Quantum Information Processing (2019) 18:252
https://doi.org/10.1007/s11128-019-2365-8

Cryptanalysis of multiparty quantum digital signatures

Xiao-Qiu Cai[1,2] · Tian-Yin Wang[2] · Chun-Yan Wei[1,2] · Fei Gao[1,3]

Received: 6 December 2018 / Accepted: 28 June 2019 / Published online: 2 July 2019

Abstract
Multiparty quantum digital signatures play an important role in quantum networks which sign and distribute message among users with information-theoretic security. In this work, we give a cryptanalysis of a multiparty quantum digital signature scheme and then propose a new attacks strategy, whereby dishonest participants can frame an honest participant if they collude with each other. To prevent the framing attack, we study the relations between the signing key and each verification key, as well as the relations among different verification keys in this scheme, and then give the security requirements on the relations among different keys, which is also very useful for the next development of multiparty quantum digital signature schemes. Finally, we present a possible way to solve the security problem.

Keywords Unconditionally secure signature · Quantum digital signature · Framing attack

1 Introduction

Digital signature is a fundamental cryptographic primitive, which has been applied in many cases where the integrity and non-repudiation of messages are essential [1]. Nevertheless, the security of traditional digital signature schemes generally relies on some unproven assumptions related to the intractability of certain difficult mathematical problems, such as big number factorization problem and discrete logarithmic problem. With the rapid development of computing technology, especially the emer-

✉ Tian-Yin Wang
wangtianyin79@163.com

Fei Gao
gaof@bupt.edu.cn

[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] Center for Quantum Computing, Peng Cheng Laboratory, Shenzhen 518055, China

gence of advanced quantum algorithms [2], the security of traditional digital signature schemes is facing serious challenge. Once quantum computers are produced, they can be easily broken. The conception of unconditionally secure signature (USS) was therefore introduced by Chaum and Roijakkers [3], which attracted much attention due to the superiority of unconditional security, and then different proposals have also been presented besides the scheme of Chaum and Roijakkers [4]. However, most of these schemes depend on the assumption of either authenticated broadcast channels or a trusted third party, and crucially, the use of secure channels is necessary in all of them, which is not possible to realize with information-theoretic security by using only classical communication in reality [5].

Fortunately, the security of quantum digital signatures is based on the fundamental principles of quantum mechanics, and therefore it provides a new feasible way for USS. So far, a lot of novel three-party USS proposals including both theoretical and experimental aspects [6–19] have been continuously presented since the conception of quantum digital signatures was firstly introduced in 2001 [20], which make USS more and more practical. Contrast to the three-party case, the application of multiparty quantum digital signature schemes is more extensive. Nevertheless, it is very difficult to generalize three-party quantum digital signature scheme to multiparty case because of its complex security. As a result, there are very few work on multiparty quantum digital signature schemes. Recently, Arrazola et al gave the first security framework suitable for quantum USS schemes involving an arbitrary number of participants [21]. In addition, they generalize a three-party quantum digital signature scheme to the multiparty case and then prove its security against forging, repudiation and non-transferability. Most important of all, this generalized scheme retains the original advantage of three-party case that can be implemented by using any point-to-point quantum key distribution network and hence is easily realized in practice.

In this work, we analyze the security of the generalized multiparty quantum digital signature scheme [21] and then propose a new attack strategy, that is a framing attack. Using this attack, a certain number of dishonest participants can make an honest participant be penalized without being caught cheating if they collude with each other. In order to prevent the framing attack, we give the security requirements on the relations between the signing key and each verification key, as well as the relations among different verification keys. Furthermore, if a multiparty quantum digital signature scheme satisfies the given requirements, it is also secure against forging and repudiation, and therefore this work is very useful to the next development of multiparty quantum digital signature schemes. On this basis, we present an effective way to deal with the security problem at the end.

2 The generalized multiparty quantum digital signature scheme

Before presenting the security analysis of the generalized multiparty quantum digital signature scheme, let us firstly give a simple introduction of this scheme. There are a signer P_0 and N recipients $P_1, P_2, \ldots, P_N$ in this scheme, and the notations $X = \{x_1, x_2, \ldots, x_M\}$ and $\Sigma = \{0, 1\}^K$ denote the set of possible messages and the set of possible signatures, respectively, where $K = nN$ is a total signature's length (n is an integer and divisible by N). The fraction of dishonest participants can be defined as $d_f = 1 - h/N$, which determines the maximum verification level $l_{\max}$ by

$$(l_{\max} + 1)d_f < \frac{1}{2}, \tag{1}$$

where h is the number of honest participants. Then the program of this scheme can be described as follows.

