(t, n) Threshold Quantum Secret Sharing based on a Single d-level Quantum System

Changbin Lu
Fuyou Miao∗,† and Junpeng Hou

School of Computer Science and Technology, University of Science and Technology of China, Hefei, China
Department of Physics, The University of Texas at Dallas, Richardson, Texas 75080-3021, USA

A (t, n) threshold quantum secret sharing (QSS) is proposed based on single d-level quantum system. It enables the (t, n) threshold structure based on Shamir’s secret sharing and simply requires sequential communication in d-level quantum system to recover secret. Besides, the scheme employs an additional qudit to detect cheats and eavesdropping during secret reconstruction, and allows a participant to use the share repeatedly. Analyses show that the proposed scheme is resistant to typical attacks. The scheme is scalable in the number of participants and easier to realize compared to related schemes. More generally, our scheme also presents a generic method to construct new (t, n) threshold QSS schemes based on d-level quantum system with other classical threshold secret sharing.

I. INTRODUCTION

Suppose a dealer needs to share a secret message among a group of users but does not want any single user to have the whole secret. How can the dealer achieve this goal without directly allocating a copy to any user? A desirable method is to distribute a shadow derived from the secret to each user such that some certain number of users can cooperate to recover the secret while fewer users cannot obtain any information of the secret. To address the problem of confidentiality and robustness in keeping a secret among users, Shamir [1] and Blakely [2] proposed (t, n) threshold secret sharing [(t, n)-SS] scheme independently in 1979. In a (t, n)-SS scheme, a secret is split into n shares such that at least t out of n different shares are required to reveal the secret. Today, (t, n)-SS has become a fundamental cryptographic primitive and been widely used in many applications such as group authentication [3], threshold signature [4, 5], group key agreement [6], threshold encryption [7], secure multiparty computation [8], etc.

In recent years, quantum cryptography has attracted much attention due to its higher security than classical cryptography. Based on physical laws such as Heisenberg uncertainty principle and resulted quantum non-cloning theorem, quantum cryptographic protocols are able to provide unconditional security while classical ones usually have computational security based on computational complexity. Thus, using quantum-information-assisted schemes, i.e., quantum secret sharing (QSS), to share secrets among users is more reliable and promising. Such scheme was first proposed by Hillery et al. [9] in 1999, which takes advantage of a three-qubit entangled Greenberger-Horne-Zeilinger (GHZ) state. In the scheme, a GHZ triplet is split and each of the other two participants get a particle. Both participants are allowed to measure their particles in either x or y basis (natural basis) and their results are combined to give the dealer’s measurement result. In this way, a joint secret is established between the dealer and corresponding users. Following the similar idea, the QSS is further generalized to d-level platform [10] by utilizing multiparticle (> 3) entanglement GHZ state. Subsequently, another QSS[11] was proposed using the d-dimensional GHZ state in a different way, in which participants use an X-basis measurement and classical communication to distinguish two orthogonal states and reconstruct the original secret. However, these entanglement-based schemes all have a poor scalability because it is difficult to keep quantum correlations with increasing participants. Obviously, supporting such QSS with more participants requires more entanglement states to be prepared, however, with the increase of state number, entanglement state preparation becomes much more difficult. Moreover, quantum correlations are prone to be spoiled through interacting with environment.

Currently, many existing QSS schemes are of type (n, n) [9–17], which requires all n shareholders, instead of any t or more than t shareholders, to cooperate in recovering the secret. Therefore, they are less flexible than (t, n) ones and has limited applications. Since the first threshold QSS [18] was proposed, there have been mainly 2 methods to construct threshold QSS. The first method is purely using some special quantum states [18–21] in scheme construction. For example, in the seminal work [18], an arbitrary three-dimensional quantum state (qutrit) was employed to construct a (2, 3) threshold scheme, which maps the secret qutrit to three qutrits and each resulting qutrit is taken as a share. The second method is incorporating classical threshold SS with quantum operations and thus keep (t, n) threshold structure [22–26]. These schemes employ quantum operations to embed private value and shares of classical threshold SS into quantum states, such that t or more than t participants can recover the initial quantum state to gain the secret only after they each complete their operations respectively. The first threshold QSS scheme was proposed based on Shamir (t, n)-SS in [22]. In that scheme, a secret is initially embedded into quantum state; then, any t or more than t participants sequentially apply Hadamard transformation and proper rotation oper-

∗Corresponding author.
Email: mfy@ustc.edu.cn
ations on the quantum state, and finally the secret can be regained after applying certain measurements on that state. Several quantum computation algorithms, such as phase shift operation or Quantum Fourier Transform, are also introduced to embed classical shares into quantum state [24–26].

