Quantum Information Processing (2018) 17:310
https://doi.org/10.1007/s11128-018-2059-7

Verifiable threshold quantum secret sharing with sequential communication

Changbin Lu[1] · Fuyou Miao[1] · Junpeng Hou[2] · Keju Meng[1]

Received: 2 April 2018 / Accepted: 6 September 2018 / Published online: 3 October 2018
© Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract
A (t, n) threshold quantum secret sharing (QSS) is proposed based on a 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 provides a verification mechanism which 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. Moreover, the scheme is scalable in participant number 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 from other classical threshold secret sharing.

Keywords Quantum cryptography · (t, n) threshold structure · Verification mechanism · d-level MUBs

1 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

✉ Fuyou Miao
mfy@ustc.edu.cn

Changbin Lu
lcb@mail.ustc.edu.cn

Junpeng Hou
Junpeng.Hou@utdallas.edu

Keju Meng
mkj@mail.ustc.edu.cn

[1] School of Computer Science and Technology, University of Science and Technology of China, Hefei, China

[2] Department of Physics, The University of Texas at Dallas, Richardson, Texas 75080-3021, USA

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 the well-defined (t, n) threshold secret sharing $[(t, n)$-SS$]$ scheme independently in 1979, with two criteria, should be respected. The first one is reliability, meaning the scheme should allow at least t users who can recover the secret. The second criterion is confidentiality: It means less than t users should not gain any information about the secret (even with unlimited computation resource). 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] and secure multiparty computation [8].

In recent years, quantum cryptography has attracted much attention due to its inherent security. Based on physical laws such as Heisenberg uncertainty principle and the resulted quantum no-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. Furthermore, QSS provides a robust and secure solution for quantum state storage and computation [9]. Such scheme was first proposed by Hillery et al. [10] 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 [11] by utilizing multiparticle (> 3) entanglement GHZ state. Subsequently, another QSS [12] 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 are all poor in scalability because it gets difficult to keep quantum correlations among more and more participants. Obviously, supporting such QSS with more participants requires more entangled state to be prepared; however, with the increase in the number of qubits, entangled 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 (n, n) type [10–20] including some experimental demonstrations [21–24], 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 have limited applications. Since the first threshold QSS [9] was proposed, there have been mainly two methods to construct threshold QSS. The first method is purely using some special quantum systems [9,25–30] in schemes' construction. For example, in the seminal work [9], an arbitrary three-dimensional quantum state (or qutrit) was employed to construct a (2, 3) threshold scheme, which maps the private qutrit to three qutrits and each resulted qutrit is taken as a share.

The second method is incorporating classical threshold SS with quantum operations and thus keep (t, n) threshold structure [31–35]. 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. The first threshold QSS scheme based on Shamir's (t, n)-SS was proposed in [31]. In this scheme, a secret is initially embedded into quantum states; then, any t or more than t participants sequentially apply Hadamard transformation and proper rotation operations on the quantum state; finally, the secret can be regained after applying certain measurements on the state. Several quantum computation algorithms, such as phase shift operation or quantum Fourier transform, are also introduced to embed classical shares into quantum states [32–34].

In this paper, we propose a (t, n) threshold QSS scheme based on a single d-level quantum system, where dimension d is an odd prime number. In our scheme, the dealer generates n shares from a secret and allocates each share to shareholders 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); subsequently, the qudit is measured in an appointed basis by the last participant. After the announcement of measurement result, participants exchange random numbers embedded in the qudit such that they can recover the dealer's secret. To guarantee the security against eavesdropping and cheats, a verification mechanism is established which uses an additional qudit to check the consistency of recovered secrets. Compared with existing QSS schemes, our scheme stands out for the following properties:

(i) It is more general and practicable than 2-level QSS; moreover, private shares can be used repeatedly.
(ii) It is scalable in the number of participants compared with schemes based on entangled states.
(iii) As a (t, n) threshold QSS, it is more flexible in application than (n, n)-QSS;
(iv) Based on the verification mechanism, it does not depend on any trusted third party and is able to detect any cheat and eavesdropping during secret reconstruction.
(v) Other classical (t, n)-SS schemes can be used to replace Shamir's scheme while keeping all the aforementioned properties.

