt{2}}|4\rangle(|0\rangle + |3\rangle), \\ &|\psi_{17}\rangle = \frac{1}{\sqrt{2}}|5\rangle(|0\rangle - |4\rangle), \quad |\psi_{18}\rangle = \frac{1}{\sqrt{2}}|5\rangle(|0\rangle + |4\rangle), \\ &|\psi_{19}\rangle = \frac{1}{\sqrt{2}}|1\rangle(|0\rangle - |5\rangle), \quad |\psi_{20}\rangle = \frac{1}{\sqrt{2}}|1\rangle(|0\rangle + |5\rangle). \end{aligned}$$

Through Theorem 1, it is not difficult to find that the above set of orthogonal product states cannot be perfectly distinguished by LOCC no matter who goes first.

2.2. Unitary operations

To study the variation of the relevant quantum states under unitary transformations, we encode the quantum states in Eq. (1) as follows:

$$\begin{aligned} &|\psi_{0,0,i-1}\rangle = |\psi_{2i-1}\rangle, \quad |\psi_{0,1,i-1}\rangle = |\psi_{2i}\rangle, \\ &|\psi_{1,0,j-1}\rangle = |\psi_{2j-1+2(d-1)}\rangle, \quad |\psi_{1,1,j-1}\rangle = |\psi_{2j+2(d-1)}\rangle, \\ &|\psi_{1,0,d-2}\rangle = |\psi_{4d-5}\rangle, \quad |\psi_{1,1,d-2}\rangle = |\psi_{4d-4}\rangle. \end{aligned} \tag{11}$$

To further investigate the orthogonal product states in Eq. (11), we construct a set of unitary operations

$$\begin{aligned} &U_0 = \sum_{i=0}^{d-1}|i\rangle\langle i|, \\ &U_l = |0\rangle\langle 0| + \sum_{i=1}^{d-1-l}|i\rangle\langle i+l| + \sum_{i=1}^{l}|(d-1-l)+i\rangle\langle i|, \\ &U_{l+d-1} = |0\rangle\langle 0| - \sum_{i=1}^{d-1-l}|i\rangle\langle i+l| - \sum_{i=1}^{l}|(d-1-l)+i\rangle\langle i|, \end{aligned} \tag{12}$$

where $l = 1, 2, \ldots, d-2$.

Furthermore, U_l and U_{l+d-1} act on the computational basis $\{|k\rangle\}_{k=0}^{d-1}$, from which we can obtain

$$\begin{aligned} U_l|k\rangle \;=\; &|0\rangle\langle 0|k\rangle + \sum_{i=1}^{d-1-l}|i\rangle\langle i+l|k\rangle \\ &+ \sum_{i=1}^{l}|(d-1-l)+i\rangle\langle i|k\rangle \end{aligned}$$

$$= \begin{cases} |0\rangle, & k=0, \\ |((d-1-l)+k)\rangle, & k=l; \\ |((d-1-l)+k) \bmod (d-1)\rangle, & k\neq l, \end{cases} \quad (13)$$

$$\begin{aligned} U_{l+d-1}|k\rangle &= |0\rangle\langle 0|k\rangle - \sum_{i=1}^{d-1-l} |i\rangle\langle i+l|k\rangle \\ &\quad - \sum_{i=1}^{l} |(d-1-l)+i\rangle\langle i|k\rangle \\ &= \begin{cases} |0\rangle, & k=0, \\ -|((d-1-l)+k)\rangle, & k=l; \\ -|((d-1-l)+k) \bmod (d-1)\rangle, & k\neq l. \end{cases} \end{aligned} \quad (14)$$

According to the above U_l and U_{l+d-1}, we can obtain a set of unitary operations on $\mathbb{C}^d \otimes \mathbb{C}^d$,

$$\begin{aligned} V_{0,0,d-1-l} &= U_l \otimes U_l, \\ V_{0,1,d-1-l} &= U_{l+d-1} \otimes U_{l+d-1}, \end{aligned} \quad (15)$$

where $l = 0,1,2,\ldots,d-2$ and note that $V_{0,0,d-1} = V_{0,0,0} = U_0 \otimes U_0$ and $V_{0,1,d-1} = V_{0,1,0} = U_{d-1} \otimes U_{d-1}$.

Theorem 2 Let $|\psi_{x,y,z}\rangle$ be an orthogonal product state in Eq. (11) and $V_{\alpha,\beta,\gamma}$ be unitary operation in Eq. (15). The equation can then be obtained, i.e.,

$$V_{\alpha,\beta,\gamma}|\psi_{x,y,z}\rangle = |\psi_{\delta_1,\delta_2,\delta_3}\rangle, \quad (16)$$

where $x,y,\alpha,\beta = 0,1$, $z = 0,1,\ldots,d-2$, $\delta_1 = (\alpha+x) \bmod 2$, $\delta_2 = (\beta+y) \bmod 2$ and $\delta_3 = (\gamma+z) \bmod (d-1)$.

Proof To facilitate the computation, we take $|\psi_{0,0,i-1}\rangle$ as the example, and the others can utilize a similar approach to prove. Since $V_{0,0,d-1-l}$ and $V_{0,1,d-1-l}$, we can then obtain that the result of performing $V_{0,0,d-1-l}$ or $V_{0,1,d-1-l}$ on the $|\psi_{0,0,i-1}\rangle$,

$$\begin{aligned} & V_{0,0,d-1-l}|\psi_{0,0,i-1}\rangle \\ &= (U_l \otimes U_l)\left(\frac{|0\rangle - |i\rangle}{\sqrt{2}} \otimes |i\rangle\right), \\ &= \begin{cases} |\psi_{0,0,((d-1-l)+(i-1))}\rangle, & i=l; \\ |\psi_{0,0,((d-1-l)+(i-1)) \bmod (d-1)}\rangle, & i\neq l, \end{cases} \end{aligned} \quad (17)$$

$$\begin{aligned} & V_{0,1,d-1-l}|\psi_{0,0,i-1}\rangle \\ &= (U_{l+d-1} \otimes U_{l+d-1})\left(\frac{|0\rangle - |i\rangle}{\sqrt{2}} \otimes |i\rangle\right), \\ &= \begin{cases} -|\psi_{0,0,((d-1-l)+(i-1))}\rangle, & i=l; \\ -|\psi_{0,0,((d-1-l)+(i-1)) \bmod (d-1)}\rangle, & i\neq l. \end{cases} \end{aligned} \quad (18)$$

Since a global phase does not affect the unitary operation on the quantum state, we remove the global phase (-1) in Eq. (18). Therefore, by Eqs. (17) and (18), we can prove that Eq. (16) is true. □

3. Quantum secret sharing scheme

Now we give our scheme in several steps. Alice aims to share her confidential information among Bob_i $(i = 1,2,\ldots,n)$ such that any t out of them collaborate to reconstruct Alice's secret. In our protocol, we use the data block transmission[32] and the decoy-photon technique.[33,35] In addition, the quantum channel is public in our scheme, while the classical channel is authenticated, ensuring that transmitted messages remain untampered.

