SCIENTIFIC REPORTS

OPEN

(t, n) Threshold d-Level Quantum Secret Sharing

Xiu-Li Song[1], Yan-Bing Liu[1], Hong-Yao Deng[2] & Yong-Gang Xiao[1]

Received: 31 January 2017
Accepted: 13 June 2017
Published online: 25 July 2017

Most of Quantum Secret Sharing(QSS) are (n, n) threshold 2-level schemes, in which the 2-level secret cannot be reconstructed until all n shares are collected. In this paper, we propose a (t, n) threshold d-level QSS scheme, in which the d-level secret can be reconstructed only if at least t shares are collected. Compared with (n, n) threshold 2-level QSS, the proposed QSS provides better universality, flexibility, and practicability. Moreover, in this scheme, any one of the participants does not know the other participants' shares, even the trusted reconstructor Bob_1 is no exception. The transformation of the particles includes some simple operations such as d-level CNOT, Quantum Fourier Transform(QFT), Inverse Quantum Fourier Transform(IQFT), and generalized Pauli operator. The transformed particles need not to be transmitted from one participant to another in the quantum channel. Security analysis shows that the proposed scheme can resist intercept-resend attack, entangle-measure attack, collusion attack, and forgery attack. Performance comparison shows that it has lower computation and communication costs than other similar schemes when $2 < t < n - 1$.

A dealer who wants to share a secret among a group of participants, usually splits the secret into a few pieces. These pieces of the secret is called shares, which are distributed to different participants, and a share is only held by a participant. The secret can be reconstructed only when enough participants collaborate together. This is the basic idea of Secret Sharing (SS) in modern cryptography. A significant role of SS is that it protects secret information from being lost, destroyed, or altered. Therefore, SS is widely applied to threshold signature, threshold cryptography, secure multi-party computation, and group key management, etc.

Quantum Secret Sharing (QSS) is the expansion of SS in the quantum cryptography field, and the difference between the two is that QSS' security is based on the fundamental principle of quantum physics. As a cryptographic scheme, QSS uses quantum information to deal with the problem of sharing classical or quantum secret. That is to say, the dealer distributes a secret that may be classical message or an unknown quantum state among a group of participants, and reconstructing the secret need a certain number of participants to collaborate together. The first QSS scheme was proposed by Hillery *et al.*[1] in 1999, based on Greenberger-Home-Zeilinger(GHZ) state. Since then, many design and analysis schemes on QSS have been proposed[2–20] such as circular QSSs[2–4], dynamic QSSs[5,6], single particle QSSs[7–9], graph state QSSs[10–12], verifiable QSSs[13–15], and other QSSs that may be based on Calderbank–Shor–Steane codes[16], or based on phase shift operation[17–19], or based on quantum search algorithm[20].

According to different threshold, the existing QSS schemes can be classified into two categories: (n, n) QSS[2–12,18–20] and (t, n) QSS[10,11,13–17]. For the former, the secret cannot be reconstructed until all n shares are collected. For the latter, the secret can be reconstructed only if at least t shares are collected. Furthermore, these QSS schemes can be fallen into two categories: 2-level QSS[2–6,10,12,17–20] and d-level QSS[7–9,11] depending on the dimension of Hilbert space. For the former, the quantum secret and its shares are all in 2 dimension Hilbert space. For the latter, the dimension of the quantum states is more than 2, that is $d > 2$. In general, QSS uses different levels of authority to control the participants' access privileges. Though each participant holds a share, only the qualified subsets of the participants can reconstruct the secret. All the qualified subsets are decided according to different application requirements. Each qualified subset may have different number of participants, and a participant may belong to several qualified subsets. To the (t, n) threshold QSS scheme, the number of participants of each qualified subset is t.

Compared with (n, n) QSS, the design of (t, n) QSS is more complex, because it need employ the technologies such as graph state or error-correcting encoding. In term of practice, (t, n) QSS is more flexible, because the reconstruction of a secret for (t, n) QSS need at least t participants whereas for (n, n) QSS must be n participants. Compared to 2-level QSS, the design of d-level QSS is more difficult. The main reason is that the operations of the quantum computational cell need higher dimensional unitary operations, such as quantum Fourier transform

[1]Chongqing University of Posts and Telecommunications, School of Computer Science and Technology, Chongqing, 400065, China. [2]Yangtze Normal University, College of Computer Engineering, Chongqing, 408000, China. Correspondence and requests for materials should be addressed to X.-L.S. (email: songxl@cqupt.edu.cn)

(QFT), d-dimensional Pauli operations, etc. In addition, the universality and practicability of d-level QSS are better than that of 2-level QSS, because the dimension of Hilbert space may be d, which is higher than 2.

Inspired by the flexibility of (t, n) threshold and the universality of d-level, in this paper, we propose a (t, n) threshold d-level QSS scheme. The scheme has generic properties of (t, n) threshold SS, e.g., the dealer Alice distributes n shares to n participants, and each participant only holds a share; any t out of the n participants can reconstruct the original secret. In addition, compared with the existing QSS schemes, the proposed QSS has better properties as follows. Owing to items 1 and 2, it provides lower computation cost; owing to item 3, it provides lower communication cost; owing to item 4, it is safer in resisting some common attacks.

- There only exist simple operations such as quantum Fourier transform (QFT) and generalized Pauli operator. The complex operations, e.g., the graph state or error-correcting encoding, do not appear in our scheme;
- Only the participant Bob_1 need apply quantum Fourier transform (QFT) to his own particle, other participants do not need;
- It is unnecessary to transmit the quantum particles from one participant to the next in order;
- Any one of the participants does not know the other participants' shares, even the trusted reconstructor Bob_1 is no exception.

Preliminaries

In this section, the related preliminaries are introduced including quantum Fourier transform (QFT) and inverse quantum Fourier transform (IQFT), generalized Pauli operator, and Shamir's (t, n) threshold SS. These preliminaries will be used in presenting (t, n) threshold QSS scheme.

