IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 31, 2019, accepted September 5, 2019, date of publication September 17, 2019,
date of current version September 30, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2941971

Security of Verifiable Threshold Quantum Secret Sharing With Sequential Communication

XIAOQIU CAI[1,2], TIANYIN WANG[2], RUILING ZHANG[3], AND FEI GAO[1,4]

[1]State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2]School of Mathematical Science, Luoyang Normal University, Luoyang 471934, China
[3]School of Information Technology, Luoyang Normal University, Luoyang 471934, China
[4]Center for Quantum Computing, Peng Cheng Laboratory, Shenzhen 518055, China

Corresponding authors: Tianyin Wang (wangtianyin79@163.com) and Fei Gao (gaofei_bupt@hotmail.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61672110, Grant 61671082, Grant 61976024, Grant 61972048, Grant 61572246, and Grant 61602232, in part by the Program for Science and Technology Innovation Research Team in Universities of Henan Province under Grant 18IRTSTHN014, in part by the Plan for Scientific Innovation Talents of Henan Province under Grant 184200510011, in part by the Project for Teaching Reform and Practice Research of High Education in Henan Province under Grant 2019SJGLX094Y, and in part by the Key Project for Inter-Governmental International Scientific and Technological Innovation Cooperation under Grant 2016YFE0104600.

ABSTRACT A verifiable (t, n) threshold quantum secret sharing scheme with sequential communication was proposed recently. In this work, we analyze its security and then give two new participant attacks. Using the first participant attack, the first participant can obtain the dealer's secrets by himself with nonzero probability without being detected. Using the second participant attack, a dishonest participant can gain access to the dealer's secrets by himself in the secret reconstruction phase while he can make the other participants recover false secrets instead of the real ones without being detected. Furthermore, we present an effective way to prevent these attacks.

INDEX TERMS Verifiable secret sharing, verifiability, quantum secret sharing, participant attack.

I. INTRODUCTION

Threshold secret sharing scheme is a basic cryptographic primitive, in which a secret s is divided into n shares such that any t of the n shares can be used to reconstruct the secret s, but any set of $t-1$ or fewer shares contains absolutely no information on the secret s [1]. Clearly, (t, n) threshold secret sharing can be well used to solve the problem that the dealer does not trust one of the agents completely. Nevertheless, in some special cases, the agents do not trust the dealer either. To deal with the possible deception from the dealer, Chor et al firstly introduced the concept of verifiable secret sharing in 1985 [2], which not only satisfies all the requirements of secret sharing but also allows each agent of the secret to verify that the share is consistent with the other shares [3]. Specifically, if the dealer is honest, then the cheaters cannot obtain any information about s, and t or more than t honest agents can reconstruct s if they cooperate with each other. In addition, it can detect whether a dishonest dealer sends fake shares to some or all of the agents, and whether a dishonest agent submits a fake share during the reconstruction phase.

Verifiable secret sharing is a useful tool in much theoretical work. For example, unconditionally-secure verifiable secret sharing schemes are constructed and used to design secure multiparty protocols in [4]–[6]. Recently, unconditionally-secure verifiable secret sharing attracted much attention. A lot of unconditionally-secure verifiable secret sharing schemes [7]–[9] were reported under the assumption that the players can communicate over pairwise secure channels in this model [6].

The security of quantum secret sharing schemes is based on the fundamental principles of quantum physics, and therefore it allows a dealer to distribute shares securely even in the presence of an opponent with infinite computing resources. Due to the security superiority, many proposals for quantum secret sharing have been reported in both theoretical and experimental aspects [10]–[16] since it was firstly introduced by Hillery *et al.* [17].

Combining both verifiability and security superiority of quantum secret sharing, the concept of verifiable quantum secret sharing was then introduced, which gives a new way

The associate editor coordinating the review of this manuscript and approving it for publication was Derek Abbott.

to realize unconditionally-secure verifiable secret sharing. In contrast to classical proposals, verifiable quantum secret sharing can also guarantee the unconditional security of pairwise channels. So far, various verifiable quantum secret sharing schemes have been proposed [18]–[21], which provide a new mechanism for detecting the cheat of the dishonest agent who submits a fake share during the secret reconstruction phase, or checking the consistency of the reconstruction secret.

Recently, a verifiable (t, n) threshold quantum secret sharing scheme with sequential communication was proposed based on a single d-level quantum system [22]. Compared with the existing quantum secret sharing schemes, this scheme stands out with the following advantages. Firstly, it is more general and more practicable than 2-level quantum secret sharing scheme; in addition, the private shares can be used repeatedly. Secondly, it is scalable in the number of participants compared with those schemes based on entangled states. Thirdly, it is more flexible in application than (n, n) quantum secret sharing scheme. Fourthly, other classical (t, n) threshold secret sharing schemes can be used to replace Shamir's scheme while keeping all the aforementioned advantages. Most importantly, this scheme is considered to be independent of any trusted third party and able to detect any cheat and eavesdropping during secret reconstruction.

In this paper, we analyze the security of the verifiable (t, n) threshold quantum secret sharing scheme [22] and then give two new participant attacks. Using the first attack, the first participant Bob_1 can obtain the dealer's secrets by himself with nonzero probability without being detected. Using the second attack, a dishonest participant can gain access to the dealer's secrets by himself in the secret reconstruction phase. At the same time, he can make the other participants recover false secrets instead of the real ones without being detected. Therefore, this scheme does not satisfy the security and verifiability in some sense. Moreover, we discuss how people deal with such security problems and then give an effective way to prevent these attacks.

The rest of this paper is organized as follows. In Section II, a brief description of the verifiable (t, n) threshold quantum secret sharing scheme with sequential communication is reviewed. In Section III, we analyze the security of the verifiable (t, n) threshold quantum secret sharing scheme with sequential communication, and then present two new participant attacks. In Section IV, we study how people deal with the security problems and then give an improved version to prevent these attacks. Finally, conclusions are given in Section V.

II. VERIFIABLE THRESHOLD QUANTUM SECRET SHARING SCHEME WITH SEQUENTIAL COMMUNICATION

In this section, let us give a brief description of the verifiable (t, n) threshold quantum secret sharing scheme with sequential communication [22], which includes both the classical private share distribution phase and the secret sharing phase. Moreover, a dealer Alice and n agents $\mathrm{Bob}_1, \mathrm{Bob}_2, \ldots, \mathrm{Bob}_n$ are also involved.