(1) Every recipient P_i $(i = 1, 2, \ldots, N)$ shares a secret key of nM bits with P_0 and a secret key of $2\frac{nM}{N}(1 + \lceil \mathtt{log}_2 n \rceil)$ bits with each of the other recipients P_j $(j \neq i)$, which can be completed by quantum key distribution, where M is a positive integer and denotes the number of possible messages in X.

(2) For each possible message $x \in X$, P_0 selects a string σ^x of $K = nN$ bits uniformly randomly and divides it into N sections $\{\sigma_1^x, \sigma_2^x, \ldots, \sigma_N^x\}$. P_0 transmits σ_i^x to P_i $(i = 1, 2, \ldots, N)$ via a secure channel by the shared secret keys.

(3) For each possible message $x \in X$, P_i randomly divides the set $\{1, 2, \ldots, n\}$ into N disjoint subsets $\{p_{i,1}^x, p_{i,2}^x, \ldots, p_{i,N}^x\}$ and uses the bit values of σ_i^x at the randomly chosen positions $p_{i,j}^x$ to form the string $v_{i,j}^x$.

(4) For all $i \neq j$, every participant P_i sends the string $v_{i,j}^x$ and the positions $p_{i,j}^x$ to participant P_j via a secure channel by their shared secret keys. P_i holds $v_{i,i}^x$ and $p_{i,i}^x$ to himself.

(5) Every participant P_j defines a test for a section σ_i^x as the following. They form a shorter string $\sigma_{i,j}^x$ from σ_i^x by choosing just the bits corresponding to the positions $p_{i,j}^x$. Then the test is defined as

$$T_{i,j,l}^x(\sigma_i^x) = \begin{cases} 1 & \mathtt{if}\ h(\sigma_{i,j}^x, v_{i,j}^x) < s_l \frac{n}{N} \\ 0 & \mathtt{otherwise} \end{cases} \tag{2}$$

where $h(\sigma_{i,j}^x, v_{i,j}^x)$ is the Hamming distance between $\sigma_{i,j}^x$ and $v_{i,j}^x$, and s_l is a defined fraction that satisfies

$$\frac{1}{2} > s_{-1} > s_0 > s_1 > \cdots > s_{l_{\max}}. \tag{3}$$

(6) The verification function for a message–signature pair is defined as

$$\begin{aligned} &\mathtt{Ver}_{(i,l)}(x, \sigma) \\ &= \begin{cases} \mathtt{True} & \mathtt{if}\ \sum_{j=1}^{n} T_{j,i,l}^x(\sigma_j^x) > Nf_l \\ \mathtt{Faulse} & \mathtt{otherwise} \end{cases} \end{aligned} \tag{4}$$

here f_l is a threshold given by

$$f_l = \frac{1}{2} + (l + 1)d_f. \tag{5}$$

(7) $\mathtt{Sign}(x) = \sigma_x$ is the signature function.

(8) The dispute resolution method is majority vote (MV).

3 The cryptanalysis

As mentioned in [21], the validity of a message–signature pair in traditional digital signature schemes based on public-key cryptography is tested by a public verification function, but different participants have different verification functions in USS schemes, which makes it possible in principle for two or more participants to disagree on the validity of a message–signature pair. Consequently, USS schemes must have a mechanism to judge the authenticity of a message–signature pair when some subset of users disagree whether a given message–signature pair should be accepted. In particular, dispute resolution is necessary to convince an outsider of the authenticity of a disputed message–signature pair. Anyone has an access to the public verification method in traditional digital signature schemes, in the sense there are no outsiders to the scheme. Furthermore, it has been shown that a USS scheme that satisfies the definition of unforgeability and has an appropriate dispute resolution method also satisfies non-repudiation and transferability, both of which are also essential for any reasonable signature scheme, which means that dispute resolution is very necessary and crucial to a USS scheme.