Quantum Fourier Transform and Inverse Quantum Fourier Transform.

Definition 1. Quantum Fourier transform (QFT), a quantum version of the standard discrete Fourier transform, is a unitary transformation of d-level quantum system. For $y, x \in \{0, 1, \ldots, d-1\}$, the QFT is defined by refs 21 and 22

$$QFT|y\rangle = \frac{1}{\sqrt{d}}\sum_{x=0}^{d-1}\omega^{y\cdot x}|x\rangle, \tag{1}$$

where $\omega = e^{2\pi i/d}$ is a primitive d-th root of unity.

Definition 2. For $x, y \in \{0, 1, \ldots, d-1\}$, the inverse quantum Fourier transform (IQFT) is defined by

$$QFT^{-1}|x\rangle = \frac{1}{\sqrt{d}}\sum_{y=0}^{d-1}\omega^{-x\cdot y}|y\rangle. \tag{2}$$

Between the QFT and the IQFT, there exists the relationship given by

$$QFT^{-1}(QFT|y\rangle) = QFT^{-1}(\frac{1}{\sqrt{d}}\sum_{x=0}^{d-1}\omega^{y\cdot x}|x\rangle) = |y\rangle. \tag{3}$$

Pauli Operator.

Definition 3. On Hilbert space of d-level quantum system, the generalized Pauli operator is defined by ref. 23

$$U_{\alpha,\beta} = \sum_{x=0}^{d-1}\omega^{\beta\cdot x}|x+\alpha\rangle\langle x|, \tag{4}$$

where $\alpha, \beta \in \{0, 1, \ldots, d-1\}$.

In particular, on Hilbert space of d-level quantum system, the X gate and Z gate are represented by ref. 24

$$X = U_{1,0} = \sum_{x=0}^{d-1}|x+1\rangle\langle x|, \quad Z = U_{0,1} = \sum_{x=0}^{d-1}\omega^{x}|x\rangle\langle x|. \tag{5}$$

Shamir's (t, n) threshold SS.

Definition 4. Suppose that there are a trusted dealer and n participants $P = \{P_1, P_2, \ldots, P_n\}$, Shamir's (t, n) threshold SS[25] consists of the following two algorithm:

Share generation algorithm: The dealer randomly chooses a polynomial with degree $t-1$: $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{t-1}x^{t-1}$, where $(a_0, a_1, \ldots, a_{t-1}) \in Z_d^t$, and a_0 is a secret. The dealer computes n shares $f(x_i)$ for $(i = 1, 2, \ldots, n)$, then he/she sends n shares to n participants via a secure channel, and each participant P_i holds only a share $f(x_i)$.

Secret reconstruction algorithm: There are n distinct points $\{(x_i, f(x_i))|i = 1, 2, \ldots, n\}$ on the polynomial $f(x)$ in the 2-dimensional plane, so if and only if at least t points $\{(x_r, f(x_r))|r = 1, 2, \ldots, t\}$ are given, the polynomial $f(x)$ can be reconstructed by using the Lagrange interpolation formula as follows

$$f(x) = \sum_{r=1}^{t} f(x_r)\prod_{1\le j\le t, j\ne r}\frac{x-x_j}{x_j-x_r}. \tag{6}$$

If any t out of the n participants, denoted by $R = \{P_1, P_2, \ldots, P_t\}$, take out their shares $(x_r, (f(x_r)))$ *for* $(r = 1, 2, \ldots, t)$. Then the t participants can reconstruct the original secret a_0 based on the above Equation (6)

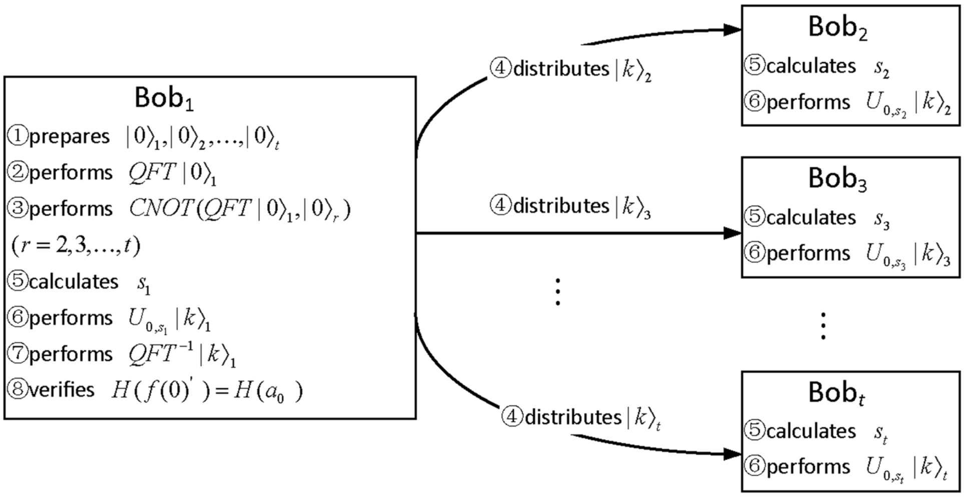
Bob$_1$
①prepares $|0\rangle_1, |0\rangle_2, \ldots, |0\rangle_t$
②performs $QFT\,|0\rangle_1$
③performs $CNOT(QFT\,|0\rangle_1, |0\rangle_r)$
$(r = 2, 3, \ldots, t)$
⑤calculates s_1
⑥performs $U_{0,s_1}\,|k\rangle_1$
⑦performs $QFT^{-1}\,|k\rangle_1$
⑧verifies $H(f(0)') = H(a_0)$
④distributes $|k\rangle_2$
④distributes $|k\rangle_3$
④distributes $|k\rangle_t$
Bob$_2$
⑤calculates s_2
⑥performs $U_{0,s_2}\,|k\rangle_2$
Bob$_3$
⑤calculates s_3
⑥performs $U_{0,s_3}\,|k\rangle_3$
Bob$_t$
⑤calculates s_t
⑥performs $U_{0,s_t}\,|k\rangle_t$

Figure 1. Reconstruction process of the original secret.

$$a_0 = f(0) = \sum_{r=1}^{t} f(x_r) \prod_{1 \le j \le t, j \ne r} \frac{x_j}{x_j - x_r}. \tag{7}$$

Results

The Proposed QSS Scheme.