A. CLASSICAL PRIVATE SHARE DISTRIBUTION PHASE

This phase includes the following three steps.

1) Alice chooses a random polynomial

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

over a finite field $\mathrm{GF}(d)$, where the notation GF is the abbreviation of Galois Field, d is an odd prime number, and $s = a_0 = f(0)$ is the private value and $a_0, a_1, \ldots, a_{t-1} \in \mathrm{GF}(d)$.

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

3) Alice sends each share $f(x_j)$ to the corresponding agent Bob_j via a private channel for $j = 1, 2, \ldots, n$.

By the way of Shamir's secret sharing, the dealer distributes n classical private shares to n agents $\mathrm{Bob}_1, \mathrm{Bob}_2, \ldots, \mathrm{Bob}_n$, respectively.

B. SECRET SHARING PHASE

Alice prepares three identical states $|\Phi_v\rangle = |\phi_0^0\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j\rangle$, $v = 1, 2, 3$, and then distributes the secrets $S_1, S_2 \in \mathrm{GF}(d)$ and a check value $N \in \mathrm{GF}(d)$ to m $(m \geq t)$ participants $\mathrm{Bob}_1, \mathrm{Bob}_2, \ldots, \mathrm{Bob}_m$ as follows.

(i) Alice performs the operation $U_{p_0^v q_0^v} = X_d^{p_0^v} Y_d^{q_0^v}$ on $|\Phi_v\rangle$, which transforms the state $|\Phi_v\rangle$ into $|\Phi_v\rangle_0 = |\phi_{p_0^v}^{q_0^v}\rangle$, where $X_d = \sum_{r=0}^{d-1}\omega^r|r\rangle\langle r|$, $Y_d = \sum_{r=0}^{d-1}\omega^{r^2}|r\rangle\langle r|$, $\omega = e^{\frac{2\pi i}{d}}$ is the dth root of unity, $p_0^1 = S_1, p_0^2 = S_2, p_0^3 = N, q_0^1 = q_0^2 = q_0^3 = d - s$ with $p_0^v, q_0^v \in \mathrm{GF}(d)$, $S_1 = S_2 N \bmod d$.

(ii) Suppose that Alice wants the m participants Bob_1, Bob_2, $\ldots$, Bob_m to share the secrets S_1, S_2, she sends $\otimes_{v=1}^3|\Phi_v\rangle_0$ to Bob_1, hereafter the notation $\otimes$ denotes the direct product of quantum states. Upon receiving them, Bob_1 performs the operation $U_{p_1^v q_1^v} = X_d^{p_1^v} Y_d^{q_1^v}$ on $|\Phi_v\rangle_0$ for $v = 1, 2, 3$, where p_1^1, p_1^2, and p_1^3 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 $p_1^v, q_1^v \in \mathrm{GF}(d)$. After that, the states $\otimes_{v=1}^3|\Phi_v\rangle_0$ are transformed into $\otimes_{v=1}^3|\Phi_v\rangle_1 = \otimes_{v=1}^3|\phi_{p_0^v + p_1^v}^{q_0^v + q_1^v}\rangle$ and are then sent to Bob_2 by Bob_1.

(iii) Bob_j $(j = 2, 3, \ldots, m)$ repeats the same procedure sequentially as that Bob_1 does in Step (ii), i.e., Bob_j performs the operation $U_{p_j^v q_j^v} = X_d^{p_j^v} Y_d^{q_j^v}$ on $|\Phi_v\rangle_{j-1}$ for $v = 1, 2, 3$ and thus gets the states $\otimes_{v=1}^3|\Phi_v\rangle_j = \otimes_{v=1}^3|\phi_{\sum_{r=0}^j p_r^v}^{\sum_{r=0}^j q_r^v}\rangle$, where $p_j^v, q_j^v \in \mathrm{GF}(d)$, $q_j^v = c_j = f(x_j)\prod_{r=1, r\neq j}^m \frac{x_r}{x_r - x_j} \bmod d$. Then Bob_j sends the states $\otimes_{v=1}^3|\Phi_v\rangle_j$ to the next participant Bob_{j+1}.

(iv) The last participant Bob_m measures the states $\otimes_{v=1}^3\Phi_v\rangle_m$ with the basis $\{|\phi_l^0\rangle\}_l$. Then he publishes the measurement results R_1, R_2, R_3.

(v) After all m participants exchange their random numbers, they compute $p_0^1 = (R_1 - \sum_{j=1}^{m} p_j^1) \mathrm{mod} d$, $p_0^2 = (R_2 - \sum_{j=1}^{m} p_j^2) \mathrm{mod} d$, $p_0^3 = (R_3 - \sum_{j=1}^{m} p_j^3) \mathrm{mod} d$, respectively. Then they check whether the following equation

$$p_0^1 = p_0^2 p_0^3 \mathrm{mod} d \tag{2}$$

holds. If it holds, they share the secrets $S_1 = p_0^1$, $S_2 = p_0^2$; otherwise, they think that the secret sharing is invalid and then abort this round.

III. CRYPTANALYSIS OF VERIFIABLE THRESHOLD QUANTUM SECRET SHARING SCHEME WITH SEQUENTIAL COMMUNICATION

To better understand the verifiable threshold quantum secret sharing scheme and its cryptanalysis, a simple introduction on the cyclic property of mutually unbiased bases (MUBs) is firstly given [15]. It has been shown that if d is an odd prime, then there are d MUBs $\{|\phi_l^0\rangle\}_l, \{|\phi_l^1\rangle\}_l, \ldots, \{|\phi_l^{d-1}\rangle\}_l$ except the computational basis $\{|j\rangle | j = 0, 1, \ldots, d-1\}$ [22], where

$$|\phi_l^k\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{j(l+kj)} |j\rangle, \tag{3}$$

here $k \in \{0, 1, \ldots, d-1\}$ labels the basis, $l \in \{0, 1, \ldots, d-1\}$ enumberates the states of the given basis. Furthermore, the unitary operations $X_d = \sum_{r=0}^{d-1} \omega^r |r\rangle\langle r|$ and $Y_d = \sum_{r=0}^{d-1} \omega^{r^2} |r\rangle\langle r|$ can transform the state $|\phi_l^k\rangle$ into $|\phi_{l+1}^k\rangle$ and $|\phi_l^{k+1}\rangle$, respectively, which means there always exists an operation $U_{l'k'} = X_d^{l'} Y_d^{k'}$ for any $l', k' \in \{0, 1, \ldots, d-1\}$ such that