In this paper, we propose a \((t, n)\) threshold QSS scheme based on a single \(d\)-level quantum system, where dimension \(d\) is a prime number. In our scheme, the dealer generates \(n\) shares from a secret and allocates each share to shareholder as in Shamir’s \((t, n)\)-SS. To recover the secret, at least \(t\) participants perform proper unitary operations (in some order) sequentially on a vector of a set of Mutually Unbiased (orthonormal) Bases (MUBs) and after that, the qudit is measured in an appointed basis by dealer. After the announcement of measurement result, participants exchange the random numbers embedded into qudit such that they can recover dealer’s secret. To guarantee security against eavesdropping and cheats, an additional qudit is used to check the consistency of recovered secrets. Compared with existing QSS schemes, our scheme stands out for the following properties: i) private shares can be used repeatedly, ii) more general and practicable than 2-level QSS, iii) scalable to the number of participants, iv) can be generalized to employ other classical \((t, n)\)-SS schemes while keeping all the aforementioned properties.

II. SECRET SHARING BASED ON A SINGLE \(D\)-LEVEL QUANTUM SYSTEM

A. The cyclic property of the MUBs

In this paper, we construct a \((t, n)\) threshold quantum secret sharing scheme based on a set of MUBs which has the cyclic property [12]. It has been proved that \(d + 1\) MUBs can be found in a \(d\)-dimensional complex vector space if \(d\) is an odd prime [27, 28]. Besides the computational basis \(\{|j\rangle : j = 0, 1, ..., d - 1\}\), the explicit forms of the remaining \(d\) sets of MUBs are \(\varphi_{l, k} = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{j(l+k)} |j\rangle\), where \(k = 0, 1, ..., d - 1\) labels the basis, \(l = 0, 1, ..., d - 1\) enumerates the vectors of the given basis and \(\omega = e^{2\pi i/d}\) is the \(d\)th root of unity. For any 2 values \(l \neq l'\), these MUBs have the following property

\[ \langle \varphi_{l, k} | \varphi_{l', k'} \rangle = 0, \tag{1} \]

and this indicates that \(\varphi_{l, k}\) may serve as a basis. Moreover, they are mutually unbiased because

\[ \left| \langle \varphi_{l, k} | \varphi_{l', k'} \rangle \right|^2 = \frac{1}{d} \tag{2} \]

holds for \(l \neq l'\) and \(k \neq k'\). Beside from the viewpoint of bra-ket notation, equation (2) can also be inferred from Number Theory due to \(\sum_{j=0}^{d-1} \omega^{pj+qj^2} = \sqrt{d}\) for \(p, q \in \mathbb{Z}, q \neq 0\) and prime number \(d\).

The set of MUBs has a cyclic property, i.e., there exist unitary operations \(U_{l'k'}\) for any \(l', k' \in \{0, 1, ..., d - 1\}\) transforming a given vector \(|\varphi_{l, k}\rangle\) to \(|\varphi_{l+l', k+k'}\rangle\). Specifically, the operations \(X_d = \sum_{r=0}^{d-1} \omega^r |r\rangle \langle r|\) and \(Y_d = \sum_{r=0}^{d-1} \omega^{2r} |r\rangle \langle r|\) can transform the vector \(|\varphi_{l, k}\rangle\) into \(|\varphi_{l+1, k}\rangle\) and \(|\varphi_{l, k+1}\rangle\) respectively due to

\[ X_d |\varphi_{l, k}\rangle = \frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} \omega^r |r\rangle \langle r| \sum_{j=0}^{d-1} \omega^{jl(l+kj)} |j\rangle \]

\[ = \frac{1}{\sqrt{d}} \sum_{r, j=0}^{d-1} \omega_r \omega^{jl(l+kj)} |r\rangle |\delta_{rj} \tag{3} \]

\[ = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{j(l+1)+kj} |j\rangle = |\varphi_{l+1, k}\rangle, \]

while the correctness of \(Y_d\) can be proven in the same way. As a result, the unitary operations \(U_{l'k'}\) is just the combination of those two operators \(U_{l'k'} = X_d Y_d\) and note that \([X_d, Y_d] = 0\) guarantees the definition of exponents.