3.1. Preparation phase

The dealer Alice uses the following steps to distribute her secret.

Step 3.1.1 Alice randomly chooses a_i $(i \in \{0,1,\ldots,t-1\})$ from a finite field $\text{GF}(d-1)$ to form her private information. Then, she defines a polynomial, denoted by

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1}x^{t-1} \bmod (d-1), \quad (19)$$

where $s = f(0) = a_0 \bmod (d-1)$ is a secret. Here, Alice selects distinct elements $x_i \in \text{GF}(d-1)$ for $i = 1,2,\ldots,n$. Each x_i serves as a unique identifier for Bob_i', functioning as a piece of personal information that distinguishes one recipient from another.

Furthermore, Alice pronounces the values of all x_i and computes $f(x_i)$. Then, she sends the computed values to Bob_i through a certain secure quantum secure direct communication protocol. Note that Alice and Bob_i share a secret that is only known by them.

Step 3.1.2 Alice and the participants negotiate a suitable hash function $H(\boldsymbol{x})$, where $\boldsymbol{x} = (x_1, x_2, \ldots, x_{n+2})$ represents a $(n+2)$-dimensional vector. In addition, Alice constructs an $n \times n$ matrix according to the following procedure:

$$A = \begin{bmatrix} \boldsymbol{\eta}_1 \\ \boldsymbol{\eta}_2 \\ \vdots \\ \boldsymbol{\eta}_n \end{bmatrix} = \begin{bmatrix} h_{11} & h_{12} & \ldots & h_{1n} \\ h_{21} & h_{22} & \ldots & h_{2n} \\ \vdots & \vdots & & \vdots \\ h_{n1} & h_{n2} & \ldots & h_{nn} \end{bmatrix}, \quad (20)$$

where $h_{ij} \in \text{GF}(d-1)$. After that, she sends $\boldsymbol{\eta}_i$ of the matrix A to Bob_i $(i = 1,2,\ldots,n)$ through quantum secure direct communication technology.

3.2. Distribution phase

Suppose that t participants, $\text{Bob}_1, \text{Bob}_2, \ldots, \text{Bob}_t$, cooperate to restore the original secret (see Fig. 1). Similarly, any t participants can restore the secret together in the same way.

Step 3.2.1 First, the dealer Alice randomly selects the quantum state in Eq. (1)

$$|\varphi_{\alpha,\beta,\gamma}\rangle = |\phi_1^{(0)}\rangle |\phi_2^{(0)}\rangle.$$

In order to ensure the security of the transmission process, Alice randomly selects m quantum states from $\mathcal{D}_i = \{\frac{|0\rangle - |i\rangle}{\sqrt{2}}, \frac{|0\rangle + |i\rangle}{\sqrt{2}}\}$ or $\tilde{\mathcal{D}}_i = \{\frac{|0\rangle - \mathrm{i}|i\rangle}{\sqrt{2}}, \frac{|0\rangle + \mathrm{i}|i\rangle}{\sqrt{2}}\}$ to serve as the detection quantum states, where $i = 1,2,\ldots,d-1$ and $\mathrm{i}^2 = -1$.

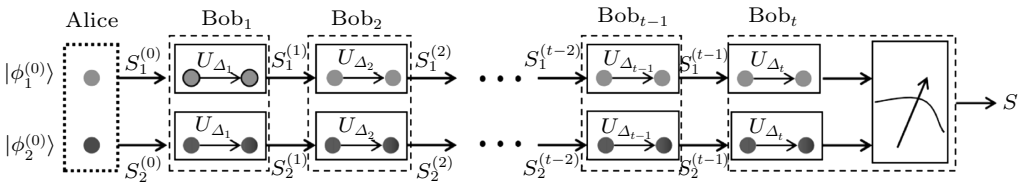


Fig. 1. The process of the information particles transferring.

Furthermore, she inserts $|\phi_2^{(0)}\rangle$ into the above detected quantum states and records its position to form the sequence $S_2^{(0)}$. Finally, Alice sends the sequence $S_2^{(0)}$ to the participant Bob$_1$. Even if the eavesdropper intercepted the above sequence, she does not know where the quantum state of the encoded information is inserted. Hence, the probability of obtaining the information is relatively small. In addition, the eavesdropper needs to fake the sequence, which also increases the probability of being detected.

Step 3.2.2 Upon receiving the transmission sequence $S_2^{(0)}$, Bob$_1$ engages in classical communication to convey receipt to Alice. Subsequently, Alice discloses the positional indices and the measurement bases employed for the detection of the quantum states within the sequence $S_2^{(0)}$ to the public domain. Bob$_1$ then proceeds to conduct measurements on his complement of detection quantum states, employing the identical bases as those announced by Alice, and relays the outcomes to her. Utilizing these data, Alice calculates the error rate. If the error rate exceeds a predetermined threshold value, then she must abort the protocol and initiate a new round with fresh resources.