Suppose that Alice is a dealer, and $B = \{Bob_1, Bob_2, \ldots, Bob_n\}$ is a set of n participants. Alice chooses any one of the participants Bob_1 as a trusted reconstructor. The role of Bob_1 is to collect any t shares from n participants and reconstruct the final secret. The proposed QSS scheme consists of three phases: initialization phase, share distribution phase, and secret reconstruction phase.

Initialization Phase. Alice first finds a suitable prime d satisfying $n \le d \le 2n$ and sets a finite field Z_d. To divide a secret $a_0 \in Z_d$ into n pieces, Alice randomly picks a polynomial with degree $t - 1$: $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{t-1}x^{t-1}$, where the coefficients $a = (a_1, \ldots, a_{t-1}) \in Z_d^{t-1}$ are randomly chosen, and the symbol $+$ means addition modulo d.

Share Distribution Phase. Similar to Share generation algorithm of Shamir's (t, n) threshold SS, Alice selects n distinct and nonzero values $x_i \in Z_d$ to compute n shares $f(x_i) \in Z_d$ for $(i = 1, 2, \ldots, n)$, and then she publishes all x_i. Each classical share $f(x_i)$ can be encoded in a random qubit string according to the encoding method of BB84 protocol[26] or other secure quantum key distribution (QKD) protocols. After having finished the encoding procedure, Alice distributes sequentially the qubit string of $f(x_i)$ to the corresponding participant Bob_i for $(i = 1, 2, \ldots, n)$ via a secure quantum channel. That is to say, each participant Bob_i holds a share $f(x_i)$. After having finished the distribution procedure of the qubit strings of all shares, the secret a_0 is shared among a group of participants. In addition, Alice selects a Hash function $H()$ such as $SHA1$ to compute hash value $H(a_0)$, and sends it to the participant Bob_1.

Secret Reconstruction Phase. we assume that all qualified subsets of the participants are decided according to the specific application scenario, and the number of participants of each qualified subset is t. On a certain day, the secret a_0 need to be reconstructed, any one of all qualified subsets is selected due to the absence of some participants. For simplicity of description, we assume that the selected qualified subset is denoted by $R = \{Bob_1, Bob_2, \ldots, Bob_t\}$. Figure 1 shows the reconstruction process of the original secret. In the process, each participant $Bob_r(r = 2, 3, \ldots, t)$ performs the steps 5 and 6, and Bob_1 performs the steps 1–8. The details of the reconstruction process are described as follows.

Step 1. As a trusted participant, Bob_1 prepares t qudit particles $|0\rangle_1, |0\rangle_2, \ldots, |0\rangle_t$, and each particle has m qubit, where $m = \lceil \log_2 d \rceil$.

Step 2. Let $|0\rangle, |1\rangle, \ldots, |d - 1\rangle$ be a standard orthonormal basis of a d-level quantum system and set a QFT based on this orthonormal basis. When Bob_1 applies the QFT to the first particle $|0\rangle_1$, the composite state $|\varphi_1\rangle$ of t particles is denoted by

$$\begin{aligned}|\varphi_1\rangle &= (QFT|0\rangle_1)\,|0\rangle_2|0\rangle_3\cdots|0\rangle_t\\ &= \left(\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{0\cdot k}|k\rangle_1\right)|0\rangle_2|0\rangle_3\cdots|0\rangle_t\\ &= \left(\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}|k\rangle_1\right)|0\rangle_2|0\rangle_3\cdots|0\rangle_t,\end{aligned} \tag{8}$$

where $\omega = e^{2\pi i/d}$ is a primitive d-th root of unity.

Step 3. Bob_1 performs respectively d-level $CNOT$ operation on the particle $|0\rangle_r$ for ($r = 2, 3, \ldots, t$). Where ($QFT|0\rangle_1$) is the control qudit and $|0\rangle_r$ is the target qudit. After performed ($t-1$) $CNOT$ operations by Bob_1, the state $|\varphi_1\rangle$ evolves as an entangled state

$$\begin{aligned}|\varphi_2\rangle &= (CNOT((QFT|0\rangle_1),\,|0\rangle_2)) \otimes (CNOT((QFT|0\rangle_1),\,|0\rangle_3)) \otimes \cdots \otimes (CNOT((QFT|0\rangle_1,\,|0\rangle_t)))\\ &= \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}|k\rangle_1|k\rangle_2|k\rangle_3\cdots|k\rangle_t.\end{aligned} \tag{9}$$

Step 4. Bob_1 sends respectively the particle $|k\rangle_r(r = 2, 3, \ldots, t)$ to the corresponding participant Bob_r through the authenticated quantum channel.

Step 5. After all participants have received their particles, each participant $Bob_r(r = 1, 2, \ldots, t)$ takes out his share $f(x_r)$ and calculates respectively the following value

$$s_r = f(x_r)\prod_{1\le j\le t, j\ne r}\frac{x_j}{x_j - x_r}\ mod\ d. \tag{10}$$

For convenience, the s_r is named shadow of the share $f(x_r)$.

