frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 19 June 2023
DOI 10.3389/fphy.2023.1213153

Quantitative security analysis of three-level unitary operations in quantum secret sharing without entanglement

Juan Xu[1,2]*, Xi Li[3], Yunguang Han[1,2], Yuqian Zhou[1,2], Zhihao Liu[3,4], Zhengye Zhang[1] and Yinxiu Song[1]

[1]College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China, [2]Collaborative Innovation Center of Novel Software Technology and Industrialization, Nanjing, China, [3]School of Computer Science and Engineering, Southeast University, Nanjing, China, [4]Key Laboratory of Computer Network and Information Integration, Ministry of Education, Southeast University, Nanjing, China

OPEN ACCESS

EDITED BY
Weibin Li,
University of Nottingham,
United Kingdom

REVIEWED BY
Lihua Gong,
Nanchang University, China
Su-Juan Qin,
Beijing University of Posts and
Telecommunications (BUPT), China

*CORRESPONDENCE
Juan Xu,
juanxu@nuaa.edu.cn

RECEIVED 27 April 2023
ACCEPTED 23 May 2023
PUBLISHED 19 June 2023

CITATION
Xu J, Li X, Han Y, Zhou Y, Liu Z, Zhang Z and Song Y (2023), Quantitative security analysis of three-level unitary operations in quantum secret sharing without entanglement.
Front. Phys. 11:1213153.
doi: 10.3389/fphy.2023.1213153

Quantum secret sharing (QSS) protocols without entanglement have showed high security by virtue of the characteristics of quantum mechanics. However, it is still a challenge to compare the security of such protocols depending on quantitative security analysis. Based on our previous security analysis work on protocols using single qubits and two-level unitary operations, QSS protocols with single qutrits and three-level unitary operations are considered in this paper. Under the Bell-state attack we propose, the quantitative security analyses according to different three-level unitary operations are provided respectively in the one-step and two-step situations. Finally, important conclusions are drawn for designing and implementing such QSS protocols. The method and results may also contribute to analyze the security of other high-level quantum cryptography schemes based on unitary operations.

KEYWORDS

quantum cryptography, quantum secret sharing, three-level unitary operation, quantitative security analysis, qutrit

1 Introduction

Quantum secret sharing (QSS) is an important branch of quantum cryptography, whose security is based on the fundamental principle of quantum mechanics. It can share both the classical message [1–11] and quantum information [12–22]. Taking QSS protocols for classical message sharing into account, it is observed that it is a more efficient and lower cost way to use single particles instead of entangled particles. In addition, to achieve the unconditional security (in theory) and the ability of detecting eavesdropping, unitary operations are always used in such protocols. The classical secret message is encoded into quanta and/or scrambles the particles by unitary operations so that the eavesdropper cannot reliably identify each quantum state by appropriate measurement.

The quantitative security analysis of such protocols can be transformed into a quantitative calculation of unitary operation security. The feasibility of this idea has been proven by our pioneering work [23]. In [23], we proposed the substitute-Bell-state attack and the definition of minimum failure probability for the attack. Thus, the quantitative security analysis can be conducted according to the different selection methods of unitary

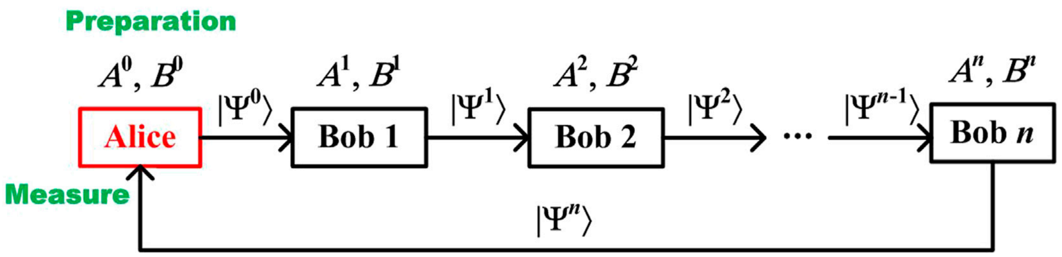

FIGURE 1
A general QSS protocol based on single states. Binary string A^0 is the secret, and B^0 is a random string. Alice prepares, transform, and finally measures the single qutrits, while Bob 1 to Bob n only do local unitary operations on these qutrits according to A^i and B^i.

operations. Several cases of two-level unitary operations were analyzed in [23] and more two-level cases are considered in our recent research [24].

However, these works on the security analysis of QSS are focused on the qubit system. In many scenarios, quantum communication protocols using high-dimensional states demonstrate larger capacity and better performance than the qubit system. Thus, it is worth studying the security of QSS protocols beyond the two-level system. Quantitative security analysis of QSS protocols remains a tough problem, and our pioneering idea is worth recommending. However, the research work based on this idea is not sufficient. In this paper, the security of QSS protocols using three-level unitary operations is analyzed quantitatively, and some comparisons between two-level and three-level situations are made. Finally, valuable conclusions are obtained, which can guide the designing and implementation of QSS protocols with single qutrits.

2 The security of unitary operations in quantum secret sharing protocols based on qutrits

2.1 Three-level Bell states and unitary operations

In a three-level quantum system, we call a single quantum state as a *qutrit*. The Z-basis of a three-level quantum system is $\{|0\rangle, |1\rangle, |2\rangle\}$, and another basis can be constructed by a quantum Fourier transform, which is called the X-basis. For an arbitrary d-level quantum system, we have

$$|X_k\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1} e^{2\pi ijk/d}|j\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1} \varpi^{jk}|j\rangle, \tag{1}$$

where $0 \le k \le d-1, \varpi = e^{2\pi i/d}$. So when $d = 3$, the X-basis can be formed as follows:

$$\{|x_0\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle), |x_1\rangle = \frac{1}{\sqrt{3}}(|0\rangle + w|1\rangle + w^2|2\rangle), |x_2\rangle = \frac{1}{\sqrt{3}}(|0\rangle + w^2|1\rangle + w|2\rangle)\}, \tag{2}$$

where $w = e^{2\pi i/3}$.