If there is no eavesdropping, Bob$_1$ uses the message $f(x_1)$ sent by Alice to calculate that

$$\gamma_1 = f(x_1) \prod_{1<j\le t} \frac{x_j}{x_j - x_1} \bmod (d-1).$$

Based on the value of γ_1, Bob$_1$ randomly selects a unitary operation $V_{\alpha_1,\beta_1,\gamma_1}$ from the set $\{V_{0,0,\gamma_1}, V_{0,1,\gamma_1}\}$, where $V_{0,0,\gamma_1}$ and $V_{0,1,\gamma_1}$ can be denoted by

$$\begin{aligned} V_{0,0,\gamma_1} &= U_{d-1-\gamma_1} \otimes U_{d-1-\gamma_1}, \\ V_{0,1,\gamma_1} &= U_{2(d-1)-\gamma_1} \otimes U_{2(d-1)-\gamma_1}. \end{aligned}$$

Using the vector η_1, he calculates the corresponding hash value $H(\alpha_1,\beta_1,\eta_1)$ and publicly announces it. Suppose that the unitary operation chosen by Bob$_1$ is

$$V_{\alpha_1,\beta_1,\gamma_1} = U_{\Delta_1} \otimes U_{\Delta_1},$$

where $\Delta_1 = d-1-\gamma_1$ or $2(d-1)-\gamma_1$.

Next, Bob$_1$ performs the unitary operation U_{Δ_1} on the initial state $|\phi_2^{(0)}\rangle$, resulting in the transformed state $|\phi_2^{(1)}\rangle$. Subsequently, Bob$_1$ randomly selects m quantum states from $\mathcal{D}_i$ or $\tilde{\mathcal{D}}_i$ as the detection quantum states. The transformed state $|\phi_2^{(1)}\rangle$ is then inserted into this collection of detection states, and the positions of insertion are meticulously recorded to construct the sequence $S_2^{(1)}$. Finally, Bob$_1$ sends the sequence $S_2^{(1)}$ to the participant Bob$_2$.

Step 3.2.3 After Bob$_2$ receives the corresponding sequence $S_2^{(1)}$ of quantum states, Bob$_1$ and Bob$_2$ adopt the method in Step 3.2.2.

If there is no eavesdropping, Bob$_2$ can construct the unitary operation $V_{\alpha_2,\beta_2,\gamma_2} = U_{\Delta_2} \otimes U_{\Delta_2}$ and expose the hash value $H(\alpha_2,\beta_2,\eta_2)$, where $\Delta_2 = d-1-\gamma_2$ or $2(d-1)-\gamma_2$ and

$$\gamma_2 = f(x_2) \prod_{\substack{1\le j\le t \\ j\ne 2}} \frac{x_j}{x_j - x_2} \bmod (d-1).$$

According to $V_{\alpha_2,\beta_2,\gamma_2}$, Bob$_2$ acts on the quantum state $|\phi_2^{(1)}\rangle$ with the unitary operation U_{Δ_2} and obtains a new quantum state $|\phi_2^{(2)}\rangle$.

Step 3.2.4 The above steps are repeated until participant Bob$_t$ completes the operation and obtains the quantum state $|\phi_2^{(t)}\rangle$.

For the first particle $|\phi_1^{(0)}\rangle$ in the quantum state $|\varphi_{\alpha,\beta,\gamma}\rangle$, Alice uses the same method to transmit it to Bob$_1$. Then, Bob$_1$ uses the unitary operation U_{Δ_1} to act on the quantum state $|\phi_1^{(0)}\rangle$ and obtains the quantum state $|\phi_1^{(1)}\rangle$. This process is repeated for t rounds until participant Bob$_t$ completes the corresponding operation and obtains the quantum state $|\phi_1^{(t)}\rangle$.

3.3. Reconstruction phase

Step 3.3.1 After completing all the unitary operations, the initial product state $|\varphi_{\alpha,\beta,\gamma}\rangle = |\phi_1^{(0)}\rangle|\phi_2^{(0)}\rangle$ chosen by Alice is changed to

$$\begin{aligned} &|\varphi_{l_1,l_2,l_3}\rangle \\ &= V_{\alpha_t,\beta_t,\gamma_t} \cdot V_{\alpha_{t-1},\beta_{t-1},\gamma_{t-1}} \cdots V_{\alpha_2,\beta_2,\gamma_2} \cdot V_{\alpha_1,\beta_1,\gamma_1} |\varphi_{\alpha,\beta,\gamma}\rangle \\ &= \left|\varphi_{(\sum_{i=1}^t \alpha_1+\alpha) \bmod 2, (\sum_{i=1}^t \beta_1+\beta) \bmod 2, (\sum_{i=1}^t \gamma_1+\gamma) \bmod (d-1)}\right\rangle. \end{aligned} \tag{21}$$

Furthermore, Alice proceeds to request that all participants, Bob$_1$, Bob$_2$, …, Bob$_t$, disclose their selected (α_i,β_i) $(i=1,2,\ldots,t)$. She then calculates the corresponding hash value $\hat{H}(\alpha_i,\beta_i,\eta_i)$. If $\hat{H}(\alpha_i,\beta_i,\eta_i) = H(\alpha_i,\beta_i,\eta_i)$ is true, then it means that all participants are honest. Finally, Alice discloses the outcomes of the integrity verification process to the public forum.

Step 3.3.2 When all participants are honest, Bob$_t$ uses the measurement operator $\mathcal{M}$ as defined in Eq. (10) to measure the quantum state $|\varphi_{l_1,l_2,l_3}\rangle$ in the hand. As a result of the

measurement process, Bob_t obtains the following outcome:

$$l_1 = \left(\sum_{i=1}^{t} \alpha_i + \alpha\right) \bmod 2, \tag{22}$$

$$l_2 = \left(\sum_{i=1}^{t} \beta_i + \beta\right) \bmod 2, \tag{23}$$

$$l_3 = \left(\sum_{i=1}^{t} \gamma_i + \gamma\right) \bmod (d-1). \tag{24}$$

Step 3.3.3 Subsequently, Bob_t sends the obtained result (l_1, l_2, l_3) to Alice. Then, Alice implements the second validation of participant honesty based on publicly available information (α_i, β_i) from all participants, as well as their secret shares γ_i. If Eqs. (22)–(24) are true, then it signifies that the unitary operations utilized by the participants are consistent with their public information.

After the completion of the second round of honesty verification, Alice reveals the parameters γ. Subsequently, Bob_t is able to retrieve the original secret that was hidden in $|\varphi_{l_1,l_2,l_3}\rangle$, that is,

$$s = l_3 - \gamma = \sum_{i=1}^{t} \gamma_i \bmod (d-1).$$

3.4. Example

In this example, we give a $(3,4)$ threshold QSS scheme using the orthogonal product states in example 1. Suppose that the finite field is GF(5) and Alice wants to share the secret $s = 4$, where Bob_i $(i = 1,2,3,4)$ has a public information $x_i = i$. To facilitate the illustration of the protocol, we assume that Bob_1, Bob_2, Bob_3 will recover this secret s.