Step 6. Each participant $Bob_r(r = 1, 2, \ldots, t)$ performs a generalized Pauli operator U_{0,s_r} on his particle $|k\rangle_r$, where U_{0,s_r} is defined by

$$U_{0,s_r} = \sum_{k=0}^{d-1}\omega^{s_r\cdot k}|k\rangle_{r\,r}\langle k|. \tag{11}$$

After the Pauli operator U_{0,s_r} ($r = 1, 2, \ldots, t$) is performed on each particle, the state $|\varphi_2\rangle$ evolves as

$$\begin{aligned}|\varphi_3\rangle &= \frac{1}{\sqrt{d}}\textstyle\sum_{k=0}^{d-1}\omega^{s_1\cdot k}|k\rangle_1\omega^{s_2\cdot k}|k\rangle_2\omega^{s_3\cdot k}|k\rangle_3\cdots\omega^{s_t\cdot k}|k\rangle_t\\ &= \frac{1}{\sqrt{d}}\textstyle\sum_{k=0}^{d-1}\omega^{(\sum_{r=1}^{t}s_r)\cdot k}|k\rangle_1|k\rangle_2|k\rangle_3\cdots|k\rangle_t\end{aligned}\ . \tag{12}$$

Step 7. Bob_1 applies QFT^{-1} to his own particle $|k\rangle_1$ and further measures it in the computational basis to obtain the secret $f(0)' = \sum_{r=1}^{t}s_r\ mod\ d$.

Step 8. Bob_1 first computes the hash value $H(f(0)')$ using a hash function $H()$, and then verifies $H(f(0)') = H(a_0)$. If the equation holds, he shares the secret with other participants; otherwise he thinks that there is at least one dishonest participant and ends the reconstruction phase.

Correctness Proof.

The proposed (t, n) threshold QSS is proven in this section. The proof of correctness will focus primarily on Equation (12) of Step 6 and the secret recovery of Step 7.

Lemma 1. If the Pauli operator $U_{0,s_r} = \sum_{k=0}^{d-1}\omega^{s_r\cdot k}|k\rangle_{r\,r}\langle k|$ is performed on the particle $|k\rangle_r$ $(r = 1, 2, \ldots, t)$ of the orthogonal entangled state $|\varphi_2\rangle$ of Equation (9) by the participant $Bob_r(r = 1, 2, \ldots, t)$, the state $|\varphi_2\rangle$ evolves as $|\varphi_3\rangle$ of Equation (12).

Proof. When the Pauli operator $U_{0,s_r} = \sum_{k=0}^{d-1}\omega^{s_r\cdot k}|k\rangle_{r\,r}\langle k|$ is performed on the particle $|k\rangle_r$ of the state $|\varphi_2\rangle$ of Equation (9) for ($r = 1, 2, \ldots, t$), the state $|\varphi_2\rangle$ evolves as

$$\begin{aligned}|\varphi_3\rangle &= \frac{1}{\sqrt{d}}\textstyle\sum_{k=0}^{d-1}U_{0,s_1}|k\rangle_1 \otimes U_{0,s_2}|k\rangle_2 \otimes \cdots \otimes U_{0,s_r}|k\rangle_t\\ &= \frac{1}{\sqrt{d}}\textstyle\sum_{k=0}^{d-1}\omega^{s_1\cdot k}|k\rangle_{11}\langle k|k\rangle_1\omega^{s_2\cdot k}|k\rangle_{22}\langle k|k\rangle_2\cdots\omega^{s_t\cdot k}|k\rangle_{tt}\langle k|k\rangle_t\\ &= \frac{1}{\sqrt{d}}\textstyle\sum_{k=0}^{d-1}\omega^{s_1\cdot k}|k\rangle_1\omega^{s_2\cdot k}|k\rangle_2\cdots\omega^{s_t\cdot k}|k\rangle_t\\ &= \frac{1}{\sqrt{d}}\textstyle\sum_{k=0}^{d-1}\omega^{(s_1+s_2+\cdots+s_t)\cdot k}|k\rangle_1|k\rangle_2\cdots|k\rangle_t\\ &= \frac{1}{\sqrt{d}}\textstyle\sum_{k=0}^{d-1}\omega^{(\sum_{r=1}^{t}s_r)\cdot k}|k\rangle_1|k\rangle_2\cdots|k\rangle_t.\end{aligned} \tag{13}$$

Lemma 2. If QFT^{-1} is applied to the particle $|k\rangle_1$ of the state $|\varphi_3\rangle$ of Equation (12), the measurement output of the transformed particle is the original secret $f(0) = \sum_{r=1}^{t} s_r \ mod \ d$.

Proof. Based on Equation (10) and Lagrange interpolation formula of Equation (7), *f*(0) can be calculated by

$$\begin{aligned} f(0) &= (f(x_1)\prod\nolimits_{1\le j\le t, j\ne 1}\frac{x_j}{x_j - x_1} + f(x_2)\prod\nolimits_{1\le j\le t, j\ne 2}\frac{x_j}{x_j - x_2} + \cdots \\ &\quad + f(x_t)\prod\nolimits_{1\le j\le t, j\ne t}\frac{x_j}{x_j - x_t}) \ mod \ d \\ &= (s_1 + s_2 + \cdots + s_t) \ mod \ d \\ &= \left(\sum\nolimits_{r=1}^{t} s_r\right) mod \ d. \end{aligned} \tag{14}$$

According to the Equation (3), Bob_1 applies QFT^{-1} to the first particle of the state $|\varphi_3\rangle$ of Equation (12) and obtains

$$\begin{aligned} &QFT^{-1}(\frac{1}{\sqrt{d}}\sum\nolimits_{k=0}^{d-1}\omega^{(\sum_{r=1}^{t} s_r)\cdot k}|k\rangle_1) \\ &= |\sum\nolimits_{r=1}^{t} s_r \ mod \ d\rangle \\ &= |f(0)\rangle. \end{aligned} \tag{15}$$

When Bob_1 further measures the first particle in his hand, the measurement output is original secret *f*(0).

Security Analysis.

In this section, the security of the proposed (t, n) threshold QSS scheme is analyzed. The security analysis focuses primarily on intercept-resend attack, entangle-measure attack, collusion attack, and forgery attack.