2 Secret sharing based on a single *d*-level quantum system

2.1 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 [13]. It has been proven that $d+1$ MUBs can be found in a d-dimensional complex vector space if d is an odd prime [36,37]. Besides the computational basis $\{|j\rangle, j = 0, 1, \ldots, d-1\}$, the explicit forms of the remaining d sets of MUBs are $\left|\varphi_l{}^k\right\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{j(l+kj)} |j\rangle$, where $k = 0, 1, \ldots, d-1$ labels the basis, $l = 0, 1, \ldots, d-1$ enumerates the vectors of the given basis and $\omega = e^{2\pi i/d}$

is the dth root of unity. For any two values $l \neq l'$, these MUBs have the following property

$$\left\langle \varphi_l{}^k \middle| \varphi_{l'}{}^k \right\rangle = 0, \tag{1}$$

and this indicates that $\left|\varphi_l^k\right\rangle$ may serve as a basis. Moreover, they are mutually unbiased because

$$\left|\left\langle \varphi_l{}^k \middle| \varphi_{l'}{}^{k'} \right\rangle\right|^2 = \frac{1}{d} \tag{2}$$

holds for $l \neq l'$ and $k \neq k'$. Besides from the viewpoint of bra-ket notation, Eq. (2) can also be inferred from number theory due to $\left|\sum_{j=0}^{d-1} \omega^{pj+qj^2}\right| = \sqrt{d}$ for $p, q \in Z$, $q \neq 0$ and prime number d.

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

$$\begin{aligned} X_d \left|\varphi_l{}^k\right\rangle &= \frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} \omega^r \left|r\right\rangle \left\langle r\right| \sum_{j=0}^{d-1} \omega^{j(l+kj)} \left|j\right\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{r,j=0}^{d-1} \omega^r \omega^{j(l+kj)} \left|r\right\rangle \delta_{rj} \\ &= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{j[(l+1)+kj]} \left|j\right\rangle = \left|\varphi_{l+1}{}^k\right\rangle, \end{aligned} \tag{3}$$

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

2.2 Threshold secret sharing based on qudits

2.2.1 Overview

The scheme is constructed based on the cyclic property of MUBs and classical (t, n)-SS. Initially, each shareholder is allocated a share generated from a private value (i.e., the secret in classical secret sharing). Then, the dealer prepares three qudits and embeds two 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, an operation adds a random number to each secret and the verification value; on the other hand, the private value in each qudit is eliminated due to classical (t, n)-SS after at least t participants complete their unitary operations. Subsequently, the last participant measures the three qudits and publishes the measurement results to all participants. Finally, all participants recover the two secrets and the verification value after disclosing their respective random numbers. Each participant is able to check the correctness of the two secrets by the verification value and thus can detect any cheats and eavesdropping during secret reconstruction.

2.2.2 Proposed scheme

The scheme consists of two phases, *Classical private share distribution* and *Secret sharing*, and we present each phase in detail as follows.

Classical private share distribution phase. In this phase, dealer Alice distributes classical private shares to n shareholders Bob_j, $j = 1, 2, \ldots, n$.

(i) Alice picks a random polynomial $f(x)$ of degree at most $(t-1)$ over finite field $\text{GF}(d)$:

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

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 $\text{GF}(d)$ 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 non-zero number $x_j \in \text{GF}(d)$ is the public information of Bob_j with $x_j \neq x_r$ for $j \neq r. n$, $(n \geq t)$, is the total number of shareholders. A shareholder is also called participant when it participates in secret reconstruction.

(iii) Alice sends each share $f(x_j)$ to the corresponding shareholder Bob_j through private channel, which guarantees shares are delivered securely from Alice to shareholders.

Secret sharing phase. The dealer Alice first prepares three identical states $|\Phi_v\rangle = \left|\varphi_0{}^0\right\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j\rangle$, $v = 1, 2, 3$, and then shares secrets $S_1, S_2 \in \text{GF}(d)$ and a check value $N \in \text{GF}(d)$ among m, $(m \geq t)$ shareholders by taking the following steps.