First, Alice selects a polynomial as follows:

$$f(x) = 4 + 3x + 2x^2 \bmod 5. \tag{25}$$

In addition, Alice calculates $f(x_i)$ $(i = 1,2,3)$ and sends $f(x_i)$ to Bob_i through the secure channel, where $f(x_i)$ $(i = 1,2,3)$ can be denoted by

$$f(x_1) = f(1) = 4;$$
$$f(x_2) = f(2) = 3;$$
$$f(x_3) = f(3) = 1.$$

Then, Alice randomly selects the quantum state $|\varphi_{1,1,3}\rangle = |\psi_{18}\rangle = \frac{1}{\sqrt{2}}|5\rangle(|0\rangle + |4\rangle)$. Therefore, Alice and participants use decoy photon state technology to transfer the first particle and second particle of $|\varphi_{1,1,3}\rangle$ to the next participant, respectively. This technique ensures secure and reliable transfer of the quantum state between participants.

Then Bob_1 calculates that

$$\gamma_1 = f(x_1) \prod_{1<j\le 3} \frac{x_j}{x_j - x_1} \bmod 5 = 2.$$

According to the value of γ_1, Bob_1 randomly selects a unitary operation $V_{0,1,2} = U_8 \otimes U_8$ and applies this unitary operation U_8 to the first particle and the second particle, respectively. The remaining participants can follow the same procedure outlined in Table 1 to obtain their respective unitary operations.

Table 1. Information for each participant.

Participants	$f(x_i)$	The value of γ_i	Unitary operation
Bob_1	$f(1) = 4$	$\gamma_1 = 2$	$V_{0,1,2} = U_8 \otimes U_8$
Bob_2	$f(2) = 3$	$\gamma_2 = 1$	$V_{0,0,1} = U_4 \otimes U_4$
Bob_3	$f(3) = 1$	$\gamma_3 = 1$	$V_{0,1,1} = U_9 \otimes U_9$

After completing all the unitary operations, the initial product state $|\varphi_{1,1,3}\rangle$ is changed to

$$|\varphi_{\hat{l}_1,\hat{l}_2,\hat{l}_3}\rangle = V_{0,1,1} \cdot V_{0,0,1} \cdot V_{0,1,2} |\varphi_{1,1,3}\rangle = |\varphi_{1,1,2}\rangle. \tag{26}$$

To measure the quantum state $|\varphi_{1,1,2}\rangle$, the set of orthogonal product states is changed to an orthogonal complete set. Therefore, the following quantum states need to be supplemented:

$$\begin{aligned}
&|\Omega_1\rangle = |0\rangle|0\rangle, \quad |\Omega_2\rangle = |1\rangle|2\rangle,\\
&|\Omega_3\rangle = |1\rangle|3\rangle, \quad |\Omega_4\rangle = |1\rangle|4\rangle,\\
&|\Omega_5\rangle = |2\rangle|3\rangle, \quad |\Omega_6\rangle = |2\rangle|4\rangle,\\
&|\Omega_7\rangle = |2\rangle|5\rangle, \quad |\Omega_8\rangle = |3\rangle|1\rangle,\\
&|\Omega_9\rangle = |3\rangle|4\rangle, \quad |\Omega_{10}\rangle = |3\rangle|5\rangle,\\
&|\Omega_{11}\rangle = |4\rangle|1\rangle, \quad |\Omega_{12}\rangle = |4\rangle|2\rangle,\\
&|\Omega_{13}\rangle = |4\rangle|5\rangle, \quad |\Omega_{14}\rangle = |5\rangle|1\rangle,\\
&|\Omega_{15}\rangle = |5\rangle|2\rangle, \quad |\Omega_{16}\rangle = |5\rangle|3\rangle.
\end{aligned} \tag{27}$$

Therefore, Bob_3 can construct a set of measurement operators

$$M = \left\{|\psi_i\rangle\langle\psi_i|, |\Omega_j\rangle\langle\Omega_j| | i = 1,2,\ldots,20; j = 1,2,\ldots,16\right\}.$$

Then, he measures the quantum state $|\varphi_{1,1,2}\rangle$ to obtain the measurement result

$$\hat{l}_1 = 1, \quad \hat{l}_2 = 1, \quad \hat{l}_3 = 2. \tag{28}$$

Through honesty verification, Alice exposes the parameter $\gamma = 3$. Therefore, Bob_3 can obtain the original secret $s = (\hat{l}_3 - \gamma) \bmod 5 = 4$.

4. Scheme analysis

4.1. Correctness analysis

Definition 1 A QSS scheme is called "correct" if, for any strategy of the adversary, $\hat{s} = s$, where s is the dealer's secret and $\hat{s}$ is the secret recovery by the participants.

In our scheme, after these unitary operations of all participants, Bob_t measures the final quantum state $|\varphi_{l_1,l_2,l_3}\rangle$ and gets $l_3 = (\sum_{i=1}^{t} \gamma_i + \gamma) \bmod (d-1)$. This condition contributes to recovering the shared secret perfectly. Therefore, we can state the following theorem.

Theorem 3 In the absence of effective eavesdropping the dealer's secret can be perfectly reconstructed by the participants for an honest implementation of the secret distribution and recovery phase of the proposed scheme.