To analyze the security of QSS protocols based on qutrits quantitatively, we design the Bell-state attack, which uses three-level Bell states and unitary operations. In a $d \times d$-level double quantum system, the d-level Bell state can be denoted as

$$|\psi_{nm}\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1} w^{jn}|j\rangle|j+m\rangle, \tag{3}$$

where $w = e^{2\pi i/3}$, $d \ge 2$, $0 \le n, m \le d-1$, and the symbol '+' means module d plus. Obviously, there are d^2 d-level Bell states. In addition, the vector group $\{|\psi_{nm}\rangle\}$ constitutes a complete orthogonal basis of the double quantum system. Thus, nine Bell states forming a complete orthogonal basis in a three-level quantum system can be specified as

$$\begin{aligned}
|\psi_{00}\rangle &= \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle),\\
|\psi_{01}\rangle &= \frac{1}{\sqrt{3}}(|01\rangle + |12\rangle + |20\rangle),\\
|\psi_{02}\rangle &= \frac{1}{\sqrt{3}}(|02\rangle + |10\rangle + |21\rangle),\\
|\psi_{10}\rangle &= \frac{1}{\sqrt{3}}(w|00\rangle + w^2|11\rangle + |22\rangle),\\
|\psi_{11}\rangle &= \frac{1}{\sqrt{3}}(w|01\rangle + w^2|12\rangle + |20\rangle),\\
|\psi_{12}\rangle &= \frac{1}{\sqrt{3}}(w|02\rangle + w^2|10\rangle + |21\rangle),\\
|\psi_{20}\rangle &= \frac{1}{\sqrt{3}}(w^2|00\rangle + w|11\rangle + |22\rangle),\\
|\psi_{21}\rangle &= \frac{1}{\sqrt{3}}(w^2|01\rangle + w|12\rangle + |20\rangle),\\
|\psi_{22}\rangle &= \frac{1}{\sqrt{3}}(w^2|02\rangle + w|10\rangle + |21\rangle).
\end{aligned} \tag{4}$$

Without loss of generality, the first Bell state $|\psi_{00}\rangle = (1/\sqrt{3})(|00\rangle + |11\rangle + |22\rangle)$ is chosen to be the initial state that the eavesdropper uses for a Bell-state attack. Furthermore, an arbitrary three-level double quantum state can be expressed as follows:

$$|ab\rangle = (x_1|\psi_{00}\rangle + x_2|\psi_{10}\rangle + x_3|\psi_{20}\rangle + y_1|\psi_{01}\rangle + y_2|\psi_{11}\rangle + y_3|\psi_{21}\rangle + z_1|\psi_{02}\rangle + z_2|\psi_{12}\rangle + z_3|\psi_{22}\rangle), \tag{5}$$

where $x_i, y_i, z_i \in \mathbb{C}$ $(i = 1, 2, 3)$.

A unitary operation is a bounded linear operation U: $H \to H$ on a Hilbert space H that satisfies $UU^* = I$, where U^* is the adjoint of U and I: $H \to H$ is the identity operation. In a three-level system, the unitary operations can be represented by a 3*3 matrix. For simplicity, we consider the double quantum states consisting of three basis states, that is, one of x_1, x_2, and x_3; y_1, y_2, and y_3; or z_1, z_2, and z_3 is 1 (see Formula 5). Here, $x_i = 1$ is bound to $y_i = 0$ and $z_i = 0$ because the two-qutrit quantum state is obtained under a Bell-state attack and selected unitary operation (see Section 2.3). Therefore, there will be six situations showed as follows (if the unitary matrix at the left side of the arrow is supposed to be used in a Bell-state attack, three Bell states will be obtained at the right side of the arrow):

$$\begin{aligned}
\boldsymbol{U_{01}} &= \frac{\mathbf{1}}{\sqrt{\mathbf{3}}}\begin{pmatrix} \mathbf{1} & \boldsymbol{w} & \mathbf{1} \\ \boldsymbol{w} & \mathbf{1} & \mathbf{1} \\ \boldsymbol{w}^2 & \boldsymbol{w}^2 & \mathbf{1} \end{pmatrix} \to |\psi_{00}\rangle, |\psi_{11}\rangle, |\psi_{22}\rangle, \\
\boldsymbol{U_{02}} &= \frac{\mathbf{1}}{\sqrt{\mathbf{3}}}\begin{pmatrix} \mathbf{1} & \boldsymbol{w}^2 & \mathbf{1} \\ \boldsymbol{w}^2 & \mathbf{1} & \mathbf{1} \\ \boldsymbol{w} & \boldsymbol{w} & \mathbf{1} \end{pmatrix} \to |\psi_{00}\rangle, |\psi_{12}\rangle, |\psi_{21}\rangle, \\
\boldsymbol{U_{03}} &= \frac{\mathbf{1}}{\sqrt{\mathbf{3}}}\begin{pmatrix} \boldsymbol{w} & \boldsymbol{w} & \mathbf{1} \\ \mathbf{1} & \boldsymbol{w}^2 & \mathbf{1} \\ \boldsymbol{w}^2 & \mathbf{1} & \mathbf{1} \end{pmatrix} \to |\psi_{10}\rangle, |\psi_{01}\rangle, |\psi_{22}\rangle, \\
\boldsymbol{U_{04}} &= \frac{\mathbf{1}}{\sqrt{\mathbf{3}}}\begin{pmatrix} \boldsymbol{w} & \mathbf{1} & \mathbf{1} \\ \boldsymbol{w}^2 & \boldsymbol{w}^2 & \mathbf{1} \\ \mathbf{1} & \boldsymbol{w} & \mathbf{1} \end{pmatrix} \to |\psi_{10}\rangle, |\psi_{02}\rangle, |\psi_{21}\rangle, \\
\boldsymbol{U_{05}} &= \frac{\mathbf{1}}{\sqrt{\mathbf{3}}}\begin{pmatrix} \boldsymbol{w}^2 & \boldsymbol{w}^2 & \mathbf{1} \\ \mathbf{1} & \boldsymbol{w} & \mathbf{1} \\ \boldsymbol{w} & \mathbf{1} & \mathbf{1} \end{pmatrix} \to |\psi_{20}\rangle, |\psi_{01}\rangle, |\psi_{12}\rangle, \\
\boldsymbol{U_{06}} &= \frac{\mathbf{1}}{\sqrt{\mathbf{3}}}\begin{pmatrix} \boldsymbol{w}^2 & \mathbf{1} & \mathbf{1} \\ \boldsymbol{w} & \boldsymbol{w} & \mathbf{1} \\ \mathbf{1} & \boldsymbol{w}^2 & \mathbf{1} \end{pmatrix} \to |\psi_{20}\rangle, |\psi_{02}\rangle, |\psi_{11}\rangle.
\end{aligned} \tag{6}$$

Without the loss of generality, we select the first situation as an example for research.

