SCIENTIFIC REPORTS

OPEN

SUBJECT AREAS:
QUANTUM MECHANICS
QUANTUM INFORMATION

Received
8 August 2014

Accepted
24 February 2015

Published
18 March 2015

Correspondence and requests for materials should be addressed to T.-Y.W. (wangtianyin79@163.com)

Security of quantum digital signatures for classical messages

Tian-Yin Wang[1,2], Xiao-Qiu Cai[1], Yan-Li Ren[3] & Rui-Ling Zhang[4]

[1]School of Mathematical Science, Luoyang Normal University, Luoyang, 471022, China, [2]Start Travel Collaborative Innovation center of Zhongyuan Economic area, Luoyang Normal University, Luoyang 471022, China, [3]School of Communication and Information Engineering, Shanghai University, Shanghai, 200444, China, [4]School of Information Technology, Luoyang Normal University, Luoyang 471022, China.

Quantum digital signatures can be used to authenticate classical messages in an information-theoretically secure way. Previously, a novel quantum digital signature for classical messages has been proposed and gave an experimental demonstration of distributing quantum digital signatures from one sender to two receivers. Some improvement versions were subsequently presented, which made it more feasible with present technology. These proposals for quantum digital signatures are basic building blocks which only deal with the problem of sending single bit messages while no-forging and non-repudiation are guaranteed. For a multi-bit message, it is only mentioned that the basic building blocks must be iterated, but the iteration of the basic building block still does not suffice to define the entire protocol. In this paper, we show that it is necessary to define the entire protocol because some attacks will arise if these building blocks are used in a naive way of iteration. Therefore, we give a way of defining an entire protocol to deal with the problem of sending multi-bit messages based on the basic building blocks and analyse its security.

Digital signature (DS) is a fundamental cryptographic primitive, which has been frequently used in e-commerce and e-government to ensure both the integrity and the origin of a message. However, the degree of security provided by current classical digital signature (CDS) schemes generally depends on certain unproven assumptions related to the intractability of certain difficult mathematical problems, such as big number factorization problem[1] and discrete logarithmic problem[2]. With the rapid development of quantum computing[3], the security of such CDS schemes is seriously challenged.

Fortunately, quantum digital signature (QDS) provides a way of authenticating classical messages with information-theoretic security against forging and repudiation. Gottesman and Chuang introduced the concept of QDS in 2001, and proposed the first QDS scheme for classical messages based on quantum one-way functions[4].

Recently, a novel QDS proposal for classical messages was put forth (named C-proposal hereafter), which has been implemented using phase-encoded coherent states of light in experiments[5]. However, it needs quantum memory like previous proposals, which makes it also unfeasible in practice with current technology. To deal with this problem, Dunjko et al gave the first practical QDS proposal for classical messages, in which quantum memory is no longer required[6]; in addition, this proposal has been implemented using just standard linear optical components and photodetectors[7]. Furthermore, Dunjko et al presented another two different QDS protocols for classical messages, which essentially only use the same experimental requirements as quantum key distribution[8]. Most important of all, in contrast with other DS schemes, this kind of proposals[5–8] have an important advantage: the trusted authorities are not needed any longer.

These QDS proposals[5–8] are basic building blocks, which only deal with the problem of sending single bit messages while no-forging and non-repudiation are guaranteed. For a long multi-bit message, it is only mentioned that the basic building blocks must be iterated, but the iteration of the basic building blocks still does not suffice to define the entire protocol, and therefore there still must be an additional set of rules which stipulate how disputes are resolved, or how validity of a long message is proven and so on.

In this paper, we show that it is necessary to define the entire protocol because some attacks will arise if these basic building blocks are used just in a naive way of iteration. Furthermore, based on the basic building blocks in these proposals[5–8], we propose an entire protocol to deal with the problem of sending multi-bit messages, in which the rules on how to resolve disputes, and how to prove the validity of a multi-bit message and so on are given.