Proof After the action of unitary operations, the initial state $|\varphi_{l_1,l_2,l_3}\rangle$ becomes the final quantum state

$$\begin{aligned}&|\varphi_{l_1,l_2,l_3}\rangle\\ &= V_{\alpha_t,\beta_t,\gamma_t}\cdot V_{\alpha_{t-1},\beta_{t-1},\gamma_{t-1}}\cdots V_{\alpha_2,\beta_2,\gamma_2}\cdot V_{\alpha_1,\beta_1,\gamma_1}|\varphi_{\alpha,\beta,\gamma}\rangle\\ &= \Big|\varphi_{(\sum_{i=1}^{t}\alpha_1+\alpha)\bmod 2,(\sum_{i=1}^{t}\beta_1+\beta)\bmod 2,(\sum_{i=1}^{t}\gamma_1+\gamma)\bmod (d-1)}\Big\rangle.\end{aligned} \tag{29}$$

Bob_t can distinguish $|\varphi_{l_1,l_2,l_3}\rangle$ with the measurement operator $\mathcal{M}$. Therefore, Bob_t can obtain that

$$\begin{aligned}l_1 &= \Big(\sum_{i=1}^{t}\alpha_i+\alpha\Big)\bmod 2,\\ l_2 &= \Big(\sum_{i=1}^{t}\beta_i+\beta\Big)\bmod 2,\\ l_3 &= \Big(\sum_{i=1}^{t}\gamma_i+\gamma\Big)\bmod (d-1).\end{aligned}$$

To obtain a secret s, Alice declares γ. After Alice's declaration, Bob_t calculates that

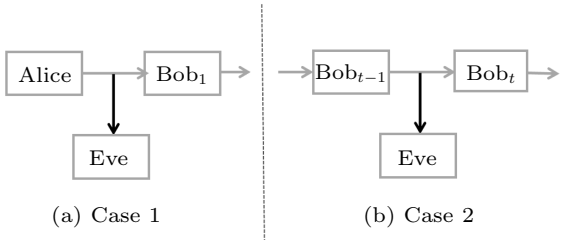
$$\hat{s} = (l_3-\gamma)\bmod (d-1) = \Big(\sum_{i=1}^{t}\gamma_i+\gamma\Big)\bmod (d-1).$$

By Lagrange interpolation, Bob_t can restore the secret s, i.e., $\hat{s}=s$.

4.2. Security analysis

In the quantum communication protocol, ensuring security is of utmost importance because it determines whether the information can be transmitted in a completely secure manner. In this section we analyze the security of our scheme against three primary quantum attacks: intercept-and-resend attack, entangle-and-measure attack, and dishonest participant attack.

(1) Intercept-and-resend attack In this paper, we primarily utilize the decoy photon technique to check eavesdropper's attacks. The detection quantum states we employ are chosen from $\mathcal{D}_i=\{\frac{|0\rangle-|i\rangle}{\sqrt{2}},\frac{|0\rangle+|i\rangle}{\sqrt{2}}\}$ or $\tilde{\mathcal{D}}_i=\{\frac{|0\rangle-\mathrm{i}|i\rangle}{\sqrt{2}},\frac{|0\rangle+\mathrm{i}|i\rangle}{\sqrt{2}}\}$, where $i=1,2,\ldots,d-1$. In the following analysis, we will consider two cases of the intercept-and-resend attack (see Fig. 2).



(a) Case 1 (b) Case 2

Fig. 2. Two cases of the intercept-and-resend attack.

Case 1 Suppose that Alice sends a quantum sequence $S_2^{(0)}$ containing the encoded quantum state $|\phi_2^{(0)}\rangle$ to Bob_1. However, Eve intercepts the transmitted quantum sequence $S_2^{(0)}$. In order to obtain the information in the original quantum state $|\psi_{\alpha,\beta,\gamma}\rangle$, Eve has to measure the detected quantum states in $S_2^{(0)}$. Therefore, the probability of successfully guessing the $S_2^{(0)}$ is

$$\mathrm{Prob}\big(\text{Eve guessing successfully } S_2^{(0)}\big)=\frac{1}{[4(d-1)]^m}.$$

Furthermore, the probability of Eve being successfully detected is

$$\mathrm{Prob}\big(\text{Eve being successfully detected}\big)=1-\frac{1}{[4(d-1)]^m}.$$

Therefore, Bob_1 must be detected as the number of intercepted quantum states (m) increases. Thus, it shows that the interception and retransmission in this case is a failure.

Case 2 During the transmission between Bob_{t-1} and Bob_t, Eve intercepts the quantum state sequence $S_2^{(t-1)}$ containing the encoded state $|\phi_2^{(t-1)}\rangle$. Therefore, the probability of successfully guessing the $S_2^{(t-1)}$ is

$$\mathrm{Prob}\big(\text{Eve guessing successfully } S_2^{(t-1)}\big)=\frac{1}{[4(d-1)]^m}.$$

When the eavesdropper Eve only obtains the quantum state $|\phi_2^{(t-1)}\rangle$, she cannot distinguish $|\psi_{\alpha,\beta,\gamma}\rangle$ due to Theorem 1. Therefore, Eve needs to intercept the quantum state sequence $S_1^{(t-1)}$ containing the quantum state $|\phi_1^{(t-1)}\rangle$, and the probability that she has successfully guessed the quantum state is

$$\mathrm{Prob}\big(\text{Eve guessing successfully } S_1^{(t-1)}\big)=\frac{1}{[4(d-1)]^m}.$$

Thus, the probability that Eve obtains the quantum state $|\psi_{\alpha',\beta',\gamma'}\rangle=|\phi_1^{(t-1)}\rangle|\phi_2^{(t-1)}\rangle$ is

$$\begin{aligned}&\mathrm{Prob}\big(\text{Eve obatining successfully } |\psi_{\alpha',\beta',\gamma'}\rangle\big)\\ &=\frac{1}{[4(d-1)]^{2m}}.\end{aligned} \tag{30}$$

To obtain the secret s, Eve measures the state $|\psi_{\alpha',\beta',\gamma'}\rangle=|\phi_1^{(t-1)}\rangle|\phi_2^{(t-1)}\rangle$ with the measurement operator $\mathcal{M}$ to obtain

$$\gamma'=\Big(\sum_{i=1}^{t-1}\gamma_i+\gamma\Big)\bmod (d-1).$$

Furthermore, $s=(\sum_{i=1}^{t}\gamma_i)\bmod(d-1)=(\gamma'+\gamma_t-\gamma)\bmod(d-1)$. Suppose that guess γ_t is relatively independent of γ, so the probability that Eve can successfully guess them is

$$\mathrm{Prob}\big(\text{Eve guessing successfully } \gamma_t \text{ and } \gamma\big)=\frac{1}{(d-1)^2}.$$

Therefore, the probability that Eve has guessed the secret correctly without being detected is

$$\begin{aligned}&\text{Prob}\big(\text{Eve guessing correctly the secret}\big)\\ =\ &\frac{1}{16^m(d-1)^{2(m+1)}}.\end{aligned}\tag{31}$$

In essence, the likelihood of accurately deducing the concealed information without detection in a robust communication protocol is ordinarily minute. Consequently, it is improbable for an eavesdropper to extract meaningful intelligence from this type of assault. Hence, the success of such an attack is precluded.