Next, to measure the security of different unitary operations, we first provide a general QSS protocol based on qutrits, and then propose the so-called Bell-state attack and state the minimum failure probability for this attack. The quantitative computing results show how to select appropriate three-level unitary operations to protect the QSS protocols against a Bell-state attack.

2.2 A general quantum secret sharing protocol based on qutrits

A generic QSS protocol based on qutrits is shown in Figure 1 (it is supposed to be a (n, n) secret sharing threshold protocol). The procedure is as follows:

(1) First, Alice prepares qutrits all in $|0\rangle$. A binary string A^0 is the secret to be shared. Alice performs unitary operations on qutrits according to the value of A^0 and a random string B^0 (to be used to change the basis).
(2) After that, the qutrit sequence, denoted as $|\Psi^0\rangle$, is sent to Bob 1.
(3) Bob 1 to Bob n perform local three-level unitary operations according to the values of A and B.
(4) Bob n sends the qutrits back to Alice. Then, Bob 1 to Bob n declare the information about individual unitary operations (not unitary operations themselves) via classical communication.
(5) Alice measures the qutrits using proper bases according to the information and publishes the result.
(6) Only when all the Bobs collaborate together, the secret can be revealed. Sample detection can be implemented by classical communication to judge if there is a wiretap.

In addition, unitary operations can be executed in one or two steps, which were defined in our previous work, shown as follows [23].

Definition 1. (one-step unitary operation): Bob i performs *once* a random local unitary operation on each quantum state before sending. All possible options are put into "{}", called a unitary operation set.

Definition 2. (two-step unitary operation): Bob i performs *twice* a random local unitary operation on each quantum state before sending, and the probability of the first and second operations being the same is *zero*. The symbol "{; }" is used to indicate the two-step unitary operation, while the first possible options are listed before the semicolon, and the subsequent options, after the semicolon.

2.3 Bell-state attack in a three-level quantum system

Bob i is supposed to be dishonest during the execution of the three-level QSS protocol. He aims to generate a Bell-state attack to obtain the integrated encoded information from Bob i+1 to Bob j. The schematic diagram of the Bell-state attack is illustrated in Figure 2 (which is a variant of the substitute-Bell-state attack [23]), and the procedure of the attack is as follows:

(1) Bob i retains the single qutrits $|\Psi^{i-1}\rangle$ sent from Bob i-1 and does nothing on these particles. Meanwhile, he generates N three-level Bell states $|\Phi\rangle_{12} = \otimes_{k=1}^{N} |\phi_k\rangle_{12}$. $|\phi_k\rangle_{12}$ can be any one of the nine Bell states given in Formula 4. Without the loss of generality, $|\phi_k\rangle$ is assumed to be $|\psi_{00}\rangle = (1/\sqrt{3})(|00\rangle + |11\rangle + |22\rangle)$.
(2) Bob i transmits the second particles $|\Phi\rangle_2$ of the Bell states to Bob $i+1$ and retains the first particles $|\Phi\rangle_1$.
(3) Bob i intercepts the single qutrits $|\Psi^{i+1}\rangle$ sent from Bob j to Bob j +1 and replaces it with $|\Psi^{i-1}\rangle$.
(4) The particle sequences $|\Phi\rangle_1$ and $|\Psi^j\rangle$ are combined in pairs by Bob i to form new N Bell states $|\Phi'\rangle_{12} = \otimes_{k=1}^{N} |\phi_k'\rangle_{12}$. Then, Bob i measures the new Bell states by proper bases in order to obtain integrated encoded information from Bob i+1 to Bob j.
(5) When samples are tested, Bob i claims the unitary operations that are consistent with the comprehensive effect of the unitary

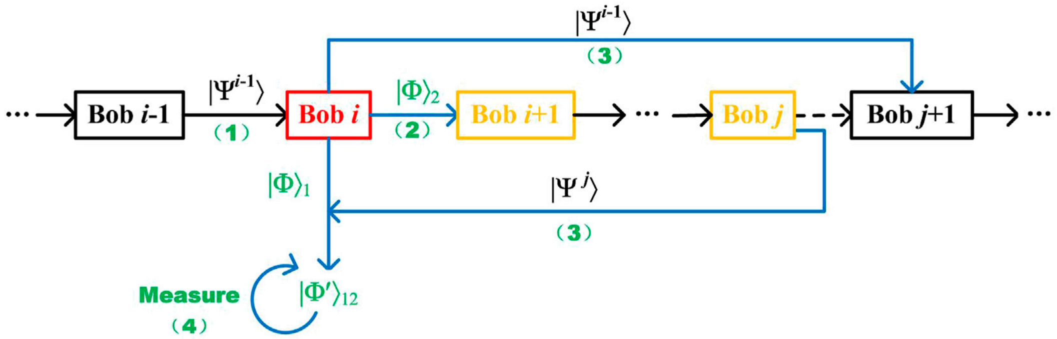

FIGURE 2
Schematic diagram of Bell-state attack from Bob i for the integrated encoding information from Bob i+1 to Bob j. $|\Phi\rangle_1$and $|\Phi\rangle_2$ are the two particles of the Bell states Bob i generates. Bob i intercepts and captures $|\Psi^j\rangle$ sent from Bob j to Bob j+1, and replaces it by $|\Psi^{i-1}\rangle$. $|\Phi\rangle_1$and $|\Psi^j\rangle$ are combined to form new Bell states $|\Phi'\rangle_{12}$.

operations that Bob i +1, Bob i +2, . . ., and Bob j implemented, to avoid the attack from being detected.