B. Threshold secret sharing based on qudits

1. Overview

Generally speaking, the scheme is constructed based on the cyclic property of MUBs and classical threshold secret sharing.

Initially, Each shareholder is allocated a share generated from a private value (i.e., the secret in classical secret sharing). Then, the dealer prepares \(3t\) qudits and then embeds 2 secrets and a verification value into each qudit respectively, moreover, each qudit also includes the same private value. These qudits are delivered along a line of at least \(t\) participants. On receiving the qudits, each participant performs unitary operations related to the share on the qudits. On one hand, these operations add a random number to each secret and the verification value, on the other hand, they remove the private value in each qudit by classical \((t, n)\) threshold secret sharing. Subsequently, the last participant measures the 3 qudits and publishes the measurement results to all participants. Finally, all participants recover the 2 secrets and the verification value after disclosing their respective random numbers. Each participant is able to check the correctness of the 2 secrets by the verification value, and thus can detect any cheat during the secret reconstruction.

2. Proposed scheme

The scheme consists of two phases (a) classical private share distribution and (b) secret sharing, and we present each phase in details as following.
Classical private share distribution phase. In this initial step, dealer Alice first distributes classical private shares to n shareholders Bob_j.

(i) Alice picks a random polynomial \( f(x) \) of degree \( t-1 \) over finite field \( GF(d) \):

\[
\begin{align*}
f(x) &= a_0 + a_1 x + \ldots + a_{t-1} x^{t-1} \mod d, \\
s &= a_0 = f(0)
\end{align*}
\]

where \( s = a_0 = f(0) \) is the private value and all coefficients \( a_j, j = 0, 1, \ldots, t-1 \), are in the finite field \( GF(d) \) for a large prime \( d \).

(ii) Alice computes \( f(x_j) \) as the share of shareholder \( Bob_j \) for \( j = 1, 2, \ldots, n \), where \( x_j \in GF(d) \) is the public information of \( Bob_j \) with \( x_j \neq x_r \) for \( j \neq r \).

(iii) Alice sends each share \( f(x_j) \) to the corresponding shareholder \( Bob_j \) through quantum secure direct communication presented in [29, 30], which guarantees shares are delivered securely from Alice to shareholders.

Secret sharing phase. The dealer Alice first prepares three identical states \( |\Phi_v \rangle = |\varphi^0_v \rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j \rangle, v = 1, 2, 3, \) and then shares secrets \( S_1, S_2 \in GF(d) \) among \( m (m \geq t) \) shareholders by taking the following steps.

(i) Alice performs the operations \( U_{p_0, q_0} v \) on \( |\Phi_v \rangle \), and transform the states \( |\Phi_v \rangle \) into \( |\Phi_{v_0} \rangle = |\varphi_{p_0, q_0} v \rangle \), where \( p_0 = S_1, p_0^2 = S_2, p_0^3 = N, q_0^1 = q_0^2 = q_0^3 = d - s \) with \( p_0, q_0 \in \{0, 1, \ldots, d-1\}, S_1 = NS_2 \mod d \).

(ii) Suppose that Alice needs to share secrets \( S_1, S_2 \) among \( m \) \( (m \geq t) \) participants \( \{Bob_j, j = 1, 2, \ldots, m\} \), she sends the three states \( |\Phi_{v_0} \rangle \) to \( Bob_1 \). Upon receiving the 3 states, \( Bob_1 \) performs operations \( U_{p_1, q_1} v \) on \( |\Phi_{v_0} \rangle \) respectively, where \( p_1^v \) are mutually independent random numbers, \( q_1^v = c_1 = f(x_1) \prod_{r=2}^{m} \frac{x_r - x_1}{x_r} \mod d \), and \( p_1^v, q_1^v \in \{0, 1, \ldots, d - 1\} \). As a result, the states \( |\Phi_{v_0} \rangle \) are transformed into \( |\Phi_{v_1} \rangle = |\varphi_{p_0, p_1, q_0, q_1} v \rangle \). \( Bob_1 \) delivers the states \( |\Phi_{v_1} \rangle \) to \( Bob_2 \).