$$U_{l'k'} |\phi_l^k\rangle = |\phi_{l+l'}^{k+k'}\rangle. \tag{4}$$

From Section 2, we can see that the verifiable (t, n) threshold quantum secret sharing scheme is constructed based on this cyclic property of MUBs. Firstly, the dealer Alice allocates a share generated from a private value s to each agent Bob_j $(j = 1, 2, \ldots, n)$ by classical (t, n) threshold secret sharing [1]. Then she prepares three identical qudits and embeds the two secrets S_1, S_2 and the verification value N into each qudit, respectively. These qudits are transmitted among m participants in sequence. Upon receiving the qudits, each participant performs unitary operations related to his share on the qudits. On the one hand, a random number is added to each secret and the verification value by an operation; on the other hand, the private value in each qudit is eliminated due to classical (t, n) threshold secret sharing when at least t participants complete their operations. Subsequently, the last participant Bob_m can measure $\otimes_{v=1}^{3} |\Phi_v\rangle_m$ with the right basis $\{|\phi_l^0\rangle\}_l$. In an ideal case, if these qudits are not disturbed, the measurement results R_1, R_2, R_3, and the random numbers $p_j^1, p_j^2, p_j^3, j = 0, 1, \ldots, m$ must satisfy

$$R_1 = \sum_{j=0}^{m} p_j^1 \mathrm{mod} d, \tag{5}$$

$$R_2 = \sum_{j=0}^{m} p_j^2 \mathrm{mod} d, \tag{6}$$

$$R_3 = \sum_{j=0}^{m} p_j^3 \mathrm{mod} d. \tag{7}$$

Consequently, when Bob_m publishes the measurement outcomes to all participants, they can recover the secrets S_1, S_2 and the verification value N after disclosing their respective random numbers.

As mentioned in [22], the last participant Bob_m is crucial to this scheme because he is responsible for keeping and measuring the qudits in true basis. Therefore, he is able to deceive the other participants by announcing wrong measurement results. In addition, other participant can also cheat by using a wrong share in secret reconstruction. Additionally, the qudits are obviously vulnerable to an external eavesdropper in transmission. Accordingly, a verification mechanism is necessary to this scheme. By using Eq.(2) to detect cheat or eavesdropping, it is claimed that this scheme is able to detect any cheat and eavesdropping during secret reconstruction because it is thought that this scheme can find the cheat by participants with the probability

$$p_d = \frac{d-1}{d}, \tag{8}$$

which converges to 100% if d approaches to infinity.

As we know, cryptanalysis is an important and interesting work in cryptography, which estimates the security of cryptographic schemes, finds potential loopholes and tries to solve the security problems [23]–[28]. As pointed out by Lo and Ko, breaking cryptographic systems was as important as building them [29]. In the study of quantum cryptography, quite a few effective attack strategies have been proposed, such as teleportation attack [30], dense-coding attack [31], correlation-extractability attack [32], denial-of-service attack [33]–[35], and so on. Understanding those attacks will be helpful for us to design new schemes with high security.

Participant attack, firstly proposed by Gao *et al.* [36], is a special internal attack. In contrast to other opponents outside, the dishonest participants have many advantages. Firstly, they know partial information legally. Secondly, they can tell a lie in the process of eavesdropping check to try to avoid introducing errors. Thus, it is a powerful attack and should be paid more attention to. Now it has become an important study point [37]–[44].

Here we give two new participant attack strategies on the verifiable (t, n) threshold quantum secret sharing scheme with sequential communication, which are to be described in detail as follows.

A. PARTICIPANT ATTACK 1

The participant attack 1 includes the following steps.

(1) In the classical private share distribution phase, the first participant Bob_1 performs his actions faithfully.

(2) In the secret sharing phase, when Bob_1 receives the three qudits $\otimes_{v=1}^{3}|\Phi_v\rangle_0 = \otimes_{v=1}^{3}|\phi_{p_0^v}^{q_0^v}\rangle$ from Alice in Step (ii), he immediately measures each of them with a random basis $\{|\phi_l^k\rangle\}_l$, and the measurement outcomes are denoted as $p_{0'}^1, p_{0'}^2, p_{0'}^3$, respectively. Here it should be noted that the three qudits are measured with the same basis $\{|\phi_l^k\rangle\}_l$ chosen randomly. At the same time, Bob_1 prepares three new identical quantum states $|\Phi_{v'}\rangle = |\phi_0^0\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j\rangle$, $v' = 1, 2, 3$.

(3) Bob_1 chooses two fake secrets $S_1', S_2' \in \text{GF}(d)$ and a fake check value $N' \in \text{GF}(d)$ with $S_1' \neq p_{0'}^1, S_2' \neq p_{0'}^2$ and $S_1' = S_2' N' \text{mod} d$. Then he verifies whether the three measurement outcomes $p_{0'}^1, p_{0'}^2, p_{0'}^3$ satisfy the following equation

$$p_{0'}^1 = p_{0'}^2 p_{0'}^3 \text{mod} d \tag{9}$$

or not. If it is true, then he performs the operation $U_{p_0^{v'} q_0^{v'}} = X_d^{p_0^{v'}} Y_d^{q_0^{v'}}$ on $|\Phi_{v'}\rangle$ for $v' = 1, 2, 3$, where $p_0^1 = S_1'$, $p_0^2 = S_2'$, $p_0^3 = N'$, $q_0^1 = q_0^2 = q_0^3 = k \in \text{GF}(d)$. Otherwise, Bob_1 performs the operation $U_{p_0^{v'} q_0^{v'}} = X_d^{p_0^{v'}} Y_d^{q_0^{v'}}$ on $|\Phi_{v'}\rangle$ for $v' = 1, 2, 3$, where $p_0^1 = S_1'$, $p_0^2 = S_2'$, $p_0^3 = N'$, but $q_0^1 = q_0^2 = q_0^3 = k' \in \text{GF}(d)$ with $k' \neq k$. After that, the states $\otimes_{v'=1}^{3}|\Phi_{v'}\rangle$ are transformed into $\otimes_{v'=1}^{3}|\Phi_{v'}\rangle_0 = \otimes_{v'=1}^{3}|\phi_{p_0^{v'}}^{q_0^{v'}}\rangle$.