(i) Alice performs the operations $U_{p_0{}^v q_0{}^v} = X_d{}^{p_0{}^v} Y_d{}^{q_0{}^v}$ on $|\Phi_v\rangle$, which transform the states $|\Phi_v\rangle$ into $|\Phi_v\rangle_0 = \left|\varphi_{p_0{}^v}{}^{q_0{}^v}\right\rangle$, where $p_0{}^1 = S_1$, $p_0{}^2 = S_2$, $p_0{}^3 = N$, $q_0{}^1 = q_0{}^2 = q_0{}^3 = d - s$ with $p_0{}^v, q_0{}^v \in \text{GF}(d)$, $S_1 = S_2 N \bmod d$.

(ii) Suppose that Alice needs to share secrets S_1, S_2 among m $(m \geq t)$ participants $\{\text{Bob}_j, j = 1, 2, \ldots, m\}$, she sends the three states $|\Phi_v\rangle_0$ to Bob_1. Upon receiving the three states, Bob_1 performs operations $U_{p_1{}^v q_1{}^v}$ on $|\Phi_v\rangle_0$, respectively, where $p_1{}^v$ are mutually independent random numbers, $q_1{}^v = c_1 = f(x_1)\prod_{r=2}^{m}\frac{x_r}{x_r - x_1} \bmod d$, $v = 1, 2, 3$, and $p_1{}^v, q_1{}^v \in \text{GF}(d)$. As a result, the states $|\Phi_v\rangle_0$ are transformed into $|\Phi_v\rangle_1 = \left|\varphi_{(p_0{}^v + p_1{}^v)}{}^{(q_0{}^v + q_1{}^v)}\right\rangle$. Bob_1 delivers the states $|\Phi_v\rangle_1$ to Bob_2.

(iii) Each of the other participants Bob_j, $j = 2, 3, \ldots, m$, repeats the same procedure sequentially as Bob_1 does in previous step (ii). That is, Bob_j performs the operations $U_{p_j{}^v q_j{}^v}$ on $|\Phi_v\rangle_{j-1}$ accordingly and thus gets the states $|\Phi_v\rangle_j = \left|\varphi_{\sum_{r=0}^{j} p_r{}^v}{}^{\sum_{r=0}^{j} q_r{}^v}\right\rangle$, where $p_j{}^v, q_j{}^v \in \text{GF}(d)$, $p_j{}^v$ are mutually independent random numbers, ${q_j}^v = c_j = f(x_j)\prod_{r=1,r\neq j}^{m}\frac{x_r}{x_r-x_j} \bmod d$. Subsequently, Bob_j sends $|\Phi_v\rangle_j$ to next participant Bob_{j+1}, $j = 2, 3, \ldots, m-1$.

(iv) Consequently, the last participant Bob_m keeps the three states and chooses the basis $\left\{\left|{\varphi_l}^0\right\rangle\right\}_l$ to measure these three states. The results are labeled R_1, R_2, R_3, respectively, and then Bob_m publishes the results.

(v) The measurement basis is $\left\{\left|{\varphi_l}^0\right\rangle\right\}_l$ due to

$$\sum_{j=0}^{m} q_j = d - s + \sum_{j=1}^{m} c_j \bmod d = 0 \bmod d. \tag{4}$$

In this case, measurement results R_1, R_2, R_3 and the random numbers ${p_j}^1, {p_j}^2, {p_j}^3$, $j = 0, 1, \ldots, m$ satisfy

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

After all m participants exchange their random numbers, they obtain the values ${p_0}^1 = R_1 - \sum_{j=1}^{m} {p_j}^1$, ${p_0}^2 = R_2 - \sum_{j=1}^{m} {p_j}^2$ and ${p_0}^3 = R_3 - \sum_{j=1}^{m} {p_j}^3$, respectively.

(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

$${p_0}^1 = {p_0}^2{p_0}^3 \bmod d. \tag{6}$$

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.