(2) Entangle-and-measure attack In this paper, this attack means the eavesdropper Eve entangles the auxiliary particles and measures them to obtain the information. To depict this process, we assume that the auxiliary particle is $|E\rangle$, if Eve first performs the unitary transform U_E on her particles $\{|k\rangle,|0\rangle-|k'\rangle\}$ $(k=0,1,\ldots,d-1;k'=1,\ldots,d-1)$ and the auxiliary one $|E\rangle$ in the following forms:

$$U_E|k\rangle|E\rangle=\sum_{l=0}^{d-1}a_{kl}|l\rangle|e_{kl}\rangle,\tag{32}$$

$$U_E(|0\rangle-|k'\rangle)|E\rangle=\sum_{l=0}^{d-1}a_{0l}|l\rangle|e_{0l}\rangle-\sum_{l=0}^{d-1}a_{k'l}|l\rangle|e_{k'l}\rangle,\tag{33}$$

where $|E\rangle$ is the initial state of Eve's ancillary system; $|e_{kl}\rangle$ and $|e_{k'l}\rangle$ are the pure auxiliary states determined uniquely by the unitary transform U_E.

For convenience, we take the quantum state $|\psi_{2i-1}\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|i\rangle)|i\rangle$ $(i=1,2,\ldots,d-1)$ as an example to analyse two cases of the entangle-and-measure attack.

Case 1 Assuming that the eavesdropper Eve adopts the entangle-and-measure attack on the second particle, the quantum state $|\psi_{2i-1}\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|i\rangle)|i\rangle$ becomes

$$\begin{aligned}&|\tilde{\Phi}\rangle=(I\otimes U_E)|\psi_{2i-1}\rangle|E\rangle\\ =\ &\frac{1}{\sqrt{2}}(|0\rangle-|i\rangle)\Big(\sum_{l=0}^{d-1}a_{il}|l\rangle|e_{il}\rangle\Big)\\ =\ &\frac{1}{\sqrt{2}}\Big(\sum_{l=0}^{d-1}a_{il}|0\rangle|l\rangle|e_{il}\rangle-\sum_{l=0}^{d-1}a_{il}|i\rangle|l\rangle|e_{il}\rangle\Big).\end{aligned}\tag{34}$$

Finally, the participant Bob measures $|\tilde{\Phi}\rangle$ using the operator $\mathcal{P}=|\psi_{2i-1}\rangle\langle\psi_{2i-1}|$, and the quantum state obtained after the measurement is changed to

$$\begin{aligned}\mathcal{P}|\tilde{\Phi}\rangle\ &=\ \frac{1}{\sqrt{2}}(a_{ii}|0\rangle|i\rangle|e_{ii}\rangle-a_{ii}|i\rangle|i\rangle|e_{ii}\rangle)\\ &=\ \frac{1}{\sqrt{2}}(|0\rangle-|i\rangle)|i\rangle\otimes a_{ii}|e_{ii}\rangle\\ &=\ |\psi_{2i-1}\rangle\otimes a_{ii}|e_{ii}\rangle.\end{aligned}\tag{35}$$

Case 2 Assuming that the eavesdropper Eve adopts the entangle-and-measure attack on the first particle and the second particle, the quantum state $|\psi_{2i-1}\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|i\rangle)|i\rangle$ becomes

$$\begin{aligned}|\tilde{\Psi}\rangle\ &=\ (U_E\otimes U_E)|\psi_{2i-1}\rangle|E_1\rangle|E_2\rangle\\ &=\ \frac{1}{\sqrt{2}}\Big(\sum_{l=0}^{d-1}\sum_{l'=0}^{d-1}a_{0l}b_{il'}|l\rangle|l'\rangle|e_{0l}\rangle|\varepsilon_{il'}\rangle\\ &\quad-\sum_{l=0}^{d-1}\sum_{l'=0}^{d-1}a_{il}b_{il'}|l\rangle|l'\rangle|e_{il}\rangle|\varepsilon_{il'}\rangle\Big),\end{aligned}\tag{36}$$

where $|e_{0l}\rangle$, $|e_{il}\rangle$ and $|\varepsilon_{il'}\rangle$ are the pure auxiliary states determined uniquely by the unitary transform U_E.

Finally, the participant Bob measures $|\tilde{\Psi}\rangle$ using the operator $\mathcal{P}=|\psi_{2i-1}\rangle\langle\psi_{2i-1}|$, and the quantum state obtained after the measurement is changed to

$$\begin{aligned}\mathcal{P}|\tilde{\Psi}\rangle\ &=\ \frac{1}{2\sqrt{2}}\big[|0\rangle|i\rangle(a_{00}|e_{00}\rangle-a_{i0}|e_{i0}\rangle-a_{0i}|e_{0i}\rangle+a_{ii}|e_{ii}\rangle)\\ &\quad-|i\rangle|i\rangle(a_{00}|e_{00}\rangle-a_{i0}|e_{i0}\rangle-a_{0i}|e_{0i}\rangle+a_{ii}|e_{ii}\rangle)\big]\\ &\quad\otimes b_{ii}|\varepsilon_{ii}\rangle=|\psi_{2i-1}\rangle\otimes|W_1\rangle\otimes|W_2\rangle,\end{aligned}\tag{37}$$

where $|W_1\rangle=a_{00}|e_{00}\rangle-a_{i0}|e_{i0}\rangle-a_{0i}|e_{0i}\rangle+a_{ii}|e_{ii}\rangle$ and $|W_2\rangle=b_{ii}|\varepsilon_{ii}\rangle$.

By Eqs. (35) and (37), it implies that Eve has no effect on the whole system of QSS if she intends to eavesdrop without being detected. In other words, she is unable to extract any confidential information. Consequently, the entangle-and-measure attack proves to be unsuccessful.