Results

As mentioned above, these QDS proposals[5–8] are basic building blocks, which only deal with the problem of sending single bit messages while no-forging and non-repudiation are guaranteed. For a long multi-bit message, it is only mentioned that the basic building block must be iterated, but the iteration of the basic building block still does not suffice to define the entire protocol. Specifically, some attacks will arise if these building blocks are used to deal with the problem of sending a multi-bit message in a naive way of iteration. Without loss of generality, we take three players' case of C-proposal as an example.

The C-proposal. Before presenting the attacks, let us give a simple introduction of C-proposal, which can be described in Figure 1.

The analysis of C-proposal. From C-proposal, it can be seen that if its basic building blocks are used to deal with the problem of sending a multi-bit message just in a naive way of iteration, and a signed multi-bit message (M, PrivKey$_M$) (we will call it a message-signature pair hereafter) will be verified in the way of bit by bit, and there is no correlation among quantum signatures on signed message bits except that their labels are pre-determined and sequential. Furthermore, as mentioned in Ref. 8, a QDS protocol has two stages: a preparation stage (distribution) and a message stage. The distribution stage serves to establish the required classical-quantum (or fully classical) correlations, which can later, in the message stage, be used by the sender to transmit messages to the recipients. Additionally, no further communication with any of the other players is required when the sender (say Alice) sends a message-signature pair to a recipient, and both the transferal and the verification of the message-signature pair should no longer require any feedback from Alice at all; in addition, Alice may send a lot of different message-signature pairs to the recipient and other ones later (in the message stage). Therefore, the verifier Charlie knows neither the length of a signed message nor the initial label of quantum signature for the message sent by the recipient. These will give a chance for a dishonest recipient (say Bob) to forge an integrated message-signature pair by the following known-message attacks.

Forgery attack 1. Suppose that Bob has obtained a valid message-signature pair (M, PrivKey$_M$) from Alice, where $M = m_1 \| m_2 \| \cdots \| m_n$, and PrivKey$_M$ = PrivKey$_{m_1}$ $\|$ PrivKey$_{m_2}$ $\| \cdots \|$ PrivKey$_{m_n}$, here $\|$ denotes the concatenation of bits or bit strings. He chooses some continuous bits from M (e.g., the first half bits) and the corresponding private keys from PrivKey$_M$, which are denoted as (M', PrivKey$_{M'}$), where

$$M' = m_i \| m_{i+1} \| \cdots \| m_j, 1 \le i \le j \le n \tag{1}$$

and

$$\text{PrivKey}_{M'} = \text{PrivKey}_{m_i} \| \text{PrivKey}_{m_{i+1}} \| \cdots \| \text{PrivKey}_{m_j} \tag{2}$$

Then he sends the new message-signature pair (M', PrivKey$_{M'}$) to Charlie. It can be seen that the forged message-signature pair (M', PrivKey$_{M'}$) is a subset of the valid message-signature pair (M, PrivKey$_M$) and each signed bit m_k is not changed, $i \le k \le j$, i.e., $M' \subseteq M$, PrivKey$_{M'} \subseteq$ PrivKey$_M$. Therefore, each bit-signature pair (m_k, PrivKey$_{m_k}$) of (M', PrivKey$_{M'}$) matches the corresponding

(1) To sign a single bit (message $m = 0$ or 1) in the future, Alice generates two sequences $\texttt{PrivKey}_0 = \{\theta_1^0, ..., \theta_L^0\}$ and $\texttt{PrivKey}_1 = \{\theta_1^1, ..., \theta_L^1\}$, where $\theta_k^m \in \{\frac{2r\pi}{N} | r = 0, ..., N-1\}$. The pair $(m, \texttt{PrivKey}_m)$ is called a private key pair for message m.