2.2.3 Correctness of the scheme

The scheme is correct because, after the dealer and all m $(m \geq t)$ participants complete their operations, each final state becomes

$$\begin{aligned}|\Phi\rangle_m &= \left(\prod_{r=0}^{m} {X_d}^{{p_r}^v}{Y_d}^{{q_r}^v}\right)|\Phi\rangle \\ &= \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\omega^{\sum_{r=0}^{m}\left(j{p_r}^v + j^2{q_r}^v\right)}|j\rangle,\end{aligned} \tag{7}$$

for $v = 1, 2, 3$.

Besides, all participants in Shamir's (t, n)-SS can recover the secret by summing up all components, i.e.,

$$s = f(0) = \sum_{j=1}^{m} c_j \bmod d = \sum_{j=1}^{m} f(x_j) \prod_{r=1, r\neq j}^{m} \frac{x_r}{x_r - x_j} \bmod d, \tag{8}$$

which can be immediately obtained by Lagrange interpolation formula.

Thus, we have $\sum_{j=1}^{m} c_j = Nd + s, N \in Z$, so the Eq. (4) holds. Then, due to Eq. (4) which is $\sum_{j=0}^{m} q_j = 0 \bmod d$, it follows that when Bob$_m$ measures the final states in the basis $\left\{\left|\varphi_l{}^0\right\rangle\right\}_l$, he obtains the real results satisfying Eq. (6). Finally, with published results, all m participants can recover secrets by exchanging their random numbers. Here, the proposed scheme satisfies reliability, the first criteria of a well-defined (t, n)-SS since it allows at least t participants recovering the secret.

3 Security analysis

In this section, we show that our scheme is perfect and secure against various attack strategies including intercept–resend attack, participant attack and joint attack. Then, we will analyze the validity of the verification mechanism against cheat and eavesdropping.

3.1 Confidentiality analysis

Here, we mainly prove the perfect security of the scheme. A (t, n)-QSS scheme is perfect with respect to the probability distribution of secret over secret space if less than t participants obtain no information about the secret.

Theorem 1 *The proposed (t, n)-QSS scheme is perfect with respect to the probability distribution of secret over secret space. That is,*

$$I(S_v; \Omega) = H(S_v) - H(S_v|\Omega) = 0 \tag{9}$$

where Ω denotes the set of shares available for less than $t-1$ participants, $H(S_v)$ is the information entropy of the secret S_v, $v = 1, 2$ and $I(S_v; \Omega)$ which represents the mutual information of S_v with Ω.

Proof Suppose that $m(m \geq t)$ participants $\{\mathrm{Bob}_j, j = 1, 2, \ldots, m\}$, with the corresponding shares $\{f(x_j), j = 1, 2, \ldots, m\}$, collaborate to recover each secret $S_v, v = 1, 2$ in normal case.

Without losing generality, assume exactly $t-1$ participants $\{\mathrm{Bob}_j, j = 1, 2, \ldots, t-1\}$ conspire in the attack and Bob$_{t-1}$ measures $|\Phi_v\rangle_{t-1}$. But only with true measurement basis which is no longer the appointed basis $\left\{\left|\varphi_l{}^0\right\rangle\right\}_l$, they can get correct results; otherwise due to Eq. (2), they will get the correct results with the probability $1/d$. The key point is that the measurement basis is encoded by the private value s used in

Classical private share distribution phase. But according to Shamir's[1] (t, n)-SS, for $m \geq t$, each private value

$$s = \sum_{j=1}^{m} f(x_j) \prod_{r=1, r \neq j}^{m} \frac{x_r}{x_r - x_j} \bmod d, \tag{10}$$

and s is uniformly distributed over GF(d) if $t-1$ participants $\{\text{Bob}_j, j = 1, 2, \ldots, t-1\}$ conspire. That is, with the shares $\Omega = \{f(x_j), j = 1, 2, \ldots, t-1\}$ available, they have the probability $P(s|\Omega) = 1/d$ to obtain s. Further, they can get correct results and random numbers exchanged from others and then recover the secrets. Thus, the probability to obtain S_v is $1/d$. As a result, we have conditional entropy $H(S_v|\Omega) = \log d$.