(3) Dishonest participant attack For the QSS scheme, it is indeed possible for a dishonest participant to provide a forged secret share, rendering it impossible for other participants to reconstruct the original secret. However, the dishonest participant can still utilize the correct secret shares to obtain the genuine secret. Moreover, multiple dishonest participants can collaborate to extract information about the secret by utilizing valid shares. This highlights the destructive influence of malicious participants within the scheme. In our proposed scheme, we assume that the last participant Bob_t is honest. In the subsequent analysis, we will demonstrate that our scheme is designed to withstand attacks from dishonest participants.

Case 1 When there is only one dishonest player, we assume that Bob_{t-1} is dishonest. If Bob_{t-1} uses an intercept-and-resend attack or entangle-and-measure attack, according to the above analysis, then he must not get useful information.

Suppose that Bob_{t-1} attacks with fake encoded quantum states. Since the particles transmitted by Alice are not transmitted simultaneously, Bob_{t-1} cannot get two particles simultaneously. Therefore, after Bob_{t-1} gets the quantum state $|\phi_2^{(t-1)}\rangle$, he needs to fake the quantum state $|\tilde{\phi}_2^{(t-1)}\rangle$ by guessing. Furthermore, the probability of success of the forged quantum state is

$$\text{Prob}\big(|\tilde{\phi}_2^{(t-1)}\rangle=|\phi_2^{(t-1)}\rangle\big)=\frac{1}{3(d-1)}.$$

After Bob_{t-1} gets the quantum state $|\phi_1^{(t-1)}\rangle$, he needs to fake the particle $|\tilde{\phi}_1^{t-1}\rangle$ according to $|\phi_2^{(t-1)}\rangle$. Therefore, the probability of two particles simultaneously forging the success is

$$\text{Prob}\big(|\tilde{\phi}_2^{(t-1)}\rangle = |\phi_2^{(t-1)}\rangle, |\tilde{\phi}_1^{(t-1)}\rangle = |\phi_1^{(t-1)}\rangle\big) = \frac{1}{4(d-1)}.$$

To obtain the secret s, Bob_{t-1} measures the state $|\psi_{\alpha',\beta',\gamma'}\rangle = |\phi_1^{(t-1)}\rangle|\phi_2^{(t-1)}\rangle$ with the measurement operator $\mathcal{M}$ to obtain

$$\gamma' = \left(\sum_{i=1}^{t-1}\gamma_i + \gamma\right) \bmod (d-1).$$

Furthermore, $s = (\sum_{i=1}^{t}\gamma_i) \bmod (d-1) = (\gamma' + \gamma_t - \gamma) \bmod (d-1)$. Suppose that guess γ_t is relatively independent of γ, so the probability that Bob_{t-1} can successfully guess them is

$$\text{Prob}\big(\text{Bob}_{t-1} \text{ guessing successfully } \gamma_t \text{ and } \gamma\big) = \frac{1}{(d-1)^2}.$$

Therefore, the probability that Bob_{t-1} has guessed the secret correctly without being detected is

$$\text{Prob}\big(\text{Eve guessing correctly the secret}\big) = \frac{1}{4(d-1)^3}. \quad (38)$$

Case 2 When there are at least two dishonest players, we assume that Bob_1 and Bob_{t-1} are dishonest. After Bob_1 receives the states $|\phi_2^{(0)}\rangle$ and $|\phi_1^{(0)}\rangle$ from Alice, he will fake the quantum states $|\tilde{\phi}_2^{(0)}\rangle$ and $|\tilde{\phi}_1^{(0)}\rangle$ to transmit them to the next participant.

Until Bob_{t-1} gets $|\tilde{\phi}_2^{(t-1)}\rangle$ and $|\tilde{\phi}_1^{(t-1)}\rangle$, and Bob_{t-1} obtains the state $|\psi_{v_1,v_2,v_3}\rangle = |\tilde{\phi}_1^{(t-1)}\rangle|\tilde{\phi}_2^{(t-1)}\rangle$ with the unitary operation. Furthermore, Bob_{t-1} measures the state $|\psi_{v_1,v_2,v_3}\rangle = |\tilde{\phi}_1^{(t-1)}\rangle|\tilde{\phi}_2^{(t-1)}\rangle$ with the measurement operator $\mathcal{M}$ to obtain

$$v_3 = \sum_{i=1}^{t-1}\gamma_i \bmod (d-1).$$

Bob_1 and Bob_{t-1} do not successfully recover the original secret due to their corresponding quantum state after their unitary operations. v_3 does not satisfy the Lagrange interpolation. Therefore, the probability of Bob_1 and Bob_{t-1} being successfully detected is

$$\text{Prob}\big(\text{Bob}_1 \text{ and } \text{Bob}_{t-1} \text{ being successfully detected}\big) = \frac{1}{(d-1)}. \quad (39)$$

By Eqs. (38) and (39), it can be inferred that as the value of d increases, the probability of success for dishonest participants becomes significantly small. This indicates that the attack by dishonest participants is ultimately unsuccessful.

5. Comparisons

In this section, we present a comparison of our proposed protocol with existing schemes[17–19,36] based on five parameters, which are displayed in Table 1.

Tavakoli's scheme[17] and Karimipour's scheme[36] both utilize d-dimensional single quantum states to construct (n,n)-threshold QSS schemes. However, neither of these schemes provide verifiable capabilities for every participant, and Karimipour's scheme was not secure from a dishonest participant who could recover the secret without the help of the other participants. In contrast, our proposed scheme offers verifiable capabilities for every participant and is secure against all dishonest participants. Therefore, our scheme is better suited for detecting participant honesty than the previous schemes.

Qin's scheme[18] and Bai's scheme[19] both use d-dimensional entangled quantum states to construct (t,n)-threshold QSS schemes. In contrast, our scheme employs product states, which are simpler to prepare and store than entangled states used in Refs. [18,19]. Overall, our proposed scheme provides advantages over existing schemes in terms of verifiability and simplicity. In addition, Hsu *et al.*[25] constructed the secret sharing scheme based on quantum product states, realizing only the case of two players. In our scheme, we construct (t,n)-threshold QSS schemes using quantum product states. Therefore, the access structure implemented by our scheme is more general.