A simple strategy for dispute resolution is to designate a trusted arbiter who has the final word on the validity of a message–signature pair [22–24]. Obviously, the drawback of this strategy is the necessity of trust. Another strategy for dispute resolution is MV, in which more than half of the users determine the valid of a message–signature pair or not, and hence the security of the scheme does not depend on an arbiter any longer by this way. Contributing to this advantage, it has been adopted in many quantum digital signature schemes [6–19,21]. However, the MV strategy requires all the participants to vote on the validity of a message–signature pair, and therefore it is rather complicated and resource expensive. Therefore, it is expected that dispute resolution will be invoked relatively rarely, otherwise it will greatly decrease the efficiency and restrict the application of this kind of quantum digital signature schemes in reality. To attain this goal, some necessary penalties should be introduced in the scheme, for example, the participant who loses in MV will be responsible for the expensive resources. By this way, whether a rational participant is honest or dishonest, he will avoid any action that could lead to someone invoking it if he might lose the dispute resolution. In this sense, the dispute resolution almost does not affect the effectiveness of the scheme.

To guarantee the security and reduce invoking dispute, two different types of thresholds s_l and f_l are chosen in the generalized multiparty quantum digital signature scheme, both rely on the verification level l and are determined by the real fraction d_f of dishonest participants. The first threshold s_l is used to determine whether a given part of the message–signature pair passes the test or not by Eq. (2). The second threshold f_l is used to determine how many parts of the message–signature pair need to pass the test in order for it to be accepted at this level by Eq. (4). It is evident that two honest participants can differ by at most $d_f N$ tests, and therefore it is thought that the attack of making honest participants disagrees on the validity of a message–signature pair can be effectively prevented by choosing f_l and f_{l-1} such that

$$f_l - f_{l-1} > d_f \tag{6}$$

from Eq. (4). Nevertheless, to choose the proper thresholds f_l and f_{l-1} that satisfy Ineq. (6), the numbers of dishonest participants must be clarified for each recipient P_i $(i = 1, 2, \ldots, N)$.

Unfortunately, there is no way to discriminate a participant is honest or dishonest except the parties concerned, which means the real fraction d_f of dishonest participants is unknown to other participants. In general, both the threshold s_l and f_l should be preset according to the security requirement of practical application. As a result, there is no way to guarantee the thresholds f_l and f_{l-1} must satisfy the Ineq. (6), which will give a chance for dishonest participants to deceive. Specifically, here we propose a new attack strategy, for simplicity, we name it a framing attack, whereby dishonest participants can frame an honest participant in dispute resolution. Suppose that the verification threshold f_l is set in advance, and then the signer P_0 can frame an honest participant if he/she colludes with n' dishonest participants, where $n' = N - [Nf_l] - 1 < \frac{N}{2}$ and [ ] is a function of extracting the integral part of a real number.

Without loss of generalization, suppose that the prior n' participants $P_1, P_2, \ldots, P_{n'}$ are dishonest, and they collude with P_0 to frame an honest participant $P_{n'+1}$; the framing attack can be described as follows.

(i) This step is the same as step (1).
(ii) This step is also the same as step (2) except that the signer P_0 sends a fake section $\sigma_{n'+1}^{x'}$ to $P_{n'+1}$.
(iii) This step is also the same as step (3).
(iv) For all $i \neq j$, every participant P_i transmits the string $v_{i,j}^x$ and the positions $p_{i,j}^x$ to participant P_j over a secure channel by using their shared secret keys except that n' dishonest participants $P_1, P_2, \ldots, P_{n'}$ send a fake string $v_{i,n'+1}^{x'}$ $(i = 1, 2, \ldots, n' + 1)$ to the participant $P_{n'+1}$, respectively. The participant P_i keeps $v_{i,i}^x$ and $p_{i,i}^x$ to himself.
(v) The remaining steps are also the same as that in the generalized multiparty quantum digital signature scheme.

From this attack, it can be seen that every participant $P_i\,(i \neq n'+1)$ holds $N-1$ normal strings $v_{1,i}^x, v_{2,i}^x, \ldots, v_{n',i}^x, v_{n'+2,i}^x, \ldots, v_{N,i}^x$ and a fake string $v_{n'+1,i}^x$ except that the participant $P_{n'+1}$ holds $N-n'-1$ normal strings $v_{n'+2,n'+1}^x, v_{n'+3,n'+1}^x, \ldots, v_{N,n'+1}^x$ and $n' + 1$ fake strings $v_{1,n'+1}^x, v_{2,n'+1}^x, \ldots, v_{n'+1,n'+1}^x$. As does in the generalized multiparty quantum digital signature scheme, all the normal strings can pass the verification at the level l in Formu. (2) because no extra errors are introduced, but the fake strings can be made not pass the same verification by the dishonest participants through flipping all or most of the bit values when sending them. Accordingly, for each participant $P_i\,(i = 1, 2, \ldots, n')$,