Intercept-Resend Attack. Without loss of generality, Eve is assumed as an eavesdropper, who has unlimited computing power whose technology is only limited by the laws of quantum mechanics. Suppose Eve controls the quantum channel and intercepts any one quantum particle on the way from Bob_1 to $Bob_r(r \in \{2, 3, \ldots, t\})$ in Step 4, then she measures the intercepted particle by using the computational basis $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$. With the probability of $1/d$ she can succeed with the attack and get $k(k \in \{0, 1, \ldots, d-1\})$. Further she prepares a new particle that is the same as the intercepted one, and then resends the new particle to $Bob_r(r \in \{2, 3, \ldots, t\})$. Unfortunately, the measurement outcome k does not contain any information about private share $f(x_r)$ or its shadow s_r. Therefore, Eve cannot get any valuable information in the intercept-resend attack.

Entangle-Measure Attack. In entangle-measure attack, the eavesdropper Eve may use a unitary operation to entangle an ancillary particle on the intercepted one, and then measures the ancillary particle to obtain valuable information. Suppose Eve intercepts all $t-1$ particles transmitted from Bob_1 to $Bob_r(r \in \{2, 3, \ldots, t\})$, and then prepares an ancillary particle $|e\rangle_a(e \in \{0,1, \ldots, d-1\})$. Further, she entangles the ancillary particle $|e\rangle_a$ on any one of the intercepted particles such as $|k\rangle_u$ by using d-level $CNOT$ operation, where $|k\rangle_u$ is the control qudit and $|e\rangle_a$ is the target qudit. The state $|\varphi_2\rangle$ of Equation (9) evolves as $|\varphi_2\rangle'$

$$\begin{aligned} |\varphi_2\rangle' &= (CNOT(|k\rangle_u, |e\rangle_a))\,|\varphi_2\rangle \\ &= \frac{1}{\sqrt{d}}\sum\nolimits_{k=0}^{d-1}|k\rangle_1|k\rangle_2\cdots|k\rangle_u\cdots|k\rangle_t|k\oplus e\rangle_a. \end{aligned} \tag{16}$$

Next step, Eve chooses another particle $|k\rangle_v$ as control particle to perform d-level $CNOT$ operation on the target particle $|e\rangle_a$. Now the state $|\varphi_2\rangle'$ evolves as $|\varphi_2\rangle''$

$$\begin{aligned} |\varphi_2\rangle'' &= (CNOT(|k\rangle_v, |k\oplus e\rangle_a))\,|\varphi_2\rangle' \\ &= \frac{1}{\sqrt{d}}\sum\nolimits_{k=0}^{d-1}(|k\rangle_1|k\rangle_2\cdots|k\rangle_v\cdots|k\rangle_t|k\oplus k\oplus e\rangle_a. \\ &= |\varphi_2\rangle|e\rangle_a \end{aligned} \tag{17}$$

It can be seen that the ancillary particle $|e\rangle_a$ is disentangled out from the entangled state $|\varphi_2\rangle'$, and the original state $|\varphi_2\rangle$ is not changed. If Eve measures the ancillary particle $|e\rangle_a$, she obtains e, which is the same as prepared at the beginning. From this, Eve can come to the conclusion that the particles $|k\rangle_u$ and $|k\rangle_v$ are the same.

Suppose Eve takes each intercepted particle $|k\rangle_r(r = 2, 3, \ldots, t)$ as control particle respectively, and $|e\rangle_a$ as target particle to perform d-level $CNOT$ operation. As a result, she finds all particles $|k\rangle_2, |k\rangle_3, \ldots, |k\rangle_t$ are the same. Similar to the entangle-measure attack, the measurement outcome of the particle $|k\rangle_r(r = 2, 3, \ldots, t)$ does not contain any information about private share $f(x_r)$ or its shadow s_r. Therefore, Eve cannot also get any valuable information in the entangle-measure attack, only knowing that all transmitted particles $|k\rangle_2, |k\rangle_3, \ldots, |k\rangle_t$ are the same.

Collusion Attack. As is known to all, QSS scheme uses the qualified subsets to prevent collusion attack of the participants. After analyzing the existing QSS schemes, we find some schemes cannot resist collusion attack, in which some participants can collude to get the private information of other participants. That is to say, in these QSS schemes, by getting rid of several qualified participants, the unqualified subsets of participants can reconstruct the original secret. Classifying collusion attacks of the existing QSS schemes, the study focuses on the following cases.

Case 1: Collusion attack of Bob_{e-1} and Bob_{e+1}

In refs 17, 22 and 27, if Bob_{e-1} and Bob_{e+1} are dishonest, they can collude to get the private information of Bob_e. The reason is that the refs 17, 22 and 27 have the same security loopholes: the private information of the previous participant is transformed by using the unitary operation, and then it is transmitted to the next participant. If Bob_{e-1} and Bob_{e+1} collaborate, Bob_{e-1} may send the particle transformed by himself such as $U_{e-1}|k\rangle_{e-2}$ to Bob_{e+1}. As a result, Bob_{e+1} not only holds the particle $U_{e-1}|k\rangle_{e-2}$ transmitted by Bob_{e-1}, but also holds the particle $U_eU_{e-1}|k\rangle_{e-2}$ transmitted by Bob_e. Given this, Bob_{e+1} can calculate out U_e operation of Bob_e, and further he can deduce the private information of Bob_e.

Case 2: Collusion attack of the first participant Bob_1 and the last participant Bob_n

As ref. 6 pointed out there exists a security loophole in the dynamic QSS of ref. 5, i.e., the first participant and the last one can collude to obtain the master key of the dealer without the other participants' cooperation. Ref. 4 also found that the circular QSS of ref. 3 is not secure as the first participant and the last one can illegally obtain the secret messages without introducing any error. The refs 3 and 5 also have the same security loopholes: the dealer and n participants transmit the transformed private information one by one. The transmission route forms a circle, in which the first participant is at the left of the dealer, and the last one is at the right of the dealer. If the first participant colludes with the last one, they can obtain the dealer's private information.