(4) Bob_1 performs the remaining actions faithfully as those in the original scheme.

(5) In Step (v), if the other $m-1$ participants Bob_2, Bob_3, ..., Bob_m think that the secret sharing attempt is corrupt meanwhile Eq.(9) does not hold, then Bob_1 can discriminate that both the basis $\{|\phi_l^k\rangle\}_l$ and the basis $\{|\phi_l^{k'}\rangle\}_l$ must be wrong; if the other $m-1$ participants Bob_2, Bob_3, ..., Bob_m think that the secret sharing attempt is corrupt meanwhile Eq.(9) holds, then Bob_1 can discriminate that the basis $\{|\phi_l^k\rangle\}_l$ must be wrong; if the other $m-1$ participants Bob_2, Bob_3, ..., Bob_m think that the secret sharing attempt is not corrupt meanwhile Eq.(9) does not hold, then Bob_1 can discriminate that the basis $\{|\phi_l^k\rangle\}_l$ must be wrong but the basis $\{|\phi_l^{k'}\rangle\}_l$ may be right; Otherwise, Bob_1 can discriminate that the basis $\{|\phi_l^k\rangle\}_l$ may be right.

(6) In the next round, i.e., the dealer distributes two new secrets to the m participants Bob_1, Bob_2, ..., Bob_m, Bob_1 performs the above attack process (1)-(5) again. The difference is that if he has known that the basis $\{|\phi_l^k\rangle\}_l$ or the basis $\{|\phi_l^{k'}\rangle\}_l$ may be right, then he uses it to measure the qudits that are encoded with new secrets and check value by the dealer instead of using a random basis, and if the other $m-1$ participants Bob_2, Bob_3, ..., Bob_m think that the secret sharing attempt is also not corrupt in this round, then he can further confirm that the basis $\{|\phi_l^k\rangle\}_l$ or the basis $\{|\phi_l^{k'}\rangle\}_l$ may be right; else if the other $m-1$ participants Bob_2, Bob_3, ..., Bob_m think that the secret sharing attempt is corrupt in this round, then he can confirm that the basis $\{|\phi_l^k\rangle\}_l$ or the basis $\{|\phi_l^{k'}\rangle\}_l$ must be wrong. Otherwise, if Bob_1 has known that the basis $\{|\phi_l^k\rangle\}_l$ or the basis $\{|\phi_l^{k'}\rangle\}_l$ or both must be wrong in the previous round, then he performs the same attack process except that the measurement basis randomly chosen by him is not $\{|\phi_l^k\rangle\}_l$ or $\{|\phi_l^{k'}\rangle\}_l$ or both.

(7) The attack process (1)-(6) are repeatedly performed until the dealer announces that the private value s is not reused any longer.

From the participant attack 1, we can find that Bob_1 can obtain some useful information whether the measurement basis chosen by him in Step (2) is right or not in every round, which will improve the probability that he chooses the right basis in the next round. Specifically, if the basis $\{|\phi_l^k\rangle\}_l$ is the right basis $\{|\phi_l^{d-s}\rangle\}_l$, he will choose the right basis with the probability 100% in the remaining rounds because the private value s is reused and thus the right bases in all rounds are the same; if it is not right, he will choose the right basis with a relative larger probability in the next round because one or two bases may be excluded from the candidate bases. For example, Bob_1 will choose the right measurement basis $\{|\phi_l^{d-s}\rangle\}_l$ for the three qudits $\otimes_{v=1}^{3}|\Phi_v\rangle_0$ with the probability $\frac{1}{d}$ in the first round, but the probability that he will choose the right measurement basis $\{|\phi_l^{d-s}\rangle\}_l$ will be more than $\frac{1}{d}$ in the second round in general because he has known that the basis $\{|\phi_l^k\rangle\}_l$ or the basis $\{|\phi_l^{k'}\rangle\}_l$ or both are not right. Therefore, if this attack has been performed n' rounds by Bob_1 for $n' = 1, 2, \ldots, n$, where n is the total number of attack rounds, then the probability P_s that he will choose the right measurement basis $\{|\phi_l^{d-s}\rangle\}_l$ is

$$P_s = 1 - P_{e_1} \times P_{e_2} \times \ldots \times P_{e_{n'}} \geq 1 - (1 - \frac{1}{d})^{n'} \approx \frac{n'}{d} \tag{10}$$

due to $1 - \frac{1}{d} = P_{e_1} \geq P_{e_2} \geq \cdots \geq P_{e_{n'}}$, where P_{e_i} is the probability that Bob_1 will choose the false measurement basis in the ith round for $i = 1, 2, \ldots, n'$. Furthermore, it is evident that when Bob_1 chooses the right measurement basis $\{|\phi_l^k\rangle\}_l = \{|\phi_l^{d-s}\rangle\}_l$ in some round (e.g., the n'th round), he can easily gain access to the private value s by computing

$$s = (d - k) \text{mod} d, \tag{11}$$

in this case he can obtain the secrets distributed by the dealer in all the remaining rounds without being detected. Additionally, it should be noted that Bob_1 can discriminate the basis $\{|\phi_l^k\rangle\}_l$ or the basis $\{|\phi_l^{k'}\rangle\}_l$ or both are not right with the probability 100%, but he cannot distinguish the basis $\{|\phi_l^k\rangle\}_l$ or the basis $\{|\phi_l^{k'}\rangle\}_l$ is right with the probability 100% even if the other $m-1$ participants Bob_2, Bob_3, ..., Bob_m think that the secret sharing attempt is not corrupt meanwhile Eq.(9) holds in each of the remaining rounds. However, the error probability P_e is negligible. Without loss of generality, suppose that Bob_1 thinks the basis $\{|\phi_l^k\rangle\}_l$ chosen in the n'th round is right, which requires that the other $m-1$ participants Bob_2, Bob_3, ..., Bob_m think that the secret sharing attempt is not corrupt meanwhile Eq.(9) holds in this round and the remaining $n-n'$ rounds. If the basis $\{|\phi_l^k\rangle\}_l$ is surely right, these requirements must be satisfied; if it is not, these requirements may be also satisfied with the probability

$$P_e = \frac{1}{d} \times \frac{1}{d^2} \times \ldots \times \frac{1}{d^2} = \frac{1}{d^{2(n-n')+1}}, \tag{12}$$

which is exponentially close to 0 with the increase of n.