$$\sum_{j=1}^{n} T_{j,i,l}^x(\sigma_j^x) = N - 1 > Nf_l. \tag{7}$$

As a result, the message–signature pair (x, σ_x) can pass the verification of each participant $P_i (i = 1, 2, \ldots, n')$. Nevertheless, for the participant $P_{n'+1}$,

$$\begin{aligned}\sum_{j=1}^{n} T^x_{j,n'+1,l}(\sigma^x_j) &= N - (n' + 1) \\ &= N - (N - [Nf_l] - 1 + 1) \\ &= [Nf_l] \\ &< Nf_l,\end{aligned} \tag{8}$$

which means that the message–signature pair (x, σ_x) cannot pass the participant $P_{n'+1}$'s verification, and therefore there is a disagreement on the validity of the message–signature pair (x, σ_x). As mentioned in [21], when the validity of a message–signature pair (x, σ_x) is invoked, a MV dispute resolution method $\mathtt{MV}(x; \sigma_x)$ is defined by the following rule:

1. $\mathtt{MV}(x; \sigma_x)$ = Valid if $\mathtt{Ver}(i, -1)$= True for more than half of the participants.
2. $\mathtt{MV}(x; \sigma_x)$ = Invalid, otherwise, where $\mathtt{Ver}(i, -1)$ is the verification function at the level $l = -1$.

Since $s_{-1} > s_0 > s_1 > \cdots > s_{l_{\max}}$, we can get $h(\sigma^x_{i,j}, v^x_{i,j}) < s_{-1}\frac{n}{N}$ from $h(\sigma^x_{i,j}, v^x_{i,j}) < s_l\frac{n}{N}$. Therefore, for each participant $P_i (i = 1, 2, \ldots, n', n' + 2, \ldots, N)$, $Ver(i, -1)$=True. Clearly, there are $N - 1 > \frac{N}{2}$ participants who will vote the message–signature pair (x, σ_x) is true when $N > 2$, and thus $\mathtt{MV}(x; \sigma_x)$ = Valid. As mentioned above, the honest participant $P_{n'+1}$ who loses in the MV will be responsible for the expensive resources. So far, the framing attack has been successfully completed.

It should be noted that this attack is significative in practice, for example, suppose that the honest participant $P_{n'+1}$ is a bank, and the signer P_0 represents a company, who signs a cheque, this cheque is refused by the bank $P_{n'+1}$ because it can not pass the verification of the bank $P_{n'+1}$ according to this attack, which will have a bad influence on the repudiation of the bank $P_{n'+1}$.

4 The relations among different keys

In this section, we will give the relations between the signing key and the verification key, as well as the relations among different verification keys in the generalized multiparty quantum digital signature scheme, which are useful to deal with the framing attack. For simplicity, assume that the signing key for the message x is $K^x_{P_0}$, and the corresponding verification key held by the recipient P_i $(i = 1, 2, \ldots, N)$ is $K^x_{P_i}$.

Let us firstly analyze the relations between the signing key $K^x_{P_0}$ and the verification key $K^x_{P_i}$ in the generalized multiparty quantum digital signature scheme. As the same requirements as that in traditional digital signature schemes based on public-key cryptography, on the one hand, the signing key $K^x_{P_0}$ and the verification key $K^x_{P_i}$ must be closely correlated in order to make the message–signature (x, σ_x) pass the verification of recipient P_i, on the other hand, to prevent the repudiation of the signer P_0, the signing key $K_{P_0}^x$ must be different and cannot be elicited from the verification key $K_{P_i}^x$. Furthermore, the signing key $K_{P_0}^x = \sigma^x$ is factually the signature σ_x on the message x, but the verification key $K_{P_i}^x$ is just a part of $K_{P_0}^x$, i.e.,

$$\begin{aligned} K_{P_i}^x &= \sigma_i^x || v_{1,i}^x || v_{2,i}^x || \cdots || v_{i-1,i}^x || v_{i+1,i}^x || \\ &\quad \cdots || v_{N-1,i}^x || v_{N,i}^x, \end{aligned} \tag{9}$$

where the notation || denotes the concatenation of bit string. Clearly, the signer P_0 does not know the remaining bits of $K_{P_i}^x$ except σ_i^x because he gains no access to the precise position $p_{j,i}^x$ of each section $v_{j,i}^x$ $(j \neq i)$ in $K_{P_0}^x$. In other words, the signer P_0 holds all bits of the signing key $K_{P_0}^x$ and every recipient P_i only knows a fraction of it, i.e.,