Case 1 never happens in the proposed (t, n) threshold QSS scheme, because each participant performs unitary operation with private information in his own lab, and the transformed private information is not transmitted via the quantum channel. Case 2 never also happens in the proposed (t, n) threshold QSS scheme, because the dealer (*Alice*) and reconstructor (Bob_1) do not take part in the circular transmission route, and their private information are not passed from one participant to the next but saved in their own hands. Therefore, as long as the dealer (*Alice*) and the reconstructor (Bob_1) are both trusted entities, the proposed QSS scheme can resist collusion attack.

Forgery Attack. For secret sharing scheme, as always, it is an issue of public concern to prevent the participants from providing fake shares or shadows. In SS, Feldman[28] first studied this problem and proposed a verifiable secret sharing, in which each participant's share can be verified publicly. In QSS, Yang *et al.*[13, 14] proposed two verifiable schemes to check whether some dishonest participants provide fake shares. Song *et al.*[15] pointed out the forged quantum particles can pass the verification of other participants in ref. 13 and further proposed an new verifiable QSS scheme to improve the original one. From here we can see that verifiable QSS must provide validation function to resist forgery attack of the participants.

In the proposed QSS scheme, in order to resist forgery attack, the reconstructor Bob_1 uses hash function $H()$ to certify the authenticity of the secret. During the secret reconstruction phase, if a dishonest participant $Bob_e(e \in \{2, 3, \ldots, t\})$ performs Pauli operator $U_{0,s_{e'}}$ with a fake shadow $s_{e'}$ instead of his true s_e, though other participants provide the correct information, the original secret a_0 cannot be recovered correctly. In Step 8 of the secret reconstruction phase, when Bob_1 calculates out the secret $f(0)'$ and verifies it by checking the equation $H(f(0)') = H(a_0)$, he finds that the equation does not hold. He thinks that at least one dishonest participant has provided a fake shadow, and he terminates the reconstruction process and does not share the wrong secret $f(0)'$ with other participants. Therefore, the forgery attack of the participant Bob_e is infeasible.

Performance Analysis and Comparison. In this section, the performance of the proposed QSS scheme is analyzed and compared with five other similar schemes: Yang *et al.*'s QSS of ref. 7, Qin *et al.*'s QSS of ref. 17, Shi *et al.*'s protocol I and protocol III of ref. 22, and Li *et al.*'s QSS of ref. 27. The performance analysis and comparison of the six similar schemes can be viewed from the following three aspects: universality and practicability, computation cost, and communication cost.

Universality and Practicability. In ref. 7, Yang *et al.* prepares an n-particle entangled state to design their protocol, and each participant holds a d-level particle. In ref. 17, the dealer prepares a multi-particle sequence, in which each particle is 2-level. In the protocol I and III of ref. 22, the initiator who is taken as one of the participants prepares a d-level 2-particle entangled state, and each of other $n-1$ participants prepares respectively a d-level single particle. In ref. 27, the dealer prepares an ordered sequence of multiple EPR pairs. In the proposed QSS, the participant Bob_1 prepares a t-particle entangled state by using d-level *CNOT* operation, and each participant holds a d-level particle.

We assume that the number of the prepared single particles or EPR pairs is the same as that of the participants who reconstruct the secret in the six similar schemes. In ref. 7 and the proposed scheme, each participant holds a particle, and each particle has m qubits, where $m = \lceil \log_2 d \rceil$. As Table 1 shows, ref. 7 need prepare mn qubits, and the proposed QSS need prepare mt qubits. In the protocol I of ref. 22, the total number of the prepared particles is $n+1$, so that is $m(n+1)$ qubits. In the protocol III of ref. 22, the number of the prepared qubits is $mn(n+1)$. In ref. 17, Alice need prepare t particles, so that is mt qubits. In ref. 27, Alice need prepare t EPR pairs, so that is $2mt$ qubits.

Property	Ref. 7	Ref. 17	I of Ref. 22	III of Ref. 22	Ref. 27	The proposed QSS
(t, n) or (n, n)	(n, n)	(t, n)	(n, n)	(n, n)	(t, n)	(t, n)
Level	d	2	d	d	2	d
Qubits	mn	mt	$m(n+1)$	$mn(n+1)$	$2mt$	mt

Table 1. Comparison of universality and practicability.

Operations of the entities	Ref. 7	Ref. 17	I of Ref. 22	III of Ref. 22	Ref. 27	The proposed QSS
QFT	n		1	$n+1$		1
U operation	$nU_{s_r,0}$	$t(t+1)\,U(\theta)$	$(n-1)\,U^j$	$(n^2-1)\,U^j$	$t(2t-1)\,U_{i,j}$	tU_{0,s_r}
QFT^{-1}			1	$n+1$		1
Measure operation (M)	n		2	$2(n+1)$	t	1
Hash operation (H)						$2H$

Table 2. Comparison of computation costs.

From the Table 1 we can see that refs 17 and 27 and the proposed QSS are (t, n) schemes, and the three other QSSs are (n, n) schemes. Ref. 7, the protocol I and III of ref. 22, and the proposed QSS are d-level schemes, and the two other QSSs are 2-level schemes. The proposed QSS scheme has not only the merits of (t, n) scheme but also the merits of d-level scheme. It should has better flexibility, universality and practicability than the five other QSS schemes. Moreover, the proposed QSS prepares the same number of the particles as ref. 17, and both schemes can save more resources on the prepared particles than the four other similar schemes.

Computation Cost. Ref. 7 does not show how to prepare an n-particle entangled state, and ref. 27 also does not describe how to prepare an ordered sequence of t EPR pairs. Therefore, in order to make a simplified comparison, we do not consider computation cost of preparing the particles in the protocol I and III of ref. 22 and the proposed QSS scheme. Refs 17 and 27 and the proposed QSS describe the generation process of the shares, however, refs 7 and 22 make no reference to it. Also we do not consider computation cost of the generation process of the shares. In refs 17 and 27, each particle is 2-level. Differently, in refs 7 and 22 and the proposed QSS, each particle is d-level. To be convenient for comparison, the particle dimension d is to be set to 2, thus $m = \lceil \log_2 d \rceil = 1$.