(iii) Each of the other shareholders \( Bob_j, j = 2, 3, \ldots, m \), repeats the same procedure sequentially as \( Bob_1 \) does in (ii), that is, \( Bob_j \) performs the operations \( U_{p_j, q_j} v \) on \( |\Phi_{v_{j-1}} \rangle \) accordingly and thus get the states \( |\Phi_{v_j} \rangle = |\varphi_{\sum_{r=0}^{j} p_r, \sum_{r=0}^{j} q_r} v \rangle \), where \( p_j^v, q_j^v \in \{0, 1, \ldots, d - 1\} \), \( p_j^v \) are mutually independent random numbers, \( q_j^v = c_j = f(x_j) \prod_{r=1, r \neq j}^{m} \frac{x_r - x_j}{x_r} \mod d \). Subsequently, \( Bob_j, j = 2, 3, \ldots, m - 1 \) send \( |\Phi_{v_j} \rangle \) to next participant \( Bob_{j+1} \).

(iv) Consequently, the last participant \( Bob_m \) keeps the 3 states and chooses the basis \( \{|\varphi^0_v \rangle \} \) to measure these three states. The results are labeled \( R_1, R_2, R_3 \) and then \( Bob_m \) publishes the results.

(v) The measurement basis is \( \{|\varphi^0_v \rangle \} \) because

\[
\sum_{j=0}^{m} q_j = d - s + \sum_{j=1}^{m} c_j = 0 \mod d, \tag{4}
\]

so that measurement results \( R_1, R_2, R_3 \) and the random numbers \( p_j^v, p_j^2, p_j^3, j = 0, 1, \ldots, m \) satisfy

\[
\sum_{j=0}^{m} p_j^v = R_v \mod d, v = 1, 2, 3. \tag{5}
\]

After all \( m \) participants exchange their random numbers, they obtain the values \( p_0^1, p_0^2, p_0^3 \).

(vi) To check the correctness of the values \( p_0^1, p_0^2 \) and \( p_0^3 \), each participant can verify whether the following equation holds

\[
p_0^1 = p_0^3 \mod d. \tag{6}
\]

If it does, the secret sharing attempt is not corrupt and thus all participants share the dealer’s secrets \( S_1 = p_0^1, S_2 = p_0^2; \) otherwise they are aware that the secret sharing is invalid and abort this round.

The correctness of the scheme is that after dealer and all \( m \) participants complete their operations the final state becomes

\[
|\Phi \rangle = \left( \prod_{r=0}^{m} X^{d^r} Y^{q_r} \right) |\Phi \rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{\sum_{r=0}^{m} (j p_r + q_r)} |j \rangle. \tag{7}
\]

However, due to equation (4), we have \( \sum_{r=0}^{m} q_r = 0 \mod d \) and this ensures that when \( Bob_m \) measures the final states in the basis \( \{|\varphi^0_v \rangle \} \), he obtains the real results satisfying equation (6).

### III. Security Analysis

In this section, we show that our scheme is secure against various attacking strategies. Firstly, we consider the intercept-resend attack mounted by an external eavesdropper Eve. She may intercept the qudit \( |\varphi^k \rangle \) sent from \( Bob_j \) to \( Bob_{j+1} \), but does not have any information about the measurement basis. To figure out the secret message, she can only choose one of the \( d \) relevant bases to measure the qudit. Obviously, Eve can obtain the correct measurement result only when she happens to choose the true basis \( k' = k \), which has the probability of \( 1/d \). Even if Eve gets the correct measurement result, she is still unable to obtain the secret. Since the measurement
result is the sum of dealer’s secret and proceeding participants’ random numbers, she can infer the dealer’s secret only with the probability $1/d$ if she doesn’t know these random numbers. Even if Eve successfully intercepts the qudit directly from the dealer, she just has a probability of $1/d$ to select the true measurement basis and obtain the secret. Relatively, she will fail and change the qudit sent to Bob$_{j+1}$ with probability $(d-1)/d$. Moreover, when Eve chooses a wrong basis to measure the qudit, it causes contradiction to equation (6) and can thus be detected in step (vi) in the protocol. In a word, Eve cannot figure out the secret with the probability more than $1/d$ in intercept-resend attack. Obviously, the scheme is more secure for a larger prime $d$.

Consider that the first participant Bob$_1$ tries to infer the dealer’s secrets alone by measuring qudits sent directly from the dealer. In this case, with only one share (i.e., less than $t$ shares), he cannot recover the private value $s$ previously embedded in qudits by the dealer. Therefore, he only has the probability $1/d$ to guess the true measurement basis and thus obtain the secrets while has the probability $(d-1)/d$ to fail, which will be detected in step (vi).