On the other hand, since p_{v0} is uniformly and randomly selected from GF(d) by Alice from the view of participants, hence, $S_v = p_{v0}$ is indistinguishable from a random variable uniformly distributed over GF(d), i.e., $P(S_v) = 1/d$. Consequently, the entropy of S_v is $H(S_v) = \log d$.

Therefore, we finally have

$$I(S_v; \Omega) = H(S_v) - H(S_v|\Omega) = 0. \tag{11}$$

Since both secrets S_v, $v = 1, 2$ and the verification value S_3 all satisfy the above equation, the proposed scheme is perfect with respect to probability distribution of secrets in the secret space GF(d). Here, the criteria confidentiality is satisfied. □

Overall, we can see that with respecting the two criteria, the proposed scheme is a well-defined (t, n) QSS.

3.2 Intercept–resend attack

Here, we consider the intercept–resend attack mounted by an external eavesdropper Eve. She may intercept the qudit $\left|\varphi_l{}^k\right\rangle$ sent from Bob$_j$ to Bob$_{j+1}$, but with no information about the measurement basis. Obviously, Eve can obtain the correct measurement result only when she happens to choose the true basis $k' = k$, which has the probability of $1/d$. Moreover, the correct measurement result is the sum of dealer's secret, and preceding participants' random numbers, she can infer the dealer's secret only with the probability $1/d$ if she does not know these random numbers. Relatively, she will fail and change the qudit sent to Bob$_{j+1}$ with probability $(d-1)d$. Then, it will cause contradiction to Eq. (6) and thus be detected in step (VI) in the scheme. 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.

3.3 Participant attack

A simple 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 Eq. (4) is violated, and thus, the last participant Bob$_m$ cannot obtain correct measurement results with the basis $\{|\varphi_l{}^0\rangle\}_l$. 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 Eq. (6).

Considering 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, because Shamir's (t, n)-SS is perfect [38], i.e., no information about the secret can be obtained in Shamir's (t, n)-SS with less than t shares. Thus, he can never measure the qudits in true basis but only to guess with the negligible probability $1/d$. It means this attack works to get secret with probability $1/d$ which is the same to guess the secret.

The last participant is at the special role in the proposed scheme, with the opportunity to measure the qudits in true basis. Thus, in Sect. 3.5, we will analyze the attack mounted by the last participant, which is more challenging to the scheme's security.

3.4 Joint attack

Considering the joint attack taken by part of participants in association with entanglement swapping [39,40], 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, and 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 $\{|\varphi_l{}^0\rangle\}_l$ is wrong, and consequently, the recovered values do not satisfy $p_0{}^1 = p_0{}^2 p_0{}^3 \bmod d$.

3.5 Verification mechanism

The last participant Bob$_m$ is crucial to our scheme because he is responsible for keeping and measuring the qudits in true basis. So, he is able to deceive the other participants by announcing wrong measurement results. Of course, other participant can also cheat by using a wrong share in secret reconstruction. Moreover, the qudits are obviously vulnerable to eavesdropping. Thus, it is necessary to establish appropriate verification mechanism to detect cheat or eavesdropping. As mentioned above, the proposed scheme uses Eq. (6) as the verification mechanism.

Let consider the error rate of verification mechanism, i.e., the probability that the verification mechanism does not detect wrong secrets.

For correct measurement results R_v and the corresponding sums of random numbers of all participants, $N_v = \sum_{j=1}^{m} p_j{}^v$, $v = 1, 2, 3$, assume that the last participant Bob$_m$ publishes wrong measurements $R_v{}' \neq R_v$, $v = 1, 2, 3$. Obviously, if $(R_1{}' - N_1) = (R_2{}' - N_2)(R_3{}' - N_3) \bmod d$ happens to hold, the wrong measurement results cannot be detected. In this case, the verification mechanism fails, and thus, the other participants recover wrong secrets without being detected.