The computation costs of the six similar schemes are shown in Table 2. In ref. 7, each participant first performs QFT on his particle $|k\rangle_r (r = 1, 3, \ldots, n)$, and then applies $U_{s_r,0}|k\rangle$ to the particle $QFT|k\rangle_r$, further measures the transformed particle in his lab. The total computation cost is $nQFT + nU_{s_r,0} + nM$.

In ref. 17, the dealer Alice performs $U(\theta_a)$ on every particle of the sequence ψ_0, and then sends the transformed sequence to the participant Bob_i. For $r = 1, 2, \ldots, t$, the participant Bob_r applies $U(\theta_r)$ to the particle sequence ψ_{r-1} received from Bob_{r-1}, and then sends the transformed sequence to subsequent participant Bob_{r+1}. The total computation cost is $t(t + 1)\,U(\theta)$.

In the protocol I of ref. 22, the initiator performs QFT on the first particle, and sends the second particle (ancillary particle) to next participant. For $r = 2, 3, \ldots, n$, each participant Bob_r performs unitary operation U^j on his particle. Finally, Bob_1 performs QFT^{-1} on his particle, and then measures it to obtain the secret. The total computation cost of the protocol I is $1QFT + (n - 1)\,U^j + 1QFT^{-1} + 2M$. To resist collusion attack, the protocol I is upgraded to the protocol III. For $r = 1, 2, \ldots, n$, each participant splits his share into n pieces, and then calls the protocol I to compute each y_r. Finally, one of the participants calls protocol I to compute the summation of all y_r. The total computation cost of the protocol III is $(n + 1)\ (1QFT + (n - 1)U^j + 1QFT^{-1} + 2M)$.

In ref. 27, the dealer first sends the Y' sequence to Bob_1. For $r = 1, 2, \ldots, t - 1$, Bob_r performs $U_{i,j}(i, j \in \{0, 1\})$ on each particle of the Y' sequence received from Bob_{r-1}. Bob_t performs final operation $U = U_{B_1}U_{B_2}\cdots U_{B_t}$ on each particle of the transformed Y' sequence received from Bob_{t-1}. The total computation cost is $t(2t - 1)U_{i,j} + tM$.

In the proposed QSS, after Bob_1 performs QFT on the first particle $|k\rangle_1$, each participant $Bob_r (r = 1, 2, \ldots, t)$ applies $U_{0,s_r} = \sum_{k=0}^{d-1} \omega^{s_r \cdot k} |k\rangle_{rr}\langle k|$ to his particle $|k\rangle_r$. Finally, Bob_1 performs QFT^{-1} on his own particle, and then measures it to obtain the secret. The total computation cost is $1QFT + tU_{0,s_r} + 1QFT^{-1} + 1M + 2H$.

The computation cost of Hash operations $2H$ has slight impact on the total cost of the proposed QSS. For a single qubit, QFT is a Hadamard gate operation, which is taken as a unitary operation. We assume that the computation costs for each unitary operation in Table 2 are roughly the same. If $2 \le t = n$, the computation cost of the proposed QSS and that of the protocol I of ref. 22 are roughly the same, and both are lower than that of the four other schemes. If $2 < t < n - 1$, the computation cost of the proposed QSS is lowest in the six similar schemes.

Communication Cost. For the six similar schemes, we assume that the number of the decoy particles is l, and the number of the message particles is the same as that of the prepared single-particles or EPR pairs. In ref. 17, the transmission route of the quantum sequence is determined as: $Alice \to Bob_i \to Bob_1 \to \ldots \to Bob_t$. The total number of the transmitted particles is the sum of the message particles and the decoy particles, as shown in Table 3, which is $(t + l)\ (t + 1)$. In ref. 27, the transmission route of the Y' sequence is determined as:

Transmitted particles	Ref. 7	Ref. 17	I of Ref. 22	III of Ref. 22	Ref. 27	The proposed QSS
message particles(or initial particles)	$n-1$	$t(t+1)$			$t(t+1)$	$t-1$
decoy particles (or ancillary particles)		$l(t+1)$	n	nn	$l(t+1)$	

Table 3. Comparison of communication costs.

$Alice \rightarrow Bob_1 \rightarrow \cdots \rightarrow Bob_t$, and that of the X' sequence is determined as: $Alice \rightarrow Bob_t$. The total number of the transmitted particles is also $(t + l)$ $(t + 1)$.

In the protocol I of ref. 22, the ancillary particle is transmitted from one participant to another, and its transmission route is determined as: $Initiator \rightarrow Bob_2 \rightarrow \cdots \rightarrow Bob_n \rightarrow Initiator$. The total number of the transmitted particles is n. In the protocol III of ref. 22, for $r = 1, 2, \ldots, n$, each participant splits his share into n pieces, and every n pieces need one ancillary particle to compute y_r. The total number of the transmitted particles is nn.

In the proposed QSS and ref. 7, the decoy particles are not inserted into the message particles, and the transformed message particles are not transmitted in the quantum channel from one participant to another. The communication cost only is dominated by the distribution of the initial particles from the dealer (or the reconstructor) to every participant. The number of the transmitted particles of the proposed QSS is $t-1$, and that of ref. 7 is $n-1$. If $t=n$, the communication cost of the proposed QSS, that of ref. 7 and that of the protocol I of ref. 22 are roughly the same. If $t<n$, the communication cost of the proposed QSS is the lowest in the six similar schemes.

Discussion

Some existing QSS schemes cannot resist collusion attack of the participants, and the unqualified subsets set of participants can obtain some information about the secret. To resist collusion attack, ref. 22 upgraded the protocol I to the protocol III. With the enhancement of the security, the computation cost of the protocol III flies to $(n+1)$ times. In this paper, we present a (t, n) threshold d-level QSS scheme. Security analysis shows that our scheme can also resist collusion attack. Furthermore, if $2<t<n-1$, our scheme has lower computation and communication cost than other similar schemes including the protocol I of ref. 22. Our scheme is feasible and practical with the present technologies, because it employs quantum $CNOT$, QFT, and Pauli operator U_{0,s_r} as main transformation operations, which have been used widely in quantum field.