In a word, using the participant attack 1, the first participant Bob_1 can gain access to the private value s with the probability no less than $\frac{n'}{d}$ at the end of the n'th round for $n' = 1, 2, \ldots, n$. Furthermore, if Bob_1 has known the private value s at the end of this round, then he can obtain the secrets distributed by the dealer in all the remaining rounds without being detected. More importantly, Bob_1 has no loss even if his cheating is detected by the other $m-1$ participants Bob_2, Bob_3, $\ldots$, Bob_m because nobody can distinguish he is the attacker.

It should be noted that a participant Bob_k $(k = 2, 3, \ldots, m)$ can also perform a similar attack to gain access to the previous participant Bob_{k-1}'s share $f(x_{k-1})$ and three random numbers $p^1_{k-1}, p^2_{k-1}, p^3_{k-1}$. Specifically, when Bob_{k-2} sends the states $\otimes^3_{v=1}|\Phi_v\rangle_{k-2}$ to Bob_{k-1} in Step (ii) or Step (iii), Bob_k intercepts them. At the same time, he prepares three fake states and sends them to Bob_{k-1}. After receiving the fake states from Bob_{k-1}, Bob_k immediately measures them with a random basis $\{|\phi^k_l\rangle\}_l$. According to the measurement outcomes, Bob_k performs the corresponding operations on the real states $\otimes^3_{v=1}|\Phi_v\rangle_{k-2}$ by personating Bob_{k-1}. Then he performs his own actions faithfully. Compared with Bob_1, Bob_k cannot immediately verify the correctness of his measurement outcomes $p^1_{k-1}, p^2_{k-1}, p^3_{k-1}$, but can only judge them by whether the other $m-1$ participants think that the secret sharing attempt is corrupt or not in Step (v). Therefore, the probability that Bob_k chooses the right basis is not more than P_s by simply arguments if it is also performed n' rounds.

B. PARTICIPANT ATTACK 2

Next we show that a dishonest participant can gain access to the dealer's secrets in the secret reconstruction phase while he can make the other participants recover false secrets instead of the real ones without being detected. Without loss of generality, suppose that Bob_k $(k = 1, 2, \ldots, m)$ is the dishonest participant, he can obtain the dealer's secrets by the following attack.

(1) Bob_k performs his actions faithfully both in the classical private share distribution phase and the secret sharing phase.

(2) In the secret reconstruction phase, when Bob_k receives all the other $m-1$ participants' random numbers $p^v_1, p^v_2, \ldots, p^v_{k-1}, p^v_{k+1}, \ldots, p^v_m$ for $v = 1, 2, 3$, he immediately chooses two fake random numbers $p^{1'}_k, p^{2'}_k$ with $p^{1'}_k \neq p^1_k, p^{2'}_k \neq p^2_k$, and then derives the third number $p^{3'}_k$ by solving the following equation

$$(R_1 - \sum_{j=1,j\neq k}^{m} p^1_j - p^{1'}_k)(R_2 - \sum_{j=1,j\neq k}^{m} p^2_j - p^{2'}_k) = (R_3 - \sum_{j=1,j\neq k}^{m} p^3_j - p^{3'}_k) \bmod d. \quad (13)$$

After that, he sends them to the other $m-1$ participants Bob_1, Bob_2, $\ldots$, Bob_{k-1}, Bob_{k+1}, $\ldots$, Bob_m instead of the real three random numbers p^1_k, p^2_k, p^3_k.

(3) As does in Step (v), Bob_k recovers the dealer's secrets S_1 and S_2 by computing $S_1 = (R_1 - \sum_j^m p^1_j) \bmod d$ and $S_2 = (R_2 - \sum_j^m p^2_j) \bmod d$.

By simple deducing, it can be seen that if the two random numbers $p^{1'}_k$ and $p^{2'}_k$ are given, then the third $p^{3'}_k$ can always be found by solving Eq. (13). Obviously, the other $m-1$ participants Bob_1, Bob_2, $\ldots$, Bob_{k-1}, Bob_{k+1}, $\ldots$, Bob_m will get the fake secrets

$$p^{1'}_0 = S''_1 = (R_1 - \sum_{j=1,j\neq k}^{m} p^1_j - p^{1'}_k) \bmod d, \quad (14)$$

$$p^{2'}_0 = S''_2 = (R_2 - \sum_{j=1,j\neq k}^{m} p^2_j - p^{2'}_k) \bmod d, \quad (15)$$

and the fake check value

$$p^{3'}_0 = N'' = (R_3 - \sum_{j=1,j\neq k}^{m} p^3_j - p^{3'}_k) \bmod d. \quad (16)$$

Furthermore, it is easily deduced from Eqs. (13)-(16) that the three numbers $p^{1'}_0, p^{2'}_0, p^{3'}_0$ also satisfy

$$p^{1'}_0 p^{2'}_0 = p^{3'}_0 \bmod d, \quad (17)$$

which means that the dishonest participant Bob_k's deception cannot be detected by the other $m-1$ participants Bob_1, Bob_2, $\ldots$, Bob_{k-1}, Bob_{k+1}, $\ldots$, Bob_m.

As a result, the dishonest participant Bob_k $(k = 1, 2, \ldots, m)$ can gain access to the dealer's real secrets S_1 and S_2 by himself in the secret reconstruction phase. Furthermore, he can make the other $m-1$ participants Bob_1, Bob_2, $\ldots$, Bob_{k-1}, Bob_{k+1}, $\ldots$, Bob_m reconstruct the false secrets S''_1 and S''_2 instead of the real ones without being detected.