Obviously, if Bob$_m$ randomly and uniformly chooses three values $R_1{}'$, $R_2{}'$ and $R_3{}'$ in GF(d) as measurement results and publishes them to the other participants, there are totally d^3 tuples of $\{R_1{}', R_2{}', R_3{}'\}$. Note that R_v are published before all participants exchange their random values $p_j{}^v$, $j = 1, 2, \ldots, m$, to obtain the sums N_v. Since each participant Bob$_j$ picks its random values $p_j{}^v$ privately and independently, $N_v = \sum_{j=1}^{m} p_j{}^v$ are indistinguishable from random numbers uniformly distributed in GF(d) in the view of all participants. As a result, $(R_v{}' - N_v)$ are also indistinguishable from random numbers uniformly distributed in GF(d) for participants. In this case, there are totally d^2 randomly selected tuples of $\{R_1{}', R_2{}', R_3{}'\}$ satisfying

$$(R_1{}' - N_1) = (R_2{}' - N_2)(R_3{}' - N_3) \bmod d, \tag{12}$$

because, given $\{N_1, N_2, N_3\}$, $R_3{}'$ can always be determined for randomly selected pairs of $\{R_1{}', R_2{}'\}$.

The result is the same if any other participant cheats by using a wrong share when performing operations on quantum states.

Therefore, the error rate of the verification mechanism is $d^2/d^3 = 1/d$. Since d is a large prime, the error rate converges to 0 when d approaches to infinity.

In conclusion, the scheme can detect the cheat by participants with the probability $(d - 1)/d$, which converges to 100% if d approaches to infinity.

4 Comparisons and discussion

There are many QSS schemes, but most of them are 2-level [10,14–16,22,31,32] and with (n, n) structure [10–20,22]. For instance, in the scheme [22], 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 [14]. 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 schemes, 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 [11] initially prepares a high-fidelity entangled GHZ state with n subsystems. Once the state is produced, the number of participants is fixed. Yu *et al*. presented another QSS [12] 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 [18,33] were proposed based on quantum Fourier transform. The scheme in [18] disguises each share of a secret with true randomness, rather than classical pseudo-randomness. But schemes using entangled states will not be scalable with growing participants. Also 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 system, our scheme enjoys a strong scalability because it is almost not restricted by participant number in realization.

QSS schemes with (t, n) structure were first proposed in 1999 [9] 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. Later, some other threshold schemes are proposed with different physical characteristics, such as those in [25–27] benefit from continuous variable and in [28–30] construct from the ability of exactly distinguishing orthogonal multipartite entangled states under restricted local operation and classical communication. Some schemes [31–35] take advantage of the classical (t, n)-SS, which uses phase shift operation to embed the secret and shares generated from classical (t, n)-SS into processed quantum state, so after sequential operations, participants can collaborate to recover secret.

Compared with these previous schemes in Table 1, our scheme employs d-level unitary operation in association with classical (t, n)-SS. Due to the verification mechanism, it is free from the trusted third party who is responsible for measurement results and any cheat behavior of a participant can be detected easily.

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, in fact, other classical (t, n)-secret sharing schemes, such as linear code based (t, n)-SS [41,42], geometry based (t, n)-SS [2], and Chinese Remainder Theorem based (t, n)-SS [43,44], can also be directly used to construct new threshold QSS schemes based on a single d-level quantum system. All these new schemes share the same features as our proposed scheme. Furthermore, 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 completing its d-level unitary operation on a qudit sequentially, all components c_j, $j = 1, 2, \ldots m$, 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)-SS has the property of cumulative sum, i.e., the secret (i.e., private value in our scheme) s can be expressed as $s = \sum_{j=1}^{m} c_j \bmod M = \sum_{j=1}^{m} a_j s_j \bmod M$, it can be used to construct such a d-level (t, n) threshold quantum secret sharing , where

Table 1 Comparisons with previous QSSs

Schemes	Ref.[1]	Ref.[9]	Ref.[10]	Ref.[31]	Our scheme
Entanglement-free		No	No	Yes	Yes
Scalability	Yes	No	No	Yes	Yes
Level		d	2	2	d
(t, n) threshold	Yes	Yes	No	Yes	Yes
Cheat detection	No	No	No	No	Yes

c_j are the values Bob$_j$ evaluated from the shares s_j and a_j which are some public parameters, $m \geq t$ is the number of participants and M is a modulus.