It should be noted that Bob j can also be Bob i+1, and in this situation, Bob i aims only to obtain the unitary operations that Bob i +1 has performed.

Now, the key question is how to measure the effect of the Bell-state attack? To determine this, we pick up the minimum failure probability formula that we put forward previously [23, 24].

Definition 3. **(minimum failure probability)**: Assume that a QSS protocol based on single qutrits is under a Bell-state attack. The attacker has acquired N new two-qutrit states $|\phi_k\rangle$. Suppose the prior probability of $|\phi_k\rangle$ is p_k, and the number of quantum states to be distinguished is n. Thus, the minimum failure probability of the Bell-state attack (denoted as F_{min}) is defined as follows:

$$F_{min} = \frac{1}{n-1}\sum_{i\neq j}\sqrt{p_i p_j}\left|\langle\phi_i|\phi_j\rangle\right|. \tag{7}$$

Apparently, F_{min} equals to 1 minus the maximum probability of reliably distinguishing different quantum states. The value of F_{min} is between 0 and 1. When $F_{min} = 0$, the protocol is totally unsecure. In other words, all the states are mutually orthogonal; Bob i could definitely distinguish each state by proper measurement and interpret all encoded information successfully. It should be noted that $F_{min} \neq 1$ because if $F_{min} = 1$, the states to be distinguished must be the same, and this is impossible in QSS protocols.

Therefore, when F_{min} is larger, the effective information that a Bell-state attack can gain is less, that is, the QSS protocol is verified to be safer and vice versa.

2.4 The security of one-step three-level unitary operations

To research the security of three-level unitary operations under a Bell-state attack, we first provide the nine unitary operations corresponding to nine Bell states (shown in Formula 4) in Formula 8. In other words, the nine Bell states can be obtained when the second qutrit of the initial state $|\Phi\rangle_{12} = |\psi_{00}\rangle = (1/\sqrt{3})(|00\rangle + |11\rangle + |22\rangle)$ is affected individually by the nine unitary operations and recombined with the first qutrit.

$$\begin{aligned}
X_1 &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, X_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, X_3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \\
X_4 &= \begin{pmatrix} w & 0 & 0 \\ 0 & w^2 & 0 \\ 0 & 0 & 1 \end{pmatrix}, X_5 = \begin{pmatrix} 0 & 0 & 1 \\ w & 0 & 0 \\ 0 & w^2 & 0 \end{pmatrix}, X_6 = \begin{pmatrix} 0 & w^2 & 0 \\ 0 & 0 & 1 \\ w & 0 & 0 \end{pmatrix}, \\
X_7 &= \begin{pmatrix} w^2 & 0 & 0 \\ 0 & w & 0 \\ 0 & 0 & 1 \end{pmatrix}, X_8 = \begin{pmatrix} 0 & 0 & 1 \\ w^2 & 0 & 0 \\ 0 & w & 0 \end{pmatrix}, X_9 = \begin{pmatrix} 0 & w & 0 \\ 0 & 0 & 1 \\ w^2 & 0 & 0 \end{pmatrix},
\end{aligned} \tag{8}$$

where $w = e^{2\pi i/3}$.

Moreover, without the loss of generality, U_{01} (shown in Formula 6), X_1, X_5, and X_9 are chosen as the three-level unitary operations in QSS protocols for encoding the message and/or scrambling states, relabeled as

$$\begin{aligned}
U_0 &= U_{01} = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & w & 1 \\ w & 1 & 1 \\ w^2 & w^2 & 1 \end{pmatrix}, U_1 = X_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \\
U_2 &= X_5 = \begin{pmatrix} 0 & 0 & 1 \\ w & 0 & 0 \\ 0 & w^2 & 0 \end{pmatrix}, U_3 = X_9 = \begin{pmatrix} 0 & w & 0 \\ 0 & 0 & 1 \\ w^2 & 0 & 0 \end{pmatrix}.
\end{aligned} \tag{9}$$

It should be noted that U_0 can transform a qutrit between the X-basis and Z-basis.

Here is the explanation of why X_1, X_5, and X_9 are chosen as U_1, U_2, and U_3, respectively. When U_{01} is chosen, we get $|\Phi\rangle_1(U_{01}|\Phi\rangle_2) = (1/\sqrt{3})(|\psi_{00}\rangle + |\psi_{11}\rangle + |\psi_{22}\rangle)$. So we select preferentially the unitary operations leading to the states that are not orthogonal to $|\Phi\rangle_1(U_{01}|\Phi\rangle_2)$. It is easy to find that selecting X_1, X_5, and X_9 is optimal, which leads to $|\psi_{00}\rangle$, $|\psi_{11}\rangle$, and $|\psi_{22}\rangle$, and the maximum value of F_{min}. On the contrary, if other unitary operations are selected, the denominator of Formula 9 remains unchanged, while the numerator decreases, that is, F_{min} decreases and the security reduces.

Finally, there are seven sets of one-step three-level unitary operations corresponding to the aforementioned matrices, and the minimum failure probability F_{min} of each set is calculated and shown in Table 1.

From Table 1, we can conclude the following:

(1) If the four unitary operations of U_0, U_1, U_2, and U_3 are chosen for the quantum secret sharing process, only three values of the minimum failure probability are available. In other words, $F_{min} = \sqrt{3}/3$ when two unitary operations are selected; $F_{min} = 2\sqrt{3}/9$ when three are selected; and $F_{min} = \sqrt{3}/6$ when all four are selected. In a word, in one-step three-level unitary operations, the fewer unitary operations the legitimate communicator selects, the larger F_{min} is and the higher the security of this QSS protocol is verified.

(2) Based on the aforementioned analysis, the minimum failure probability formula in a three-level quantum system can be simplified as follows:

$$\boldsymbol{F_{min}} = \frac{\boldsymbol{2}}{\boldsymbol{\sqrt{3}N}}, \tag{10}$$

where N denotes the number of selected unitary operations. For the six situations listed in Formula 6, if we choose the other five situations and corresponding U_0 and X_i $(i = 1, 2, ..., 9)$, the same values of F_{min} will be attained, along with the same simplified formula of minimum failure probability.