IV. THE WAY TO PREVENT PARTICIPANT ATTACKS

The scenarios for solving the security problems will be introduced in the following content. From the participant attack 1, it can be seen that there are three key factors to the success of this attack. The first factor is that the dealer's secrets S_1 and S_2 are directly encoded to the quantum states $\otimes^2_{v=1}|\Phi_v\rangle$ in every round, and these states are transformed into the same basis $\{|\phi^{d-s}_l\rangle\}_l$ after the encoding operations for the secrets and the check value, which gives an opportunity for the first participant Bob_1 to gain access to them by measuring the encoded quantum states $\otimes^2_{v=1}|\Phi_v\rangle_0$ with a random basis $\{|\phi^k_l\rangle\}_l$. The second factor is that the verification mechanism also gives a good chance for the first participant Bob_1 to verify the correctness of the measurement basis $\{|\phi^k_l\rangle\}_l$ meanwhile it provides the verifiability of allocated secrets S_1 and S_2. The third factor is that the reused private value s provides more chances for Bob_1 to gain access to it and further verify its correctness. Accordingly, to prevent the participant attack 1, one possible way is to find a new encoding method, which must guarantee any participant cannot gain access to the two

secrets S_1 and S_2 by directly measuring the encoded quantum states except with a negligible probability. Another way is to remove the verification mechanism, which makes Bob_1 cannot distinguish the correctness of the secrets S_1 and S_2 any longer, but it also makes the original scheme lose the good property of allocated secrets' verifiability. Therefore, the feasible way to prevent the participant attack 1 is finding a new encoding method for the two secrets S_1 and S_2 while the reused times of the private value s is limited.

From the participant attack 2, it can be seen that the reason for the success of this attack is that the dishonest participant Bob_k can be the last one to submit his three random numbers, which gives him a chance to choose the fake random numbers $p_k^{1'}$, $p_k^{2'}$, and $p_k^{3'}$. Consequently, if the random numbers chosen by each participant are exchanged simultaneously among them, then any participant has no chance to perform this attack any longer.

In order to prevent the two participant attacks, here we give some improvements on the original scheme according to the above analysis, which are described as follows.

(A) In the classical private share distribution phase, Alice chooses three random polynomials

$$f_1(x) = (a_0^1 + a_1^1 x + \cdots + a_{t-1}^1 x^{t-1}) \text{mod} d, \quad (18)$$

$$f_2(x) = (a_0^2 + a_1^2 x + \cdots + a_{t-1}^2 x^{t-1}) \text{mod} d, \quad (19)$$

$$f_3(x) = (a_0^3 + a_1^3 x + \cdots + a_{t-1}^3 x^{t-1}) \text{mod} d, \quad (20)$$

where $s_v = a_0^v = f_v(0)$ is the private value and $a_0^v, a_1^v, \ldots, a_{t-1}^v \in \text{GF}(d)$ for $v = 1, 2, 3$, and s_1, s_2, s_3 are different. Then she computes $f_1(x_j), f_2(x_j), f_3(x_j)$ as the share of agent Bob_j for $j = 1, 2, \ldots, n$ with $x_j \neq x_r$ for $j \neq r$. Finally, she sends each share $f_1(x_j), f_2(x_j), f_3(x_j)$ to the corresponding agent Bob_j via a private channel for $j = 1, 2, \ldots, n$.

(B) In the secret sharing phase, Alice and each participant Bob_j ($j = 1, 2, \ldots, m$) performs the same actions as those in Steps (i)-(iv) except choosing $q_0^v = d - s_v$ and $q_j^v = c_j^v = f_v(x_j) \prod_{r=1, r\neq j}^{m} \frac{x_r}{x_r - x_j} \text{mod} d$ for $v = 1, 2, 3$.

(C) In Step (v), all the participants $\text{Bob}_1, \text{Bob}_2, \ldots, \text{Bob}_m$ exchange their three random numbers in a way of bit by bit, and then reconstruct the secrets by the same way.

(D) The private value s_v can be used no more than T rounds for $v = 1, 2, 3$, here T is a positive integer and satisfies $T \ll d$.

From the improvements, it can be seen that in Step (B), although Alice performs the similar encoding operations $U_{p_0^1 q_0^1}, U_{p_0^2 q_0^2}, U_{p_0^3 q_0^3}$ on the three quantum states $|\Phi_1\rangle, |\Phi_2\rangle, |\Phi_3\rangle$, respectively, the three states $\otimes_{v=1}^3 |\Phi_v\rangle$ are transformed into $\otimes_{v=1}^3 |\Phi_v\rangle_0 = \otimes_{v=1}^3 |\phi_{p_0^v}^{q_0^v}\rangle$, which are in three different bases $\{|\phi_l^{q_0^1}\rangle\}_l, \{|\phi_l^{q_0^2}\rangle\}_l, \{|\phi_l^{q_0^3}\rangle\}_l$ because $q_0^1 = d - s_1 \neq q_0^2 = d - s_2 \neq q_0^3 = d - s_3 \neq q_0^1 = d - s_1$. In this case, the probability that the first participant Bob_1 chooses the right basis for each of the three states $\otimes_{v=1}^3 |\Phi_v\rangle_0 = \otimes_{v=1}^3 |\phi_{p_0^v}^{q_0^v}\rangle$ is about $\frac{1}{d} \times \frac{1}{d} \times \frac{1}{d} = \frac{1}{d^3}$ in each round by the participant attack 1. At the same time, the private value s_v is reused no more than T rounds for $v = 1, 2, 3$. Consequently, the final probability P_s that Bob_1 will choose the right measurement bases $\{|\phi_l^{q_0^1}\rangle\}_l, \{|\phi_l^{q_0^2}\rangle\}_l, \{|\phi_l^{q_0^3}\rangle\}_l$ is about $\frac{T}{d^3}$, which means that the participant attack 1 can be effectively prevented in the sense the probability P_s is negligible. By simple analysis, the similar attack to steal a participant's share can be also prevented by the improvements. Furthermore, in Step (C), it is required that all the participants $\text{Bob}_1, \text{Bob}_2, \ldots, \text{Bob}_m$ exchange their three random numbers in a way of bit by bit, which makes the dishonest participant has no chance to find the fake ones that can escape the other $m - 1$ participants' check any longer. Therefore, the participant attack 2 also can be effectively prevented.

So far, we have shown the participant attack 1 can be effectively prevented by greatly reducing the probability that the dishonest participant Bob_1 can gain access to the dealer's secrets, and the participant attack 2 can be prevented only by changing the way of random numbers' exchange. Moreover, these improvements do not change the model of the original scheme, and therefore its security analysis against intercept-resend attack and joint attack can be directly applied to the improved version.