The efficiency of the proposed QSS protocol is given as $\eta = c/(q+b)$, where c denotes the number of the transmitted secrets, q is the number of the used quantum particles, and b is the number of classical particles utilized for decoding the message (classical communication used for checking eavesdropping is not counted). In order to better reflect the efficiency, we simply revise the definition of efficiency and add the successful probability of the scheme, i.e., $\eta = cp/(q+b)$, where p is the successful probability of the scheme. Therefore, the successful probability in Tavakoli's scheme[17] is $1/d$ and the successful probability in Karimipour's scheme[36] is $1/2$. In addition, the probability in other schemes is 1. For convenience, we assume that the number of decoy photon states selected for each round in all schemes is m. Thus, we can calculate the efficiency of each protocol, see Table 2.

To sum up, although our protocol is slightly less convenient than other schemes, in terms of resources, our scheme only uses quantum product states, which can achieve good cost savings. In terms of the access structure, our scheme implements (t,n)-threshold structure, which is more practical. Moreover, our protocol conducts the validation of the participants' honesty, which ensures the honesty and reliability of the participants.

Table 2. Comparison between previous QSSs and ours.

Schemes	Quantum resources	Access structure	Efficiency	Verifiability	Security
Tavakoli[17]	single quantum state	(n,n)-threshold	$\frac{1}{d((n-1)m+1)}$	No	Yes
Karimipour[36]	single quantum state	(n,n)-threshold	$\frac{1}{2((n-1)m+1)}$	No	No
Qin[18]	Bell state	(t,n)-threshold	$\frac{1}{(t+1)m+2}(t<n)$	Yes	Yes
Bai[19]	GHZ state	(t,n)-threshold	$\frac{1}{(t+3)m+3}(t<n)$	Yes	Yes
Hsu[25]	product state	$(2,2)$-threshold	$\frac{1}{2m+2}$	No	Yes
Ours	product state	(t,n)-threshold	$\frac{1}{2tm+2}(t<n)$	Yes	Yes

6. Conclusions

In this paper, we proposed a novel verifiable QSS protocol designed to achieve the (t,n)-threshold access structure. The main component of this protocol was the utilization of d-dimensional product states for both the transfer and recovery of quantum secrets. In our proposed scheme, the dealer Alice generated the quantum product state, and the participants performed unitary operations on this state to reconstruct the original secret. Furthermore, we conducted a thorough security analysis of the proposed scheme, assessing its resilience against potential attacks. Additionally, we compared our scheme with existing schemes in the field, highlighting its advantages and distinguishing features. Through this comparative analysis, we demonstrated the effectiveness and superiority of our proposed protocol in achieving secure and verifiable QSS.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant No. 12301590) and the Natural Science Foundation of Hebei Province (Grant No. A2022210002).

References

[1] Shamir A 1979 *Commun. ACM* **22** 612
[2] Blakley G R 1979 *In Proceedings of the 1979 International Workshop on Managing Requirements Knowledge (MARK)*, New York, NY, USA, 4–7 June 1979; Volume 48, pp. 313–317
[3] Hillery M, Buzek V and Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[4] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[5] Gottesman D 2000 *Phys. Rev. A* **61** 042311
[6] Xiao L, Long G L, Deng F G and Pan J W 2004 *Phys. Rev. A* **69** 052307
[7] Grice W P and Qi B 2019 *Phys. Rev. A* **100** 022339
[8] Qin H W, Zhu X H and Dai Y W 2015 *Quantum Inf. Process* **14** 2997
[9] Lipinska V, Murta G, Ribeiro J and Wehner S 2020 *Phys. Rev. A* **101** 032332
[10] Gu J, Cao X Y, Yin H L, *et al.* 2021 *Opt. Express* **29** 9165
[11] Mashhadi S 2022 *Journal of Applied Security Research* **17** 123
[12] Li F, Chen T and Zhu S 2022 *Physica A* **606** 128122
[13] Li F, Luo M, Zhu H, *et al.* 2023 *Physica A* **612** 128494
[14] Li L and Li Z 2023 *Entropy* **25** 265
[15] Xu J, Li X, Han Y, *et al* 2023 *Frontiers in Physics* **11** 1213153
[16] Wang J, Li L, Peng H and Yang Y 2017 *Phys. Rev. A* **95** 022320
[17] Tavakoli A, Herbauts I, Zukowski M and Bourennane M 2015 *Phys. Rev. A* **92** 030302
[18] Qin H and Dai Y 2016 *Information Processing Letters* **116** 351
[19] Bai C M, Zhang S and Liu L 2021 *International Journal of Theoretical Physics* **60** 3993
[20] Liu S, Lu Z, Wang P, *et al.* 2023 *npj Quantum Information* **9** 92
[21] Shen A, Cao X Y, Wang Y, *et al.* 2023 *Science China Physics, Mechanics & Astronomy* **66** 260311
[22] Li C L, Fu Y, Liu W B, *et al.* 2023 *Phys. Rev. Research* **5** 033077
[23] Gu J, Xie Y M, Liu W B, *et al.* 2021 *Opt. Express* **29** 32244
[24] Guo G P and Guo G C 2003 *Phys. Lett. A* **310** 247
[25] Hsu L Y, Li C M 2005 *Phys. Rev. A* **71** 022321
[26] Yang Y G, Wen Q Y and Zhu F C 2007 *Sci. China Ser. G* **50** 331
[27] Hu W, Zhou R G and Luo J 2022 *Chin. J. Phys.* **77** 1701
[28] Xu G B, Wen Q Y, Gao F, Qin S J and Zuo H J 2017 *Quantum Inf. Process* **16** 1
[29] Feng Y and Shi Y 2009 *IEEE transactions on information theory* **55** 2799
[30] Xu G B, Wen Q Y, Qin S J, Yang Y H and Gao F 2016 *Phys. Rev. A* **93** 032341
[31] Zhen X F, Fei S M and Zuo H J 2022 *Phys. Rev. A* **106** 062432
[32] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[33] Li C Y, Zhou H Y, Wang Y and Deng F G 2005 *Chin. Phys. Lett.* **22** 1049
[34] Walgate J and Hardy L 2002 *Phys. Rev. Lett.* **89** 147901
[35] Li C Y, Li X H, Deng F G, *et al.* 2006 *Chin. Phys. Lett.* **23** 2896
[36] Karimipour V, Asoudeh M, Gheorghiu V, Looi S Y and Griffiths R B 2015 *Phys. Rev. A* **92** 030301