5 Conclusion

This paper presents a (t, n) threshold QSS scheme based on a 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 to participant number and easy to realize. Security analyses show the scheme is secure against typical attacks. Moreover, a verification mechanism 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 a 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.

Acknowledgements We would like to thank the anonymous reviewer for helpful suggestions. This work is supported by the National Natural Science Foundation of China under Grant Nos. 61572454, 61572453, 61520106007 and Anhui Initiative in Quantum Information Technologies under Grant No. AHY150100.

References

1. Shamir, A.: How to share a secret. Commun. ACM **22**, 612 (1979)
2. Blakley, G.R.: Safeguarding cryptographic keys. In: Proceedings of national computer conference, New York, vol. 313 (1979)
3. Harn, L.: Group authentication. IEEE Trans. Comput. **62**(9), 1893 (2013)
4. Boldyreva, A.: Threshold signatures, multisignatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme. In: Public key cryptography-PKC., vol. 31, Springer, Berlin (2002)
5. Harn, L.: Group-oriented (t, n) threshold digital signature scheme and digital multisignature. IEEE Proc. Comput. Digit. Techn. **141**(5), 307 (1994)
6. Liu, Y.N., Harn, L., Mao, L., Xiong, Z.: Full-healing group-key distribution in online social networks. Int. J. Secur. Netw. **11**(1–2), 12 (2016)
7. Desmedt, Y.G.: Threshold cryptography. Eur. Trans. Telecommun. **5**(4), 449 (1994)
8. Patel, K.: Secure multiparty computation using secret sharing. In: International conference on signal processing, communication, power and embedded system, IEEE, p. 863 (2016)
9. Cleve, R., Gottesman, D., Lo, H.K.: How to share a quantum secret. Phys. Rev. Lett. **83**, 648 (1999)
10. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829 (1999)
11. Yu, I.C., Lin, F.L., Huang, C.Y.: Quantum secret sharing with multilevel mutually (un) biased bases. Phys. Rev. A **78**, 012344 (2008)
12. Bai, C.M., Li, Z.H., Xu, T.T., Li, Y.M.: Quantum secret sharing using the d-dimensional GHZ state. Quantum Inf. Process **16**(3), 59 (2017)
13. Tavakoli, A., Herbauts, I., Zukowski, M., Bourennane, M.: Secret sharing with a single d-level quantum system. Phys. Rev. A **92**, 030302 (2015)
14. Hsu, L.Y.: Quantum secret-sharing protocol based on Grover's algorithm. Phys. Rev. A **68**, 022306 (2003)
15. Guo, G.P., Guo, G.C.: Quantum secret sharing without entanglement. Phys. Lett. A **310**(4), 247–251 (2003)
16. Markham, D., Sanders, B.C.: Graph states for quantum secret sharing. Phys. Rev. A **78**, 042309 (2008)
17. Karimipour, V., Asoudeh, M.: Quantum secret sharing and random hopping: using single states instead of entanglement. Phys. Rev. A **92**, 030301 (2015)
18. Yang, W., Huang, L., Shi, R., He, L.: Secret sharing based on quantum Fourier transform. Quantum Inf. Process **12**(7), 2465 (2013)