TABLE 1 The minimum failure probability of Bell-state attack under one-step three-level unitary operations. The quantum states are obtained from the different transformations of initial state $|\psi_{00}\rangle = (1/\sqrt{3})(|00\rangle + |11\rangle + |22\rangle)$ under selected unitary operations. The curly braces of selected unitary operations, Dirac symbol and normalization of obtained quantum states are omitted.

Selected unitary Operations	Obtained quantum states	F_{min}
U_1, U_0	$\psi_{00}, \psi_{00} + \psi_{11} + \psi_{22}$	$\sqrt{3}/3$
U_2, U_0	$\psi_{11}, \psi_{00} + \psi_{11} + \psi_{22}$	$\sqrt{3}/3$
U_3, U_0	$\psi_{22}, \psi_{00} + \psi_{11} + \psi_{22}$	$\sqrt{3}/3$
U_1, U_2, U_0	$\psi_{00}, \psi_{11}, \psi_{00} + \psi_{11} + \psi_{22}$	$2\sqrt{3}/9$
U_1, U_3, U_0	$\psi_{00}, \psi_{22}, \psi_{00} + \psi_{11} + \psi_{22}$	$2\sqrt{3}/9$
U_2, U_3, U_0	$\psi_{11}, \psi_{22}, \psi_{00} + \psi_{11} + \psi_{22}$	$2\sqrt{3}/9$
U_1, U_2, U_3, U_0	$\psi_{00}, \psi_{11}, \psi_{22}, \psi_{00} + \psi_{11} + \psi_{22}$	$\sqrt{3}/6$

2.5 The security of two-step three-level unitary operations

The one-step unitary operation case is mentioned previously. We try the similar analysis in a two-step unitary operation instance.

First of all, according to the definition of a two-step unitary operation and the selected four unitary operations U_0, U_1, U_2, and U_3, all combinations can be divided into four categories as follows:

$$1.\ U_0;\begin{cases} U_1, U_2\,(3) \\ U_1, U_2, U_3\,(1) \\ U_1, U_0\,(3) \\ U_1, U_2, U_0\,(3) \\ U_1, U_2, U_3, U_0\,(1) \end{cases} \Longrightarrow 11 \text{ combinations;}$$

$$2.\ \begin{matrix} U_1, U_0 \\ \times 3 \end{matrix};\begin{cases} U_1\,(3) \\ U_1, U_2\,(3) \\ U_1, U_2, U_3\,(1) \\ U_2, U_0\,(2) \\ U_1, U_2, U_0\,(3) \\ U_1, U_2, U_3, U_0\,(1) \end{cases} \Longrightarrow 13 \times 3 = 39 \text{ combinations;}$$

$$3.\ \begin{matrix} U_1, U_2, U_0 \\ \times 3 \end{matrix};\begin{cases} U_1\,(3) \\ U_1, U_2\,(3) \\ U_1, U_2, U_3\,(1) \\ U_1, U_3, U_0\,(2) \\ U_1, U_2, U_3, U_0\,(1) \end{cases} \Longrightarrow 10 \times 3 = 30 \text{ combinations;}$$

$$4.\ U_1, U_2, U_3, U_0;\begin{cases} U_1\,(3) \\ U_1, U_2\,(3) \\ U_1, U_2, U_3\,(1) \end{cases} \Longrightarrow 7 \text{ combinations.}$$

Here, the first possible unitary operations are listed before the semicolon, and the subsequent operations, after the semicolon; the symbol "× 3" means that there are three similar unitary operation combinations in the first step; the symbol "(3)" denotes that there are three similar unitary operation combinations in the second step. For example, in the first category, "$U_1, U_2\,(3)$" indicates that there are three similar combinations, that is, $\{U_1, U_2\}$, $\{U_1, U_3\}$, and $\{U_2, U_3\}$. In short, there are totally $11 + 39 + 30 + 7 = 87$ combinations.

Second, we provide the states after continuous action of two unitary operations (shown in Table 2), supposing the initial state is $|\psi_{00}\rangle = (1/\sqrt{3})(|00\rangle + |11\rangle + |22\rangle)$. If the two unitary operations are executed in an opposite order, the same state is obtained. So there are totally 10 results, as shown in Table 2. In addition, α_{ij} $(i, j = 0, 1, 2, 3)$ denotes the obtained state after the two unitary operations, where the subscripts i and j represent the corresponding unitary operations U_i and U_j.

Third, to calculate $F_{min} = \frac{1}{n-1}\sum_{i\neq j}\sqrt{p_i p_j}|\langle\phi_i|\phi_j\rangle|$, we first calculate the norm of the inner product of the two quantum states, that is, $|\langle\phi_i|\phi_j\rangle|$ $(i \neq j)$. The results are shown in Table 3.

From Table 3 we can see that the inner product values are symmetric about the diagonal and the inner product values between α_{01}, α_{02} and α_{03} is 0. So the four combinations in the first category with "$U_1, U_2\,(3)$" and "$U_1, U_2, U_3\,(1)$" in the second step can be omitted. Therefore, there are totally $87 - 4 = 83$ combinations, which are divided into 18 situations, and the values of F_{min} are shown in Table 4.

From Table 4, it can be seen that the values of F_{min} are the same separately in cases 1 and 4; in cases 2, 5, and 10; and in cases 3 and 16. So it can be merged into 14 cases. Thus, the values of F_{min} (accurate to four decimal places) and the number of unitary operation sets corresponding to each value are shown in Table 5.

The results in Table 5 are also illustrated in Figure 3 for clarity. Then, some conclusions can be drawn based on the results.

(1) Among the two-step three-level unitary operations, the minimum failure probability of the Bell-state attack densely distributed between [0.34, 0.39], totally 48 sets, and there are 17 sets between [0.24, 0.29]. Furthermore, 12 sets have the highest value of F_{min}, that is, $\sqrt{3}/3 \approx 0.58$, and 6 sets have the second highest value of $F_{min} = 5\sqrt{3}/18 \approx 0.48$.