References

1. Hillery, M., Buzek, V. & Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **59**, 1829–1834 (1999).
2. Deng, F., Zhou, H. & Long, G. Circular quantum secret sharing. *J. Phys. A. Gen.* **39**, 14089–14099 (2007).
3. Lin, J. & Hwang, T. New circular quantum secret sharing for remote agents. *Quantum Inf. Process.* **12**, 685–697 (2013).
4. Zhu, Z. C., Hu, A. Q. & Fu, A. M. Cryptanalysis of a new circular quantum secret sharing protocol for remote agents. *Quantum Inf. Process.* **12**, 1173–1183 (2013).
5. Hsu, J. L., Chong, S. K., Hwang, T. & Tsai, C. W. Dynamic quantum secret sharing. *Quantum Inf. Process.* **12**, 331–344 (2013).
6. Wang, T. Y. & Li, Y. P. Cryptanalysis of dynamic quantum secret sharing. *Quantum Inf. Process.* **12**, 1991–1997 (2013).
7. Yang, W., Huang, L., Shi, R. & He, L. Secret sharing based on quantum Fourier transform. *Quantum Inf. Process.* **12**, 2465–2474 (2013).
8. Tavakoli, A., Herbauts, I., Żukowski, M. & Bourennane, M. Secret sharing with a single d-level quantum system. *Phys. Rev. A* **92**, 030302 (2015).
9. Karimipour, V. & Asoudeh, M. Quantum Secret Sharing and Random Hopping: Using single states instead of entanglement. *Phys. Rev. A* **92**, 030301 (2015).
10. Markham, D. & Sanders, B. C. Graph states for quantum secret sharing. *Phys. Rev. A* **78**, 42309 (2008).
11. Keet, A., Fortescue, B., Markham, D. & Sanders, B. C. Quantum secret sharing with qudit graph states. *Phys. Rev. A* **82**, 62315 (2010).
12. Sarvepalli, P. Nonthreshold quantum secret-sharing schemes in the graph-state formalism. *Phys. Rev. A* **86**, 042303 (2012).
13. Yang, Y. G., Teng, Y. W., Chai, H. P. & Wen, Q. Y. Verifiable quantum (k, n)-threshold secret key sharing. *Int. J. Theor. Phys.* **50**, 792–798 (2011).
14. Yang, Y. G., Jia, X., Wang, H. Y. & Zhang, H. Verifiable quantum (k, n)-threshold secret sharing. *Quantum Inf. Process.* **11**, 1619–1625 (2012).
15. Song, X. L. & Liu, Y. B. Cryptanalysis and improvement of verifiable quantum (k, n) secret sharing. *Quantum Inf. Process.* **15**, 851–868 (2016).
16. Sarvepalli, P. K. & Klappenecker, A. Sharing classical secrets with Calderbank-Shor-Steane codes. *Phys. Rev. A* **80**, 022321 (2009).
17. Qin, H. W., Zhu, X. H. & Dai, Y. W. (*t*, *n*) Threshold quantum secret sharing using the phase shift operation. *Quantum Inf. Process.* **14**, 2997–3004 (2015).
18. Du, Y. T. & Bao, W. S. Multiparty quantum secret sharing scheme based on the phase shift operations. *Opt. Commun.* **308**, 159–163 (2013).
19. Liu, F., Su, Q. & Wen, Q. Y. Eavesdropping on Multiparty Quantum Secret Sharing Scheme Based on the Phase Shift Operations. *Int. J. Theor. Phys.* **53**, 1730–1737 (2014).
20. Hsu, L. Y. Quantum secret-sharing protocol based on Grover's algorithm. *Phys. Rev. A* **68**, 022306 (2003).
21. Diao, Z. J., Huang, C. F. & Wang, K. Quantum Counting: Algorithm and Error Distribution. *Acta Appl Math.* **118**, 147–159 (2012).
22. Shi, R., Mu, Y., Zhong, H., Cui, J. & Zhang, S. Secure Multiparty Quantum Computation for Summation and Multiplication. *Sci. Rep.* **6**, 19655 (2016).
23. Thas, K. The geometry of generalized Pauli operators of N-qudit Hilbert space, and an application to MUBs. *IEEE International Conference on Systems, Man, and Cybernetic.* **5**, 3816–3822 (2009).
24. Yang, Y. H., Fei, G., Xia, W., Qin, S. J., Zuo, H. J. & Wen, Q. Y. Quantum secret sharing via local operations and classical communication. *Sci. Rep.* **5**, 16967 (2015).
25. Shamir, A. How to share a secret. *Commun. Acm.* **22**(11), 612–613 (1979).
26. Bennett, C. H., Brassard, G. An Update on Quantum Cryptography. Advances in Cryptology, Proceedings of CRYPTO'84, Santa Barbara, California, USA, 475–480 (1984).

27. Li, B. K., Yang, G. Y. & Wen, Q. Y. Threshold Quantum Secret Sharing of Secure Direct Communication. *Chin. Phys. Lett.* **26**, 21–24 (2009).
28. Feldman, P. A practical scheme for non-interactive verifiable secret sharing. Symposium on Foundations of Computer Science, 427–438 (1987).

Acknowledgements

This work is partially supported by National Natural Science Foundation of China (No. 61272400), Foundation Science and Forefront Technology Research Program of Chongqing Science and Technology Commission of China (Nos cstc2014jcyjA40028 and cstc2016jcyjA0571), Special Project of Information Security of National Development and Reform Commission of China (No. [2015]289),and Cultivation Foundation of Top-level Talent of Chongqing University of Posts and Telecommunications (No. RC 2016002).

Author Contributions

Study conception, design, and writing of the manuscript: X.-L.S. and Y.-B.L. Analysis, comparison and discussion: H.-Y.D. and Y.-G.X. All authors reviewed the manuscript.

Additional Information

Competing Interests: The authors declare that they have no competing interests.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.