$$\frac{1}{N} + (N-1)\frac{1}{N^2} = \frac{2N-1}{N^2}, \tag{10}$$

but the signer P_0 does not know the part $K_{P_i}^x$ held by P_i except σ_i^x, which is similar to establish an oblivious key between the signer P_0 and the recipient P_i. Due to the speciality, it is possible for multiple dishonest recipients to forge a valid message–signature pair (x, σ_x) if the fraction of the signing key $K_{P_0}^x$ they know is enough large. As mentioned in the generalized multiparty quantum digital signature scheme [21], when a dispute on the validity of a message–signature pair (x, σ_x) appears, dispute resolution is invoked and then it gives the final judgement outcome by the MV strategy; specifically, if more than half of the participants vote "True" on (x, σ_x), all participants must accept it is valid. Additionally, a participant P_i votes "True" if and only if $\texttt{Ver}(i, -1)$=True in MV, here choosing $l = -1$ is mainly to prevent the repudiation of the signer P_0, but in this case,

$$f_l = f_{-1} = \frac{1}{2} + (-1+1)d_f = \frac{1}{2}. \tag{11}$$

Consequently, the number of honest participants must be more than $\frac{N}{2}$, which is in accord with the prior assumption on security. In reverse, only if the number of dishonest participants is limited to less than $\frac{N}{2}$, the security of the scheme can be guaranteed, which means it can tolerant the worst case, i.e., there are $\frac{N}{2} - 1$ dishonest participants, in the case, $\frac{N}{2} - 1$ dishonest participants can know the fraction of the signing key $K_{P_0}^x$ is

$$\begin{aligned} &|| \bigcup_{j=1}^{\frac{N}{2}-1} K_{P_{i_j}}^x || \div || K_{P_0}^x || \\ &= \frac{1}{N}\left(\frac{N}{2} - 1\right) + \frac{1}{N^2}\left(\frac{N}{2} - 1\right)\left(\frac{N}{2} + 1\right) \\ &= \frac{3}{4} - \frac{N+1}{N^2} \end{aligned} \tag{12}$$

where $i_j \in \{1, 2, \ldots, N\}$ and the notation $|| \; ||$ denotes the length of a bit string. The fraction $\frac{3}{4} - \frac{N+1}{N^2}$ approaches to $\frac{3}{4}$ with the increase of the number N. Therefore, the fraction of the signing key $K^x_{P_0}$ that allows dishonest participants to know is not more than $\frac{3}{4} - \frac{N+1}{N^2}$ in order to resist the joint forgery attack from them, and the upper bound is close to $\frac{3}{4}$.

Secondly, let us analyze the relations among different verification keys $K^x_{P_1}$, $K^x_{P_2}$, $\ldots$, $K^x_{P_N}$ in the generalized multiparty quantum digital signature scheme. Because each verification key $K^x_{P_i}$ is a part of the signing key $K^x_{P_0}$ and the signature σ_x on a message x is the signing key $K^x_{P_0}$, any two verification keys $K^x_{P_i}$ and $K^x_{P_j}$ must be different to prevent the forgery of dishonest participants. At the same time, any two verification keys $K^x_{P_i}$ and $K^x_{P_j}$ must be closely correlated to guarantee the transferability of the message–signature pair (x, σ_x). From Eq. (9), it can be seen that each verification key $K^x_{P_i}$ held by P_i constitutes of N sections, of which σ^x_i directly comes from the signer P_0, and the remaining come from the other $N-1$ recipients, respectively. By simple deducing, it can be found that the communal part between any two verification keys $K^x_{P_i}$ and $K^x_{P_j}$ are $v^x_{i,j}$ and $v^x_{j,i}$, that is $K^x_{P_i} \bigcap K^x_{P_j} = v^x_{i,j} || v^x_{j,i}$, which takes up

$$\begin{aligned} &||K^x_{P_i} \bigcap K^x_{P_j}|| \div ||K^x_{P_i}|| \\ &= 2 \times \frac{1}{N^2} \div \frac{2N-1}{N^2} \\ &= \frac{2}{2N-1} \end{aligned} \tag{13}$$

of them, respectively.