The third attack strategy a participant may take is using a random number, instead of the component $c_j$ generated by his own share, in the unitary operation. However, this attack will not be effective since the equation (4) is violated and thus the last participant Bob$_n$ cannot obtain correct measurement results with the basis $\{ |\phi_i^0 \rangle \}_i$. That is, the published measurement results are random numbers in $GF(d)$. Therefore, after participants exchange random numbers, they all get wrong secrets. Consequently, this attack will be detected in step (vi) because of the violation of equation (6).

The last participant Bob$_{n}$ is crucial for our scheme because he can keep and measure the qudit in true basis. So, it is necessary to take appropriate methods to detect the following cheat. Assume that Bob$_{n}$ deceives other honest participants by announcing wrong measurement results after he measures the qudits correctly. However, this action will be detected because the scheme employs 2 qudits to share 2 secrets and an additional qudit to check whether $p_0^1 = p_0^3 p_0^2 \mod d$ holds. It works since Bob$_{n}$ are required to announce his measurement results before participants exchange random numbers. Consequently, he only has the sums of a secret and random numbers but without any information about $p_0^1$, $p_0^2$ or $p_0^3$ before participants exchange random numbers. In this case, the probability that the other participants recover fake secrets satisfying equation (6) but Bob$_{n}$ obtains the true secrets is $1/d$. This is because, given each pair of $(p_0^1, p_0^3)$, there is only one value of $p_0^2$ satisfying $p_0^1 = p_0^3 p_0^2 \mod d$ in $GF(d)$.

Considering the joint attack taken by part of participants in association with entanglement swapping [31, 32], they could entangle the qudit with an ancilla (e.g. Bell states), or use new entangled states to replace the qudits. However, they benefit nothing from this attack, because less than $t$ shares cannot recover the private value $s$, even though entanglement swapping renders the qudits available for cheaters in a mixed state, there is no observable result obtained. As a result, they will face the problems that possessing no knowledge on measurement basis and also that they cannot achieve random numbers used by other honest participants. Furthermore, this attack can be detected in step (vi) because the basis $\{ |\phi_i^0 \rangle \}_i$ is wrong and following that, the recovered values not satisfying $p_0^1 = p_0^3 p_0^2 \mod d$.

IV. RELATED WORK AND DISCUSSIONS

A. Related work

There are many QSS schemes, but most of them are 2-level [9, 13–15, 22–25] and with $(n, n)$ structure [9–17]. For instance, in the scheme [14], the authors use phase shift operation to embed the secret into a single qubit such that the secret can be recovered after all participants complete their operations. Besides, a special QSS based on Grover quantum searching algorithm was proposed in [13]. But these 2-level schemes have less universality and practicability when compared to $d$-level ones and $(n, n)$ structure QSS schemes are less flexible than $(t, n)$ ones in the sense that, other than any $t$ parties, all shareholders must be present to recover the secret. Compared with these scheme, our $d$-level $(t, n)$ threshold quantum secret sharing scheme is more flexible, universal and practicable. Hence, the following parts concern about $d$-level or $(t, n)$ threshold structure schemes.

The scheme in [10] initially prepares a high-fidelity GHZ state with $n$ subsystems. Once the state is produced, the number of participants is fixed. Consequently, the scheme becomes more difficult to realize with the increase of participant number. Yu et.al presented another QSS [11] based on $d$-dimensional GHZ state, which is also not scalable with the growth of participant number. In their scheme, an X-basis measurement and classical communication are used to distinguish two orthogonal states and reconstruct the original secret. Some $d$-level schemes [17, 26] were proposed based on Quantum Fourier Transform. The scheme in [17] disguises each share of a secret with true randomness, rather than classical pseudo randomness. But it is also difficult to extend with larger participants. A common problem of these schemes is that each participant needs to measure his particle at last, but some participant may fail in measurement due to inefficient detection and thus render an invalid secret sharing easily. Compared with these schemes based on special quantum state, our scheme enjoys a strong scalability because it is almost not restricted by number of participants in realization.

As for schemes with $(t, n)$ structure, the first one [18] was proposed in 1999 based on quantum error correcting code. The scheme divides a special quantum state into $n$ shares, such that any $t$ or more than $t$ participants
can recover the initial state using linear transformation. However, it is hard to map the quantum state to n quantum states in coding, moreover, the scheme is not easy to extend.