(2) Alice generates two copies of a sequence of coherent states $\texttt{QuantSig}_0 = \otimes_{l=1}^{L} \rho_l^k$ with the coherent phases matching the angles in the sequence $\texttt{PrivKey}_0$, thus $\rho_k^0 = |e^{i\theta_k^0}\alpha\rangle\langle e^{i\theta_k^0}\alpha|$, where α is a real positive amplitude. A sequence of such states is called a quantum signature. She sends a copy of the quantum signature to each of Bob and Charlie each, informing them that they correspond to message $m = 0$. Alice then does analogously for the message $m = 1$.

(3) Bob and Charlie send their copies of the sequences $\texttt{QuantSig}_0$ and $\texttt{QuantSig}_1$ through a multiport, saving the output states in quantum memory, noting which quantum signature corresponds to message $m = 0$ and which to $m = 1$.

(4) To sign a single bit m with Bob, Alice sends the pair $(m, \texttt{PrivKey}_m)$ to Bob over an untrusted channel. To authenticate the signature, Bob generates coherent states of amplitude α with the relative phase defined by the declared private key, and interferes them individually with the states he has in his quantum memory. He monitors the number of photodetection events on his signal null-port arm and confirms the authenticity of the message if the number of photodetection events was below $s_a L$.

(5) To forward m, Bob forwards to Charlie the pair $(m, \texttt{PrivKey}_m)$. Charlie then performs an analogous procedure to Bob, and he accepts the message coming from Alice if his number of photodetection events is below $s_v L$.

Figure 1 | C-proposal. (1) To sign a single bit (message $m = 0$ or 1) in the future, Alice generates two sequences $\text{PrivKey}_0 = \{\theta_1^0, \ldots, \theta_L^0\}$ and $\text{PrivKey}_1 = \{\theta_1^1, \ldots, \theta_L^1\}$, where $\theta_k^m \in \left\{\frac{2r\pi}{N} | r = 0, \ldots, N-1\right\}$. The pair ($m$, PrivKey$_m$) is called a private key pair for message m. (2) Alice generates two copies of a sequence of coherent states $\text{QuantSig}_0 = \otimes_{l=1}^{L} \rho_l^k$ with the coherent phases matching the angles in the sequence PrivKey$_0$, thus $\rho_k^0 = \left|e^{i\theta_k^0}\alpha\right\rangle\left\langle e^{i\theta_k^0}\alpha\right|$, where α is a real positive amplitude. A sequence of such states is called a quantum signature. She sends a copy of the quantum signature to each of Bob and Charlie each, informing them that they correspond to message $m = 0$. Alice then does analogously for the message $m = 1$. (3) Bob and Charlie send their copies of the sequences QuantSig$_0$ and QuantSig$_1$ through a multiport, saving the output states in quantum memory, noting which quantum signature corresponds to message $m = 0$ and which to $m = 1$. (4) To sign a single bit m with Bob, Alice sends the pair (m, PrivKey$_m$) to Bob over an untrusted channel. To authenticate the signature, Bob generates coherent states of amplitude α with the relative phase defined by the declared private key, and interferes them individually with the states he has in his quantum memory. He monitors the number of photodetection events on his signal null-port arm and confirms the authenticity of the message if the number of photodetection events was below $s_a L$. (5) To forward m, Bob forwards to Charlie the pair (m, PrivKey$_m$). Charlie then performs an analogous procedure to Bob, and he accepts the message coming from Alice if his number of photodetection events is below $s_v L$.

quantum signature $\mathrm{QuantSig}_{m_k}$ stored by Charlie, which means Bob's forgery introduces no error and therefore the forged message-signature pair (M', $\mathrm{PrivKey}_{M'}$) will be accepted by Charlie. For example, suppose that Bob has received a message-signature pair (M, $\mathrm{PrivKey}_M$) from Alice, where M = "don't pay Bob 100$." then Bob will be able to send Charlie the message M' (M' = "pay Bob 100$.") and the corresponding $\mathrm{PrivKey}_{M'}$ to Charlie, claiming that it comes from Alice, where the initial "Don't" is omitted. For $M' \subseteq M$, $\mathrm{PrivKey}_{M'} \subseteq \mathrm{PrivKey}_M$, Charlie will accept that it comes from Alice and give 100$ to Bob.