To sum up, in the generalized multiparty quantum digital signature scheme, the relation between the signing key $K^x_{P_0}$ and each verification key $K^x_{P_i}$ is an imperfect oblivious key relation between the signer P_0 and the recipient P_i, and the signing key $K^x_{P_0}$ cannot be elicited more than $\frac{3}{4} - \frac{N+1}{N^2}$ from $\frac{N}{2} - 1$ different verification keys. Furthermore, any two verification keys $K^x_{P_i}$ and $K^x_{P_j}$ have a communal part to guarantee their correlation, but the fraction of the communal part between them is not very large ($\frac{2}{2N-1}$) to prevent the forgery of dishonest participants.

5 The way to resist the framing attack

Now let us discuss how to prevent the proposed framing attack. From Steps (ii) and (iv) in Sect. 3, it can be seen that the key to the success of this attack is that the dishonest participants $P_0, P_1, P_2, \ldots, P_{n'}$ can send fake sections of verification key to the honest participant $P_{n'+1}$ without being caught cheating. By this way, they make the fraction of fake sections in the verification key $K^x_{P_{n'+1}}$ exceeds the allowable threshold $1 - f_l$, which gives rise to $P_{n'+1}$'s disagreement on the validity of the message–signature pair (x, σ_x). At the same time, they make more than half of the participants vote the message–signature pair (x, σ_x) is true in dispute resolution by sending the real sections to other participants. Thus, if there is a way for $P_{n'+1}$ to detect the deception from these dishonest participants, the framing attack can be effectively prevented. Nevertheless, his verification key $K^x_{P_{n'+1}} = \sigma^x_{n'+1}||v^x_{1,n'+1}||v^x_{2,n'+1}||\cdots||v^x_{n',n'+1}||v^x_{n'+2,n'+1}||\cdots||v^x_{N-1,n'+1}||v^x_{N,n'+1}$ directly comes from P_0 and the other $N-1$ recipients, which means everyone definitely knows the part sent by himself, and thus there is no way for $P_{n'+1}$ to discriminate whether a received section is true or not in the distribution stage if the signer P_0 colludes with the n' recipients $P_1, P_2, \ldots, P_{n'}$. What's worse, there is also no way for $P_{n'+1}$ to prove the fake sections come from these dishonest participants $P_0, P_1, P_2, \ldots, P_{n'}$ in dispute resolution. Therefore, this way is not feasible with the present method of establishing the signing key and verification keys in the generalized multiparty quantum digital signature scheme.

The second way for $P_{n'+1}$ is to avoid inducing disagreement on the validity of the message–signature pair (x, σ_x) by lowering the verification threshold f_l. Nevertheless, the number n' of dishonest recipients is dependent on the threshold f_l, and thus if the threshold f_l is set, there always exists such a number n' that can make the inequation

$$\sum_{j=1}^{n} T^x_{j,n'+1,l}(\sigma^x_j) < N f_l \tag{14}$$

is right no matter how small f_l is. In addition, although the required number n' of dishonest recipients becomes more and more large with the lowering of the verification threshold f_l, n' is always less than $\frac{N}{2}$ under the condition that the threshold f_l must be not less than $\frac{1}{2}$. Therefore, the disagreement on the validity of the message–signature pair (x, σ_x) always can be made by these dishonest participants $P_0, P_1, P_2, \ldots, P_{n'}$, which means this way is also not feasible.

The third way for $P_{n'+1}$ is to make at least $\frac{N}{2}$ participants approve the message–signature pair (x, σ_x) is invalid in MV. For each other honest participant $P_i (i = n'+2, \ldots, N)$, $\sum_{j=1}^{n} T^x_{j,i,l}(\sigma^x_j) = N-1$, if P_i votes "Faulse", the verification function $\texttt{Ver}(i, -1)$= True need be redefined as

$$\texttt{Ver}_{(i,l)}(x, \sigma) = \begin{cases} \texttt{True} & \texttt{if } \sum_{j=1}^{n} T^x_{j,i,l}(\sigma^x_j) = N \\ \texttt{Faulse} & \texttt{otherwise} \end{cases} \tag{15}$$

which will give rise to the worst security problem of repudiation because $f_l = 1 \gg f_{-1} = \frac{1}{2}$. Accordingly, this way is also not feasible. Another possible way is not to penalize the loser in dispute resolution, but this will greatly affect the effectiveness of the scheme, and therefore a balance between the penalization and effectiveness should be considered in a practical application.

From the above analysis, it can be seen that there is no good way to prevent the framing attack with the present method of establishing the signing key and verification keys in the generalized multiparty quantum digital signature scheme.