V. CONCLUSION

To sum up, we analyze the security of a verifiable (t, n) threshold quantum secret sharing scheme with sequential communication, and then propose two new participant attacks. Using the first participant attack, the first participant Bob_1 can obtain the dealer's secrets S_1 and S_2 by himself with the probability $p_s = \frac{1}{d}$ without being detected in the first round, and in this case he also can gain access to the private value s, which will give him a good chance to recover the secrets distributed by the dealer in the next round. Furthermore, the probability that Bob_1 can gain access to the private value s linearly increases with the increasing of rounds. More worse, Bob_1 has no loss even if his cheat is detected by the other $m - 1$ participants $\text{Bob}_2, \text{Bob}_3, \ldots, \text{Bob}_m$ because nobody can discriminate that he is the attacker. Using the second participant attack, a dishonest participant Bob_k can gain access to the dealer's secrets S_1 and S_2 by himself with certain probability in the secret reconstruction phase, but he can make the other participants recover false secrets instead of the real ones without being detected. Finally, we discuss how people deal with the security problems and then give an improved version to prevent these attacks.

REFERENCES

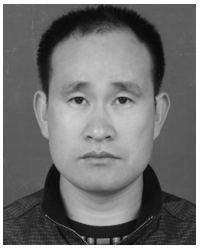
[1] A. Shamir, "How to shair a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[2] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch, "Verifiable secret sharing and achieving simultaneity in the presence of faults," in *Proc. 26th IEEE Symp. Found. Comput. Sci.*, Portland, OR, USA, Oct. 1985, pp. 383–395.

[3] M. Carpentieri, "A perfect threshold secret sharing scheme to identify cheaters," *Des., Codes Cryptogr.*, vol. 5, no. 3, pp. 183–187, May1995.