Forgery attack 2. Suppose that Bob has obtained two valid message-signature pairs (M_1, $\mathrm{PrivKey}_{M_1}$) and (M_2, $\mathrm{PrivKey}_{M_2}$) from Alice, where $M_1 = m'_1 \| m'_2 \| \cdots \| m'_{n_1}$, $\mathrm{PrivKey}_{M_1} = \mathrm{PrivKey}_{m'_1} \left\| \mathrm{PrivKey}_{m'_2} \right\| \cdots \left\| \mathrm{PrivKey}_{m'_{n_1}} \right.$, $M_2 = m''_1 \| m''_2 \| \cdots \| m''_{n_2}$, and $\mathrm{PrivKey}_{M_2} = \mathrm{PrivKey}_{m''_1} \left\| \mathrm{PrivKey}_{m''_2} \right\| \cdots \left\| \mathrm{PrivKey}_{m''_{n_2}} \right.$. He chooses some continuous bits from M_1 and M_2 (e.g., the last half bits of M_1 and the first half bits of M_2) with their corresponding private keys to form a new message-signature pair (M'', $\mathrm{PrivKey}_{M''}$), where

$$M'' = m'_{i'} \| m'_{i'+1} \| \cdots \| m'_{n_1} \| m''_1 \| \cdots \left\| m''_{j'}, 1 \le i' \le n_1, 1 \le j' \le n_2 \right. \quad (3)$$

and

$$\mathrm{PrivKey}_{M''} = \mathrm{PrivKey}_{m'_{i'}} \| \cdots \left\| \mathrm{PrivKey}_{m'_{n_1}} \right\| \mathrm{PrivKey}_{m''_1} \| \cdots \| \mathrm{PrivKey}_{m''_{j'}} \quad (4)$$

Then he sends the forged message-signature pair (M'', $\mathrm{PrivKey}_{M''}$) to Charlie. Clearly, $M'' \subseteq M_1 \cup M_2$, $\mathrm{PrivKey}_{M''} \subseteq \mathrm{PrivKey}_{M_1} \cup \mathrm{PrivKey}_{M_2}$, and therefore by similar analysis as that in forgery attack 1, the forged message-signature pair (M'', $\mathrm{PrivKey}_{M''}$) will also pass Charlie's verification.

It is noted that the label of quantum signature for the last bit of M_1 and the label of quantum signature for the first bit of M_2 must be successive in forgery attack 2, i.e., if the label of quantum signature $\mathrm{QuantSig}_{m'_{n_1}}$ for m'_{n_1} is l, then that for m''_1 must be $l + 1$, which ensures the labels of quantum signature for the forged message-signature pair (M'', $\mathrm{PrivKey}_{M''}$) are sequential and Bob's deception is not detected by Charlie. Additionally, an outside adversary Eve also can forge a valid message-signature pair when the message-signature pairs are transmitted over an insecure channel. For example, she intercepts them when Alice sends message-signature pairs to a legal recipient, and then she forges a new message-signature pair by the way that Bob does in the above forgery attacks.

As mentioned in Refs. 9, 10, a signature scheme is broken if an opponent can do any of the following with a nonnegligible probability:

Universal forgery (total break), in which he/she can forge a signature for any message.

Selective forgery, in which he/she can forge a signature for a particular message chosen by him/her.

Existential forgery, where he/she can forge a signature for at least one message, but he/she has no control over the message whose signature he obtains, i.e., the message may be random or nonsensical.