(2) The sets that have the highest value of F_{min} are $\{U_0; U_i, U_0\}$ and $\{U_i, U_0; U_i\}$ $(i = 1, 2, 3)$. This means the sets possessing the least

TABLE 2 The states after continuous action of two unitary operations. The two subscripts of α correspond to subscripts of the two used unitary operations.

Two used unitary operations	Obtained quantum state	Two used unitary operations	Obtained quantum state
U_0, U_0	$\alpha_{00} = (1/3)[(2w^2+1)\psi_{00} + (w+2)\psi_{11} + (w+2)\psi_{22}]$	U_1, U_2	$\alpha_{12} = \psi_{11}$
U_0, U_1	$\alpha_{01} = (1/\sqrt{3})[\psi_{00} + \psi_{11} + \psi_{22}]$	U_1, U_3	$\alpha_{13} = \psi_{22}$
U_0, U_2	$\alpha_{02} = (1/\sqrt{3})[w^2\psi_{00} + \psi_{11} + w\psi_{22}]$	U_2, U_2	$\alpha_{22} = w^2\psi_{22}$
U_0, U_3	$\alpha_{03} = (1/\sqrt{3})[w^2\psi_{00} + w\psi_{11} + \psi_{22}]$	U_2, U_3	$\alpha_{23} = w^2\psi_{00}$
U_1, U_1	$\alpha_{11} = \psi_{00}$	U_3, U_3	$\alpha_{33} = w\psi_{11}$

TABLE 3 The norm of inner product of the two quantum states. The inner product values are symmetric about the diagonal.

	α_{00}	α_{01}	α_{02}	α_{03}	α_{11}	α_{12}	α_{13}	α_{22}	α_{23}	α_{33}
α_{00}		$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$
α_{01}	$1/\sqrt{3}$		0	0	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$
α_{02}	$1/\sqrt{3}$	0		0	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$
α_{03}	$1/\sqrt{3}$	0	0		$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$
α_{11}	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$		0	0	0	1	0
α_{12}	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	0		0	0	0	1
α_{13}	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	0	0		1	0	0
α_{22}	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	0	0	1		0	0
α_{23}	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	1	0	0	0		0
α_{33}	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	$1/\sqrt{3}$	0	1	0	0	0	

TABLE 4 The values of F_{min} and the corresponding numbers of unitary operation sets. All the 83 non zero combinations are showed in 18 cases. The first-step possible unitary options are listed before the semicolon, and the second-step options after the semicolon.

Case	Typical unitary operations	Number of similar sets	F_{min}
1	$U_0; U_1, U_0$	3	$\sqrt{3}/3$
2	$U_0; U_1, U_2, U_0$	3	$2\sqrt{3}/9$
3	$U_0; U_1, U_2, U_3, U_0$	1	$\sqrt{3}/6$
4	$U_1, U_0; U_1$	9	$\sqrt{3}/3$
5	$U_1, U_0; U_1, U_2$	9	$2\sqrt{3}/9$
6	$U_1, U_0; U_1, U_2, U_3$	3	$\sqrt{3}/5$
7	$U_1, U_0; U_2, U_0$	6	$5\sqrt{3}/18$
8	$U_1, U_0; U_1, U_2, U_0$	9	$(5\sqrt{3} + 3\sqrt{6})/45$
9	$U_1, U_0; U_1, U_2, U_3, U_0$	3	$(11\sqrt{3} + 4\sqrt{6})/84$
10	$U_1, U_2, U_0; U_1$	9	$2\sqrt{3}/9$
11	$U_1, U_2, U_0; U_1, U_2$	3	$(4\sqrt{3} + 2\sqrt{6})/45$
12	$U_1, U_2, U_0; U_1, U_3$	6	$(8\sqrt{3} + 3)/45$
13	$U_1, U_2, U_0; U_1, U_2, U_3$	3	$(3\sqrt{3} + 1 + \sqrt{6})/36$
14	$U_1, U_2, U_0; U_1, U_3, U_0$	6	$(14\sqrt{3} + 3 + 5\sqrt{6})/108$
15	$U_1, U_2, U_0; U_1, U_2, U_3, U_0$	3	$(13\sqrt{3} + 3 + 12\sqrt{6})/198$
16	$U_1, U_2, U_3, U_0; U_1$	3	$\sqrt{3}/6$
17	$U_1, U_2, U_3, U_0; U_1, U_2$	3	$(8\sqrt{3} + 3 + 2\sqrt{6})/84$
18	$U_1, U_2, U_3, U_0; U_1, U_2$	1	$(3\sqrt{3} + 3\sqrt{6} + 3\sqrt{2})/66$

TABLE 5 The values of F_{min} and the corresponding numbers of unitary operation sets when the values in Table 4 are accurate to four decimal places. Thus 18 cases are merged to 14 cases.

F_{min}	Number of sets	F_{min}	Number of sets
0.5774	12	0.2402	3
0.3657	6	0.3849	21
0.2887	4	0.3464	3
0.2544	1	0.2628	3
0.4811	6	0.3746	6
0.3557	9	0.3435	3
0.2773	3	0.2590	3

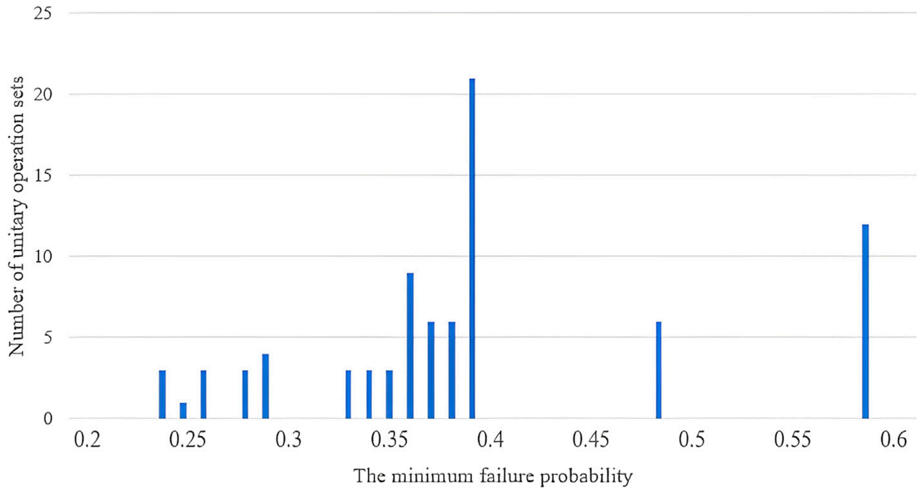

FIGURE 3
The minimum failure probability of two-step three-level unitary operations. The values of F_{min} are accurate to four decimal places and three are totally 84 unitary operation sets.

selected operations have the highest security, except for $\{U_0; U_1, U_2\}$, $\{U_0; U_1, U_3\}$, and $\{U_0; U_2, U_3\}$ whose $F_{min} = 0$. This is similar to the two-level unitary operation situation [24].