Finally, let us study how to resist the framing attack by establishing new signing key and verification keys in multiparty quantum digital signature schemes. From the perspective of the relations among different keys, the main reason for this security problem is that the relation between the signing key $K^x_{P_0}$ and each verification key $K^x_{P_i}$

is not fully asymmetrical and each other recipient $P_j (j \neq i)$ definitely knows one part $v^x_{j,i}$ of $K^x_{P_i}$, which gives a chance for these dishonest participants $P_0, P_1, P_2, \ldots, P_{n'}$ to frame $P_{n'+1}$ by sending him fake sections $\sigma^x_{n'+1}||v^x_{1,n'+1}||v^x_{2,n'+1}|| \cdots ||v^x_{n',n'+1}$. Therefore, if a perfect oblivious key is established between the signer P_0 and each recipient $P_i (i = 1, 2, \ldots, N)$, and any two verification keys $K^x_{P_i}$ and $K^x_{P_j}$ have a communal part unknown to both P_i and P_j while the fraction of this part satisfies some restriction, the framing attack can be effectively prevented. More specifically, to prevent the framing attack and guarantee the security of signature against forging and repudiation, the relations among different keys should satisfy the following security requirements.

(a) The relation between the signing key $K^x_{P_0}$ and each verification key $K^x_{P_i}$ is perfectly oblivious, and $\frac{||K^x_{P_i}||}{||K^x_{P_0}||} \geq \frac{2N-1}{N^2}$ for $i = 1, 2, \ldots, N$.

(b) $\frac{||\bigcup_{j=1}^{\frac{N}{2}-1} K^x_{P_{i_j}}||}{||K^x_{P_0}||} \leq \frac{3}{4} - \frac{N+1}{N^2}, i_j \in \{1, 2, \ldots, N\}$.

(c) $K^x_{P_i} \bigcap K^x_{P_j}$ is unknown to both P_i and P_j, and $\frac{2}{2N-1} \leq \frac{||K^x_{P_i} \bigcap K^x_{P_j}||}{||K^x_{P_i}||} \leq k_{s_l} \ll 1$ for all $i \neq j$, where the upper bound $\leq k_{s_l}$ depends on the verification threshold s_l.

The signing key $K^x_{P_0}$ and each verification key $K^x_{P_i}$ that satisfy all the requirements (a)–(c) can be established by an oblivious transfer from one to many. It should be noted that oblivious transfer has been realized and applied in quantum private queries [23–28]. Furthermore, both the upper bound and the lower bound in these requirements are obtained from the generalized multiparty quantum digital signature scheme, which may be not optimal, and therefore these requirements are not necessary to design a secure multiparty quantum digital signature scheme in the sense.

6 Conclusion

In conclusion, we analyze the security of a multiparty quantum digital signature scheme and propose a framing attack. Using this attack, a certain number of dishonest recipients $P_1, P_2, \ldots, P_{n'}$ can frame an honest participant $P_{n'+1}$ without being caught cheating when they collude with the signer P_0, which is in conflict with the security requirements of USS. Furthermore, we study the relations among different keys and then give the security requirements (a)–(c), which are sufficient to design a secure multiparty quantum digital signature scheme. On this basis, we present an effective way to deal with the security problem at the end. Finally, it should be noted that this analysis method may be valid to many multiparty digital signatures under the similar model as in [21], but it does not mean it can be extended to arbitrary multiparty digital signatures. For example, in a multiparty digital signature scheme with a trusty third party, the dispute is solved by the trusty third party but not MV, which excludes the conditions that this analysis method can be applied. We hope this work shed some light on the next development of multiparty quantum digital signatures.

Acknowledgements We are grateful to the anonymous reviewers for helpful comments. This work was supported by the National Natural Science Foundation of China (Grant Nos. 61602232, 61672110, 61572081, 61671082, 61572246), the Program for Science & Technology Innovation Research Team in Universities of Henan Province (Grant No. 18IRTSTHN014), The key scientific and technological research project of Henan Province (Grant No. 182102310930).