However, if the basic building blocks in these proposals[5–8] are used to deal with the problem of sending a multi-bit message in a naive way of iteration, a dishonest recipient or an outside adversary can successfully forge a valid signature for a particular message (chosen from a valid signed message by himself in advance) by the above known-message attacks. Furthermore, the forged message is not random or nonsensical in many cases. For example, if the signed message sent by Alice is a contract, forgery attack 1 allows Bob to delete some items that may be not beneficial to him, and forgery attack 2 allows him to add some new items from another one. Moreover, as a legal replacement for handwritten signatures, DS is not only used to send a message; in addition, the signatory of a signature scheme would like to feel that he/she may sign arbitrary documents prepared by others without fear of compromising his/her security, such as the case of a notary public who must sign more-or-less arbitrary documents on demand[10]. Therefore, it is a natural and reasonable assumption that an opponent may gain access to valid signatures for any messages of his/her choice (where each message may be chosen in a way that depends on the signatures of previously chosen messages), i.e., we should allow an opponent can do a forgery in the model of adaptive chosen-message attacks; in this case, the opponent can forge a valid signature on any message chosen by himself/herself in advance.

Discussion

It has been shown that the iteration of the basic building blocks of dealing with the problem of sending single bit messages still does not suffice to define the entire protocol. Therefore, it is a necessary and significative work to study the problem of sending multi-bit messages based on the basic building blocks.

As we know, the main tasks of DS are to prevent impersonation, repudiation and message tampering in data transfer, of which the key is to guarantee the integrity of signed messages, i.e., any alteration of a signed message will be detected in the process of verifying. In these proposals[5–8], nobody can forge a valid signature for a single message bit except with a negligible probability. Furthermore, the label of quantum signature for each message bit is predetermined and sequential. Therefore, if the start and the end of a signed message are tagged, i.e., both the initial label and the last one of quantum signatures for the signed message cannot be changed, whereby the integrity of a signed message can be guaranteed. To this goal, one way is that Charlie can acquire the two labels from the signatory Alice before verifying, but it needs some communications or feedbacks between them, which is obviously contradictory to the natural requirement for DS transferal and verification, and another way is that both the start and the end of a signed message are different from the message bits, meanwhile the signatures for them are not to be forged, which can be realized by a special encoding way. In the following, we propose an entire protocol to deal with the problem of sending multi-bit messages, in which the validity of the special encoding way to guarantee the integrity of a signed multi-bit message is proven.

Methods

A method to define an entire protocol for dealing with the problem of sending a multi-bit message is described as follows.

(I) The preparation (distribution) stage is the same as that in these proposals[5–8].

(II) In the message stage, Alice encodes each bit 0(1) of the message M by the codeword 000(010) before signing, i.e., $0 \to 000$, $1 \to 010$. Then she adds a special codeword 111 to both the start and the end of the message, in this way, the message M is encoded to $\widehat{M}$. After that, Alice signs each bit $\widehat{M}_i$ of $\widehat{M}$ by using the signing block in these proposals[5–8], where $\widehat{M}_i$ is the ith bit of $\widehat{M}$. Finally, she sends the resulting message-signature pair ($\widehat{M}$, $\mathrm{PrivKey}_{\widehat{M}}$) to Bob, where $\mathrm{PrivKey}_{\widehat{M}}$ is the concatenation of the signature $\mathrm{PrivKey}_{\widehat{M}_i}$ for the bit $\widehat{M}_i$ of $\widehat{M}$. If each signature $\mathrm{PrivKey}_{\widehat{M}_i}$ for the bit $\widehat{M}_i$ of $\widehat{M}$ passes his verification, Bob confirms the authenticity of the message $\widehat{M}$.