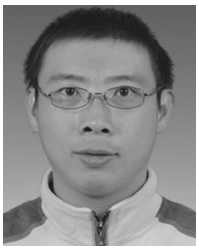
[4] M. Ben-Or, S. Goldwasser, and A. Widgerson, "Completeness theorems for non-cryptographic fault-tolerant distributed computation," in *Proc. 12th Annu. ACM Symp. Theory Comput.*, 1988, pp. 1–10.
[5] D. Chaum, C. Crépeau, and I. Damgård, "Multiparty unconditionally secure protocols," in *Proc. 12th Annu. ACM Symp. Theory Comput.*, 1988, pp. 11–19.
[6] R. Cramer, I. Damgård, and U. Maurer, "General secure multi-party computation from any linear secret-sharing scheme," in *Advances in Cryptology—EUROCRYPT 2000*. Berlin, Germany: Springer, 2000.
[7] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Advances Cryptology*. Berlin, Germany: Springer, 1991.
[8] M. Nojoummian, "Unconditionally secure proactive verifiable secret sharing using new detection and recovery techniques," in *Proc. 14th Annu. Int. Conf. Privacy, Secur. Trust*, Auckland, New Zealand, Dec. 2016, pp. 269–274.
[9] M. Yoshida and S. Obana, "Verifiably multiplicative secret sharing," *IEEE Trans. Inf. Theory*, vol. 65, no. 5, pp. 3233–3245, May 2019.
[10] W. Tittel, H. Zbinden, and N. Gisin, "Experimental demonstration of quantum secret sharing," *Phys. Rev. A, Gen. Phys.*, vol. 63, no. 4, Apr. 2001, Art. no. 042301.
[11] L. Xiao, G. L. Long, F.-G. Deng, and J.-W. Pan, "Efficient multiparty quantum-secret-sharing schemes," *Phys. Rev. A, Gen. Phys.*, vol. 69, no. 5, May 2004, Art. no. 052307.
[12] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, "Experimental single qubit quantum secret sharing," *Phys. Rev. Lett.*, vol. 95, no. 23, Dec. 2005, Art. no. 230505.
[13] T. Y. Wang, Q. Y. Wen, X. B. Chen, F. Z. Guo, and F. C. Zhu, "An efficient and secure multiparty quantum secret sharing scheme based on single photons," *Opt. Commun.*, vol. 281, no. 24, pp. 6130–6134, Dec. 2008.
[14] J. J. Shi, R. H. Shi, Y. Tang, and M. H. Lee, "A multiparty quantum proxy group signature scheme for the entangled-state message with quantum Fourier transform," *Quantum Inf. Process.*, vol. 10, no. 5, pp. 653–670, Oct. 2011.
[15] A. Tavakoli, I. Herbauts, M. Żukowski, and M. Bourennane, "Secret sharing with a single d-level quantum system," *Phys. Rev. A, Gen. Phys.*, vol. 92, no. 3, Mar. 2015, Art. no. 030302.
[16] Y. Zhou, J. Yu, Z. Yan, X. Jia, J. Zhang, C. Xie, and K. Peng, "Quantum secret sharing among four players using multipartite bound entanglement of an optical field," *Phys. Rev. Lett.*, vol. 121, no. 15, Dec. 2018, Art. no. 150502.
[17] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A, Gen. Phys.*, vol. 59, pp. 1829–1834, Mar. 1999.
[18] Q. Li, D. Y. Long, W. H. Chan, and D. W. Qiu, "Sharing a quantum secret without a trusted party," *Quantum Inf. Process.*, vol. 10, no. 1, pp. 97–106, Feb. 2011.
[19] Y. G. Yang, Y. W. Teng, H. P. Chai, and Q. Y. Wen, "Verifiable quantum (k, n)-threshold secret key sharing," *Int. J. Theor. Phys.*, vol. 50, no. 3, pp. 792–798, Mar. 2011.
[20] Y. Yang, X. Jia, H.-Y. Wang, and H. Zhang, "Verifiable quantum (k, n)-threshold secret sharing," *Quantum Inf. Process*, vol. 11, no. 6, pp. 1619–1625, 2012.
[21] H. W. Qin and Y. W. Dai, "Verifiable (t, n) threshold quantum secret sharing using d-dimensional bell state," *Inf. Process. Lett.*, vol. 116, no. 5, pp. 351–355, May 2016.
[22] C. B. Lu, F. Y. Miao, and J. P. Hou, "Verifiable threshold quantum secret sharing with sequential communication," *Quantum Inf. Process.*, vol. 17, no. 11, Nov. 2018, Art. no. 310.
[23] F. Gao, S. J. Qin, F. Z. Guo, and Q. Y. Wen, "Cryptanalysis of the arbitrated quantum signature protocols," *Phys. Rev. A, Gen. Phys.*, vol. 84, no. 2, Aug. 2011, Art. no. 022344.
[24] T. Y. Wang, J. F. Ma, and X. Q. Cai, "The postprocessing of quantum digital signatures," *Quantum Inf. Process.*, vol. 16, no. 1, Jan. 2017, Art. no. 19.
[25] C.-Y. Wei, X.-Q. Cai, B. Liu, T.-Y. Wang, and F. Gao, "A generic construction of quantum-oblivious-key-transfer-based private query with ideal database security and zero failure," *IEEE Trans. Comput.*, vol. 67, no. 1, pp. 2–8, Jan. 2018.
[26] F. Gao, S. J. Qin, W. Huang, and Q. Y. Wen, "Quantum private query: A new kind of practical quantum cryptographic protocols," *Sci. Chin.-Phys. Mech. Astron.*, vol. 62, no. 7, Jul. 2019, Art. no. 070301.
[27] X. Jia, D. He, S. Zeadally, and L. Li, "Efficient revocable ID-based signature with cloud revocation server," *IEEE Access*, vol. 5, pp. 2945–2954, 2017.
[28] H. Du, Q. Y. Wen, and S. Zhang, "A provably-secure outsourced revocable certificateless signature scheme without bilinear pairings," *IEEE Access*, vol. 6, pp. 73846–73855, 2018.
[29] H. K. Lo and T.-M. Ko, "Some attacks on quantum-based cryptographic protocols," *Quantum Inf. Comput.*, vol. 5, no. 1, pp. 40–47, Jan. 2005.
[30] F. Gao, Q.-Y. Wen, and F.-C. Zhu, "Teleportation attack on the QSDC protocol with a random basis and order," *Chin. Phys. B*, vol. 17, no. 9, pp. 3189–3194, Sep. 2008.
[31] F. Gao, S.-J. Qin, F.-Z. Guo, and Q.-Y. Wen, "Dense-coding attack on three-party quantum key distribution protocols," *IEEE J. Quantum Electron.*, vol. 47, no. 5, pp. 630–635, Mar. 2011.
[32] F. Gao, Q. Y. Wen, and F. C. Zhu, "Comment on: 'Quantum exam' [Phys. Lett. A 350 (2006) 174]," *Phys. Lett. A*, vol. 360, no. 6, pp. 748–750, Mar. 2007.
[33] Q. Y. Cai, "The ping-pong protocol can be attacked without eavesdropping," *Phys. Rev. Lett.*, vol. 91, no. 10, Aug. 2003, Art. no. 109801.
[34] F. Gao, F. Z. Guo, Q. Y. Wen, and F. C. Zhu, "Consistency of shared reference frames should be reexamined," *Phys. Rev. A, Gen. Phys.*, vol. 77, no. 1, Jan. 2008, Art. no. 014302.
[35] X.-Q. Cai and C.-Y. Wei, "Cryptanalysis of an inter-bank E-payment protocol based on quantum proxy blind signature," *Quantum Inf. Process.*, vol. 12, no. 4, pp. 1651–1671, Apr. 2013.
[36] F. Gao, S. J. Qin, Q. Y. Wen, and F. C. Zhu, "A simple participant attack on the Brádler-Dušek protocol," *Quantum Inf. Comput.*, vol. 7, no. 4, pp. 329–334, May 2007.
[37] S. J. Qin, F. Gao, Q. Y. Wen, and F. C. Zhu, "Cryptanalysis of the Hillery-Bužek-Berthiaume quantum secret-sharing protocol," *Phys. Rev. A, Gen. Phys.*, vol. 76, no. 6, Dec. 2007, Art. no. 062324.
[38] F. Gao, F.-Z. Guo, Q.-Y. Wen, and F.-C. Zhu, "Comment on 'experimental demonstration of a quantum protocol for byzantine agreement and liar detection,'" *Phys. Rev. Lett.*, vol. 101, no. 20, Nov. 2008, Art. no. 208901.
[39] T. T. Song, J. Zhang, F. Gao, W. Qiao-Yan, and Z. Fu-Chen, "Participant attack on quantum secret sharing based on entanglement swapping," *Chin. Phys. B*, vol. 18, no. 4, pp. 1333–1337, Apr. 2009.
[40] T.-Y. Wang, Q.-Y. Wen, F. Gao, S. Lin, and F.-C. Zhu, "Cryptanalysis and improvement of multiparty quantum secret sharing schemes," *Phys. Lett. A*, vol. 373, no. 1, pp. 65–68, Dec. 2008.
[41] T. Y. Wang, Q. Y. Wen, and F. C. Zhu, "Cryptanalysis of multiparty quantum secret sharing with bell states and bell measurements," *Opt. Commun.*, vol. 284, no. 6, pp. 1711–1713, Mar. 2011.
[42] T.-Y. Wang and Q.-Y. Wen, "Security of a kind of quantum secret sharing with single photons," *Quantum Inf. Comput.*, vol. 11, nos. 5–6, pp. 434–443, May 2011.
[43] T. Y. Wang and Y. P. Li, "Cryptanalysis of dynamic quantum secret sharing," *Quantum Inf. Process.*, vol. 12, no. 5, pp. 1991–1997, May 2013.
[44] T.-Y. Wang, Y.-Z. Liu, C.-Y. Wei, X.-Q. Cai, and J.-F. Ma, "Security of a kind of quantum secret sharing with entangled states," *Sci. Rep.*, vol. 7, May 2017, Art. no. 2485.

XIAOQIU CAI received the B.S. degree in mathematics from Henan University, in 2003, and the M.S. degree in applied mathematics from Shaanxi Normal University, in 2007. She is currently pursuing the Ph.D. degree with the Beijing University of Posts and Telecommunications. She is also an Associate Professor with Luoyang Normal University. Her research interests include cryptography and quantum computing.



TIANYIN WANG received the B.S. degree in mathematics from Henan University, in 2002, the M.S. degree in applied mathematics from Shaanxi Normal University, in 2005, and the Ph.D. degree in cryptography from the Beijing University of Posts and Telecommunications, in 2010. He is currently a Professor with Luoyang Normal University. His research interests include quantum cryptography and information security.

RUILING ZHANG received the B.S. degree in mathematics from Henan Normal University, in 1986, and the M.S. degree in computer application from Northwestern Polytechnical University, in 2007. She is currently a Professor with Luoyang Normal University. Her research interests include cryptography and machine learning.



FEI GAO received the B.E. degree in communication engineering and the Ph.D. degree in cryptography from the Beijing University of Posts and Telecommunications, in 2002 and 2007, respectively, where he is currently a Professor. His research interests include quantum cryptography, quantum computing, and quantum information.