References

1. Du, H.Z., Wen, Q.Y.: Certificateless proxy multi-signature. Inf. Sci. **276**, 21–30 (2014)
2. Shor, P.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**(5), 1484–1509 (1997)
3. Chaum, D., Roijakkers, S.: Unconditionally-secure digital signatures. In: Advances in Cryptology-Crypto 1990, pp. 206–214. Springer, Berlin (1991)
4. Hanaoka, G., Shikata, J., Zheng, Y.L., et al.: Unconditionally secure digital signature schemes admitting transferability. In: Advances in Cryptology-Asiacrypt 2000, pp. 130–142. Springer, Berlin (2000)
5. Ueli, M.M.: Secret key agreement by public discussion from common information. IEEE Trans. Inf. Theory **39**, 733–742 (1993)
6. Clarke, P.J., Collins, R.J., Dunjko, V., et al.: Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light. Nat. Commun. **3**, 1174 (2012)
7. Dunjko, V., Wallden, P., Andersson, E.: Quantum digital signatures without quantum memory. Phys. Rev. Lett. **112**, 040502 (2014)
8. Collins, R.J., Donaldson, R.J., Vedran, D., et al.: Realization of quantum digital signatures without the requirement of quantum memory. Phys. Rev. Lett. **113**, 040502 (2014)
9. Wallden, P., Dunjko, V., Kent, A., et al.: Quantum digital signatures with quantum key distribution components. Phys. Rev. A **91**, 042304 (2015)
10. Wang, T.Y., Cai, X.Q., Ren, Y.L., et al.: Security of quantum digital signatures for classical messages. Sci. Rep. **5**, 9231 (2015)
11. Donaldson, R.J., Collins, R.J., Kleczkowska, K., et al.: Experimental demonstration of kilometer-range quantum digital signatures. Phys. Rev. A **93**, 012329 (2016)
12. Amiri, R., Wallden, P., Kent, A., et al.: Secure quantum signatures using insecure quantum channels. Phys. Rev. A **93**, 032325 (2016)
13. Yin, H.L., Fu, Y., Chen, Z.B.: Practical quantum digital signature. Phys. Rev. A **93**, 032316 (2016)
14. Collins, R.J., Amiri, R., Fujiwara, M., et al.: Experimental transmission of quantum digital signatures over 90 km of installed optical fiber using a differential phase shift quantum key distribution system. Opt. Lett. **41**, 4883–4886 (2016)
15. Puthoor, I.V., Amiri, R., Wallden, P., et al.: Measurement-device-independent quantum digital signatures. Phys. Rev. A **94**, 022328 (2016)
16. Wang, T.Y., Ma, J.F., Cai, X.Q.: The postprocessing of quantum digital signatures. Quant. Inf. Process. **16**, 19 (2017)
17. Yin, H.L., Fu, Y., Liu, H., et al.: Experimental quantum digital signature over 102 km. Phys. Rev. A **95**, 032334 (2017)
18. Yin, H.L., Wang, M.L., Tang, Y.L., et al.: Experimental measurement-device-independent quantum digital signatures over a metropolitan network. Phys. Rev. A **95**, 042338 (2017)
19. Roberts, G.L., Lucamarini, M., Yuan, Z.L., et al.: Experimental measurement-device-independent quantum digital signatures. Nat. Commun. **8**, 1098 (2017)
20. Gottesman, D., Chuang, I.: Quantum digital signatures. arXiv:quant-ph/0105032 (2001)
21. Arrazola, J.M., Wallden, P., Andersson, E.: Multiparty quantum signature schemes. Quant. Inf. Comput. **6**, 0435 (2016)
22. Gao, F., Qin, S.J., Guo, F.Z., et al.: Cryptanalysis of the arbitrated quantum signature protocols. Phys. Rev. A **84**, 022344 (2011)
23. Sun, H.W., Zhang, L., Zuo, H.J., et al.: Offline arbitrated quantum bind dual-signature protocol with better performance in resisting existential forgery attack. Int. J. Theor. Phys. **57**, 2695–2708 (2018)
24. Fan, L.: A blind signature protocol with exchangeable signature sequence. Int. J. Theor. Phys. **57**, 3850–3858 (2018)

25. Gao, F., Liu, B., Wen, Q.Y., et al.: Flexible quantum private queries based on quantum key distribution. Opt. Exp. **20**, 17411 (2012)
26. Gao, F., Liu, B., Huang, W., et al.: Postprocessing of the oblivious key in quantum private query. IEEE. J. Sel. Top. Quant. **21**, 6600111 (2015)
27. Wei, C.Y., Wang, T.Y., Gao, F.: Practical quantum private query with better performance in resisting joint-measurement attack. Phys. Rev. A **93**, 042318 (2016)
28. Wei, C.Y., Cai, X.Q., Liu, B., et al.: A generic construction of quantum-oblivious-key-transfer-based private query with ideal database security and zero failure. IEEE Trans. Comput. **67**(1), 2–8 (2018)

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