(3) Among the six situations shown in Formula 6, if another situation is selected, that is, another Bell-state combination and corresponding U_0 and X_i (i = 1, 2, ⋯, 9) are selected, the similar calculation process and conclusions will be obtained because their mutual relationship is consistent with the first situation.

2.6 The selection of three-level unitary operations

Based on the quantitative computing results and analysis on one-step and two-step unitary operations in a three-level system, the selection rules of unitary operations are summarized as follows:

(1) The unitary operations in QSS protocols based on qutrits should be chosen carefully. **First**, the unitary operations whose F_{min} is 0 should not be chosen since the protocol is obviously insecure in such a situation. **Second**, the unitary operation to transform the basis is a *necessary* but *not a sufficient condition* for the security. In other words, the unitary operation like U_0 can change the basis; so if U_0 is not selected, the QSS protocol is totally insecure. However, although U_0 is the possible choice, the security of the protocol still cannot be guaranteed. For example, F_{min} of $\{U_0; U_1, U_2\}$, $\{U_0; U_1, U_3\}$, $\{U_0; U_2, U_3\}$, and $\{U_0; U_1, U_2, U_3\}$ is 0.

(2) More complex unitary operations cannot be counted on to generate higher security. In a one-step unitary operation, Max $[F_{min}\ (U_1, U_2, \ldots, U_i)]$ > Max $[F_{min}\ (U_1, U_2, \ldots, U_i, U_{i+1})]$, that is, fewer unitary operations lead to larger F_{min} and higher security of the QSS protocol. The two-step unitary operation has the similar situation. This is because in one-step scene, the more the unitary operations, the more the pairwise non-orthogonal quantum states obtained.

(3) When the same unitary operations are selected, the security of two-step unitary operations is not necessarily higher than that of

one-step unitary operations. There exist possibilities. For example, F_{min} $(\{U_0, U_1, U_2\})$ = F_{min} $(\{U_0;\, U_0, U_1, U_2\})$ ≈ 0.38; F_{min} $(\{U_0, U_1, U_2\}) \approx 0.38 <$ F_{min} $(\{U_0, U_1;\, U_0, U_2\})$ ≈ 0.48; F_{min} $(\{U_0, U_1, U_2\}) \approx 0.38 >$ F_{min} $(\{U_0, U_1, U_2;\, U_1, U_2\})$ ≈ 0.26. So we should choose the two-step unitary operations with the highest value of F_{min}.

(4) The maximum of F_{min} of the three-level unitary operations (≈ 0.58) is less than the maximum of F_{min} of the two-level unitary operations (≈ 0.71) [23, 24]. This does not mean that two-level unitary operations are safer than three-level unitary operations because the value of F_{min} is influenced by specified unitary operation types. We have restricted the types of two-level and three-level unitary operations, so this is just a comparison between two preset conditions.

In brief, we should choose the unitary operation sets that have a higher value of F_{min} to ensure the security of QSS protocols based on qutrits.

3 Conclusion

In this paper, we first present a general QSS protocol based on single qutrits, and then propose the Bell-state attack and the definition of minimum failure probability for the attack. In this way, QSS protocols based on single qutrits and three-level unitary operations are considered, and the quantitative security analysis is performed corresponding to different sets of four three-level unitary operations. The results show that the selection of unitary operations will significantly affect the security of such QSS protocols. As a result, some crucial rules for choosing unitary operations are given to ensure the security or achieve a higher security. This work can serve as an important guidance in designing and implementing QSS protocols based on single qutrits and three-level unitary operations. The method and results may also contribute to analyze the security of other high-level quantum cryptography protocols based on unitary operations, such as secure computation [25], quantum secure direct communication [26], quantum key agreement [27], quantum private query [28], and quantum oblivious transfer [29]. Furthermore, unitary operations are also used in other quantum algorithms, for example, the quantum blockchain algorithm [30] and quantum artificial intelligence algorithm [31], and it will be interesting in attempting to analyze their security using our method.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary Material; further inquiries can be directed to the corresponding author.

Author contributions

JX, XL, and ZL conceived the presented idea. YH and YZ verified the methods and developed the analyses. ZZ and YS completed the calculation. All authors contributed to the article and approved the submitted version.

Funding

This work is supported by the National Natural Science Foundation of China (Grant nos 62201252 and 62071240), the Innovation Program for Quantum Science and Technology (Grant no. 2021ZD0302900), and the Natural Science Foundation of Jiangsu Province, China (Grant no. BK20220804).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Matsumoto R. Message randomization and strong security in quantum stabilizer-based secret sharing for classical secrets. *Des Code Cryptogr* (2020) 88:1893–907. doi:10.1007/s10623-020-00751-w

2. Zhang Z, Li Y, Man Z. Multiparty quantum secret sharing. Phys Rev *A* (2005) 71: 044301. doi:10.1103/physreva.71.044301

3. Tavakoli A, Herbauts I, Zukowski M, Bourennane M. Secret sharing with a single d-level quantum system. *Phys Rev A* (2015) 92:030302. doi:10.1103/PhysRevA.92.030302

4. Karimipour V, Asoudeh M. Quantum secret sharing and random hopping: Using single states instead of entanglement. *Phys Rev A* (2015) 92:030301. doi:10.1103/PhysRevA.92.030301