(III) In the verifying stage, when receiving the resulting message-signature pair ($\widehat{M}$, $\mathrm{PrivKey}_{\widehat{M}}$) forwarded by Bob, Charlie firstly checks whether all codewords are legal, i.e., all codewords in the message bit sequence $\widehat{M}$ should be 000 or 010 except that the start and the end are the codeword 111. If it is not so, Charlie thinks the message M has been tampered with and rejects it. Otherwise, he continues to verify the validity of the signed message M by the same way as that in the corresponding proposal[5–8]. If each bit $\widehat{M}_i$ of the signed message $\widehat{M}$ passes his verification, Charlie decodes $\widehat{M}$ to M and accepts it coming from Alice and has not been tampered with; otherwise, he rejects it.

By this way, if Bob wants to forge a new valid message-signature pair by forgery attack 1 or forgery attack 2, he must find at least one new codeword 111 in the encoding bit sequence $\widehat{M}$ while guaranteeing there is no illegal codeword in the forged

message. Nevertheless, it is not possible. To draw this conclusion, some necessary lemmas should be proven.

Lemma 1 Suppose that $S = s_1\|s_2\|\cdots\|s_n$, $s_i \in \{000, 010\}$, $i = 1, 2, \ldots, n$, is a bit sequence, then $111 \notin S$.

The conclusion of this lemma is obvious, but it implies that if each bit 0(1) of a message M is encoded by the codeword 000(010), then it is impossible to appear a codeword 111 in the corresponding encoding sequence. For example, let a message $M = 01011001$, then the message M is encoded to the bit sequence $S =$ 000010000010010000000010, we cannot find a codeword 111 in the bit sequence S.

Lemma 2 Suppose that $S = 111\|s_1\|s_2\|\cdots\|s_n\|111$, $s_i \in \{000, 010\}$, $i = 1, 2, \ldots, n$, is a bit sequence, it is impossible to find a sequence $S' = 111\|s'_1\|s'_2\|\cdots\|s'_k\|111$, $s'_i \in \{000, 010\}$, $i = 1, 2, \ldots, k$ such that $S' \subseteq S$ except $S' = S$.

Proof. By Lemma 1, $111 \notin s_1\|s_2\|\cdots\|s_n$. In addition, both the first bit and the last one of the codewords 000 and 010 are 0, thus it is impossible to find a new codeword 111 by the way of taking one bit from a message codeword 000 or 010 and two bits from the codeword 111, or taking two bits from a message codeword 000 or 010 and one bit from the codeword 111. Therefore, it is impossible to find a new codeword 111 in the middle of the bit sequence S, and hence we cannot find a sequence $S' = 111\|s'_1\|s'_2\|\cdots\|s'_k\|111$, $s'_i \in \{000, 010\}$, $i = 1, 2, \ldots, k$ such that $S' \subseteq S$ except $S' = S$. For example, let $S = 111000010010000010111$, obviously, there is no codeword 111 in the middle of the bit sequence S, and therefore it is impossible to find a sequence $S' = 111\|s'_1\|s'_2\|\cdots\|s'_k\|111$, $s'_i \in \{000, 010\}$, $i = 1, 2, \ldots, k$ such that $S' \subseteq S$ except $S' = 111000010010000010111$.

Lemma 3 Suppose that $S_j = 1_{j_{s_1}} 1_{j_{s_2}} 1_{j_{s_3}} \left\|s_1^j\right\|s_2^j\| \cdots \left\|s_{n_j}^j\right\| 1_{j_{e_1}} 1_{j_{e_2}} 1_{j_{e_3}}$, $s_i^j \in \{000, 010\}$, $i = 1, 2, \ldots, n_j$, $j = 1, 2, \ldots, l$, it is impossible to find a sequence $S' = 111\|s'_1\|s'_2\|\cdots\|s'_k\|.111$, $s'_i \in \{000, 010\}$, $i = 1, 2, \ldots, k$ such that $S' \subseteq S_1\|S_2\|\cdots\|S_l$ except $S' = S_j$, $j = 1, 2, \ldots, l$.

Proof. When $l = 1$, this lemma reduces to Lemma 2.