Another method used in [19–21] benefits from the ability of exactly distinguishing orthogonal multipartite entangled states under restricted local operation and classical communication (LOCC). The scheme [19] requires no joint quantum operation in secret reconstruction, moreover, it is cost-efficient. The scheme in [20] employs orthogonal multipartite entangled states in d-qudit system to construct a (t, n) threshold QSS, but it is a ramp one in security, which means there exits information leak about the secret in some cases. Based on previous (t, n)-threshold LOCC-QSS scheme and a simple encoding method, a more secure (t, n)-threshold LOCC-QSS scheme was proposed in [21]. Different from special quantum systems-based scheme [18–21], some threshold QSS schemes [22–26] take advantage of the classical secret sharing. For example, schemes in [22, 23] change the field of Shamir’s (t, n)-SS into $F_{2^N}$ and encode classical bit string by some unity operation. At the same time, schemes in [24, 25] first use phase shift operation to embed private values (e.g. shares in Shamir’s (t, n)-SS, elements in linear equation) in classical secret sharing into quantum states, and then retrieve a secret by recovering quantum state. Recently, a (t, n) threshold d-level QSS scheme [26] was proposed, it needs some unitary operations such as d-level CNOT, (Inverse) Quantum Fourier Transformation, and generalized Pauli operator performed on particles. As a (t, n) threshold d-level QSS, generally speaking, it is more universal and practical than 2-level QSS. But the scheme needs a trusted third party (e.g., the dealer) measuring the quantum states in secret reconstruction. Since the strategy is quite similar to those in [10, 11, 17], it is not scalable either. Compared with these (t, n) schemes, our scheme employs d-level unitary operation in association with classical (t, n) threshold secret sharing. Due to the verification mechanism by equation (6), it is free from the trusted third party who is responsible for measurement results and any cheat behaviour by a participant can be detected easily.

### B. Discussion

Thinking further about the proposed scheme, we can find a generic method to construct such type of d-level threshold QSS schemes. Note that our scheme employs the classical Shamir’s (t, n) secret sharing, each participant, e.g., Bob$_j$, constructs a component $c_j$ from the share and then produces the d-level unitary operations from $c_j$. After each participant complete its d-level unitary operation on a qudit sequentially, all coefficients $c_j, j = 1, 2,...,m$, are actually added up and the private value $s$ is removed, which ensures that the last participant Bob$_m$ gets the correct measurement result. As a matter of fact, as long as a classical (t, n) threshold secret sharing has the property of cumulative sum, i.e., the secret (i.e., private value in our scheme) $s$, can be expressed as $s = \sum_{j=1}^{m} c_j \mod M = \sum_{j=1}^{m} a_j s_j \mod M$, it can be used to construct such a d-level (t, n) threshold quantum secret sharing, where $c_j$ is the value Bob$_j$ evaluated from the share $s_j$ and $a_j$ some public parameters, $m \geq t$ is the number of participants and $M$ is a modulus.

To be more specific, since $s$ is embedded in the qudit initially by the dealer in the form $q_0^v = d - s, v = 1, 2, 3, ...m$, each participant Bob$_j$ then sequentially performs the d-level unitary operation on the qudits, which is actually adding the component $c_j$ to $q_0^v$. After all participants complete their operations on the qudits, the private value $s$ is eliminated from $q_0^v$. Consequently, the last participant Bob$_m$ can measure the qudits correctly and all participants obtain the secrets $p_0^v, v = 1, 2, 3$ ultimately. Therefore, other classical (t, n)-secret sharing schemes, such as linear code based (t, n)-SS [33, 34], geometry based (t, n)-SS [2], Chinese Remainder Theorem based (t, n)-SS [35, 36], etc., can also be used to construct threshold QSS schemes based on a single d-level quantum system.

### V. CONCLUSION

This paper proposes a (t, n) threshold QSS scheme based on single d-level quantum system. The scheme simply requires sequential communication of a single d-level quantum system during secret reconstruction. It is flexible in application, scalable in participant number and easy to realize. Security analyses show the scheme is secure against typical attacks. Moreover, an additional qudit is used to verify recovered secrets so that eavesdropping and cheats can be detected.

By the method of our scheme, new (t, n) threshold QSS schemes based on single d-level quantum system can be easily constructed if the Shamir’s (t, n) secret sharing scheme is replaced by other classical threshold ones.

### Acknowledgments

**Acknowledgments:** This work is supported was supported by the National Natural Science Foundation of China under 61572454, 61572453, 61520106007.

[1] A. Shamir, “How to share a secret”, Commun. ACM, vol. 22, no. 11, pp. 612-613, 1979.

[2] G. R. Blakley, “Safeguarding cryptographic keys”, in