5. Lin SS, Guo G, Xu Y, Sun Y, Liu X. Cryptanalysis of quantum secret sharing with d-level single particles. *Phys Rev A* (2016) 93:062343. doi:10.1103/PhysRevA.93.062343

6. Li Z, Li Q, Liu C, Peng Y, Chan WH. Limited resource semiquantum secret sharing. *Quan Inf Process* (2018) 17(10):285. doi:10.1007/s11128-018-2058-8

7. Tsai C, Chang Y, Lai Y, Yang CW. Cryptanalysis of limited resource semi-quantum secret sharing. *Quan Inf Process* (2020) 19(8):224–8. doi:10.1007/s11128-020-02690-w

8. Hu Z, Chen C, Zhang Z, Zhang H. Secure cooperative transmission for mixed RF/FSO spectrum sharing networks. *IEEE Trans Commun* (2020) 68(5):3010–23. doi:10.1109/tcomm.2020.2971483

9. Hu WW, Zhou RG, Li X, Fan P, Tan C. A novel dynamic quantum secret sharing in high-dimensional quantum system. *Quan Inf Process* (2021) 20:159–28. doi:10.1007/s11128-021-03103-2

10. Tian Y, Li J, Chen XB, Ye CQ, Li HJ. An efficient semi-quantum secret sharing protocol of specific bits. *Quan Inf Process* (2021) 20(6):217. doi:10.1007/s11128-021-03157-2

11. Tsai CW, Yang CW, Lin J. Multiparty mediated quantum secret sharing protocol. *Quan Inf Process* (2022) 21(2):63. doi:10.1007/s11128-021-03402-8

12. Dou Z, Xu G, Chen XB, Liu X, Yang YX. A secure rational quantum state sharing protocol. *Sci China Inf Sci* (2018) 61:022501. doi:10.1007/s11432-016-9151-x

13. Zha X, Jiang R, Wang M. Two schemes of multiparty quantum direct secret sharing via a six-particle GHZ state. *Commun Theor Phys* (2020) 72(2):025102. doi:10.1088/1572-9494/ab5d01

14. Wang J, Li L, Peng H, Yang Y. Quantum-secret-sharing scheme based on local distinguishability of orthogonal multiqudit entangled states. *Phys Rev A* (2017) 95: 022320. doi:10.1103/physreva.95.022320

15. Lipinska V, Murta G, Ribeiro J, Wehner S. Verifiable hybrid secret sharing with few qubits. *Phys Rev A* (2020) 101(3):032332. doi:10.1103/physreva.101.032332

16. Zhang K, Zhang X, Jia H, Zhang L. A new n-party quantum secret sharing model based on multiparty entangled states. *Quan Inf Process* (2019) 18(3):81. doi:10.1007/s11128-019-2201-1

17. Shi R. Useful equations about Bell states and their applications to quantum secret sharing. *IEEE Commun Lett* (2019) 24(2):386–90. doi:10.1109/lcomm.2019.2954134

18. Qin H, Wallace T, Raylin T. Hierarchical quantum secret sharing based on special high-dimensional entangled state. *IEEE J Sel Top Quant* (2020) 26(3):6600106. doi:10.1007/s11128-019-2571-4

19. Sutradhar K, Om H. Efficient quantum secret sharing without a trusted player. *Quan Inf Process* (2020) 19(2):73. doi:10.1007/s11128-019-2571-4

20. Habibidavijani M, Barry S. Continuous-variable ramp quantum secret sharing with Gaussian states and operations. *New J Phys* (2019) 21(11):113023. doi:10.1088/1367-2630/ab4d9c

21. Yang Y, Ga S, Li D, Zhou YH, Shi WM. Three-party quantum secret sharing against collective noise. *Quan Inf Process* (2019) 18(7):215. doi:10.1007/s11128-019-2319-1

22. Wang Y, Lou X, Fan Z, Wang S, Huang G. Verifiable multi-dimensional (t,n) threshold quantum secret sharing based on quantum walk. *Int J Theor Phys* (2022) 61(2):24.doi:10.1007/s10773-022-05009-w

23. Xu J, Chen H, Liu W, Liu Z. Selection of unitary operations in quantum secret sharing without entanglement. *Sci China Inf Sci* (2011) 54:1837–42. doi:10.1007/s11432-011-4240-9

24. Xu J, Xi L, Liu Z, Zhou Y, Han Y, Chen D, et al. *Quantitative security analysis of two-level unitary operations in quantum secret sharing protocols based on single qubits* (2023).

25. Tan X, Zhang X, Song T. Verifiable delegated quantum computation with χ-type entangled states. *Comput Stand Inter* (2017) 54:36–40. doi:10.1016/j.csi.2016.09.008

26. Zou Z, Zhou L, Zhong W, Sheng Y. Measurement-device-independent quantum secure direct communication of multiple degree of freedom of a single photon. *Sci China Phys Mech* (2020) 63:230362. doi:10.1007/s11433-019-1450-8

27. Li L, Li Z. A multi-party quantum key agreement protocol based on Shamir's secret sharing. *Intj Theor Phys* (2019) 58:3081–90. doi:10.1007/s10773-019-04187-4

28. Yang Y, Gao S, Li D, Zhou Y, Shi W. Three-party quantum secret sharing against collective noise. *Quan Inf Process* (2019) 18:215. doi:10.1007/s11128-019-2319-1

29. Zhang X, Wei C, Qin S, Gao F, Wen Q. Practical efficient 1-out-of-n quantum oblivious transfer protocol. *Quan Inf Process* (2023) 22(2):99. doi:10.1007/s11128-022-03817-x

30. Gao XX, Xu J, Fan JH. A novel quantum byzantine consensus protocol based on malicious node prevention mechanism. In: 2022 International Conference on Blockchain Technology and Information Security; July 15-17, 2022; Huaihua (2022).

31. Zhou NR, Zhang TF, Xie XW, Wu JY. Hybrid quantum-classical generative adversarial networks for image generation via learning discrete distribution. *SIGNAL Process-image* (2023) 110:116891. doi:10.1016/j.image.2022.116891