19. Lai, H., Luo, M.X., Pieprzyk, J., Li, T., Liu, Z.M., Orgun, M.A.: Large-capacity three-party quantum digital secret sharing using three particular matrices coding. Commun. Theor. Phys. **66**(05), 501–508 (2016)
20. Kogias, I., Xiang, Y., He, Q.Y., Adesso, G.: Unconditional security of entanglement-based continuous-variable quantum secret sharing. Phys. Rev. A **95**, 012315 (2017)
21. Tittel, W., Zbinden, H., Gisin, N.: Experimental demonstration of quantum secret sharing. Phys. Rev. A **63**(4), 042301 (2001)
22. Schmidt, C., Trojek, P., Bourennane, M., Kurtsiefer, C., Zukowski, M., Weinfurter, H.: Experimental single qubit quantum secret sharing. Phys. Rev. Lett. **95**, 230505 (2005)
23. Chen, Y.A., Zhang, A.N., Zhao, Z., Zhou, X.Q., Lu, C.Y., Peng, C.Z.: Experimental quantum secret sharing and third-man quantum cryptography. Phys. Rev. Lett **95**(20), 200502 (2005)
24. Lu, H., Zhang, Z., Chen, L.K., Li, Z.D., Liu, C., Li, L.: Secret sharing of a quantum state. Phys. Rev. Lett **117**(3), 030501 (2016)
25. Lance, A.M., Symul, T., Bowen, W.P., Tyc, T., Sanders, B.C., Lam, P.K.: Continuous variable (2, 3) threshold quantum secret sharing schemes. New J. Phys. **5**, 4 (2003)
26. Lau, H.K., Weedbrook, C.: Quantum secret sharing with continuous-variable cluster states. Phys. Rev. A **88**, 042313 (2013)
27. Wu, Y., Cai, R., He, G., Zhang, J.: Quantum secret sharing with continuous variable graph state. Quantum Inf. Process. **13**, 1085 (2014)
28. Rahaman, R., Parker, M.G.: Quantum scheme for secret sharing based on local distinguishability. Phys. Rev. A **91**, 022330 (2015)
29. Yang, Y.H., Gao, F., Wu, X., Qin, S.J., Zuo, H.J., Wen, Q.Y.: Quantum secret sharing via local operations and classical communication. Sci. Rep. **5**, 16967 (2015)
30. Wang, J., Li, L., Peng, H., Yang, Y.: Quantum-secret-sharing scheme based on local distinguishability of orthogonal multiqudit entangled states. Phys. Rev. A **95**, 022320 (2017)
31. Tokunaga, Y., Okamoto, T., Imoto, N.: Threshold quantum cryptography. Phys. Rev. A **71**, 012314 (2005)
32. Qin, H., Zhu, X., Dai, Y.: (t, n) Threshold quantum secret sharing using the phase shift operation. Quantum Inf. Process **14**(8), 2997–3004 (2015)
33. Song, X.L., Liu, Y.B., Deng, H.Y., Xiao, Y.G.: (t, n) Threshold d-level quantum secret sharing. Sci. Rep. **7**, 6366 (2017)
34. Lu, C.B., Miao, F.Y., Meng, K.J., Yu, Y.: Threshold quantum secret sharing based on single qubit. Quantum Inf. Process. **17**(3), 64 (2018)
35. Lai, H., Zhang, J., Luo, M.X., Pan, L., Pieprzyk, J., Xiao, F.Y., Orgun, M.A.: Hybrid threshold adaptable quantum secret sharing scheme with reverse Huffman–Fibonacci tree coding. Sci. Rep. **6**, 31350 (2016)
36. Ivanovic, I.D.: Geometrical description of quantal state determination. J. Phys. A **14**, 3241 (1981)
37. Wootters, W.L., Fields, B.D.: Optimal state-determination by mutually unbiased measurements. Ann. Phys. **191**, 363 (1989)
38. Miao, F.Y., Xiong, Y., Wang, X.F., Badawy, M.: Randomized component and its application to (t, m, n)-group oriented secret sharing. IEEE Trans. Inf. Forensics Secur. **10**(5), 889–899 (2015)
39. Gao, F., Qin, S.J., Wen, Q.Y.: A simple participant attack on the Bradler–Dusek protocol. Quantum Inf. Comput. **7**(4), 329 (2007)
40. He, G.P.: Comment on experimental single qubit quantum secret sharing. Phys. Rev. Lett. **98**, 028901 (2007)
41. McEliece, R.J., Sarwate, D.V.: On sharing secrets and Reed–Solomon codes. Commun. ACM **24**(9), 583 (1981)
42. Massey, J.L.: Minimal codewords and secret sharing. In: Proceedings of the 6th joint Swedish–Russian international workshop on information theory. IEEE Press, Washington DC, vol. 276 (1993)
43. Asmuth, C., Bloom, J.: A modular approach to key safeguarding. IEEE Trans. Inf. Theory **30**(2), 208 (1983)
44. Mignotte, M.: How to share a secret. In: Conference on cryptography, Springer, Berlin vol. 149, 371 (1982)