When $l = 2$,

$$S_1\left\|S_2 = 1_{s_{s_1}} 1_{s_{s_2}} 1_{s_{s_3}} \left\|s_1^1\right\|s_2^1\right\| \cdots \left\|s_{n_1}^1\right\| 1_{e_{e_1}} 1_{e_{e_2}} 1_{e_{e_3}} \left\|1_{2_{s_1}} 1_{2_{s_2}} 1_{2_{s_3}} \left\|s_1^2\right\|s_2^2\right\| \cdots \left\|s_{n_2}^2\right\| 1_{2_{e_1}} 1_{2_{e_2}} 1_{2_{e_3}}, \quad (5)$$

in this case, in order to find a sequence $S' = 111\|s'_1\|s'_2\|\cdots\|s'_k\|111$, $s'_i \in \{000, 010\}$, $i = 1, 2, \ldots, k$ such that $S' \subseteq S_1\|S_2\|\cdots\|S_l$, it is necessary to find at least one new codeword 111. By lemma 2 and Formula (5), the new codeword 111 can be only chosen from $1_{1_{e_1}} 1_{1_{e_2}} 1_{1_{e_3}} \left\|1_{2_{s_1}} 1_{2_{s_2}} 1_{2_{s_3}}\right.$; if we choose $1_{1_{e_1}} 1_{1_{e_2}} 1_{1_{e_3}}$, we must choose $1_{1_{s_1}} 1_{1_{s_2}} 1_{1_{s_3}}$ as the start codeword, but in the case, $S' = S_1$; otherwise, there must exist at least one codeword $s'_i (s'_i \in S')$ such that $s'_i \notin \{000, 010\}$. If we choose $1_{1_{e_2}} 1_{1_{e_3}} 1_{2_{s_1}}$, whether we choose $1_{1_{s_1}} 1_{1_{s_2}} 1_{1_{s_3}}$ or $1_{e_{e_1}} 1_{e_{e_2}} 1_{e_{e_3}}$ as another codeword 111, obviously, there must exist at least one codeword $s'_i (s'_i \in S')$ such that $s'_i \notin \{000, 010\}$; if we choose $1_{1_{e_3}} 1_{2_{s_1}} 1_{2_{s_2}}$ or $1_{2_{s_1}} 1_{2_{s_2}} 1_{2_{s_3}}$, we will face the same difficult. Therefore, in any case, it is impossible to find a sequence $S' = 111\|s'_1\|s'_2\|\cdots\|s'_k\|111$, $s'_i \in \{000, 010\}$, $i = 1, 2, \ldots, k$ such that $S' \subseteq S_1||S_2$ except $S' = S_j$, $j = 1, 2$.

Suppose that when $n = l - 1$, this conclusion is right. When $n = l$, let $S = S_1\|S_2\|\cdots\|S_{l-1}$, according to the former assumption, it is impossible to find a sequence $S' = 111\|s'_1\|s'_2\|\cdots\|s'_k\|111$, $s'_i \in \{000, 010\}$, $i = 1, 2, \ldots, k$ such that $S' \subseteq S$ except $S' = S_j$, $j = 1, 2, \ldots, l - 1$. By similar analysis as $l = 2$, we can get that it is impossible to find a sequence $S' = 111\|s'_1\|s'_2\|\cdots\|s'_k\|111$, $s'_i \in \{000, 010\}$, $i = 1, 2, \ldots, k$ such that $S' \subseteq S||S_l$ except $Sy = S_j$, $j = 1, 2, \ldots, l$.

As a result, it is impossible to find a sequence $S' = 111\|s'_1\|s'_2\|\cdots\|s'_k\|111$, $s'_i \in \{000, 010\}$, $i = 1, 2, \ldots, k$ such that $S' \subseteq S_1\|S_2\|\cdots\|S_l$ except $S' = S_j$, $j = 1, 2, \ldots, l$. We also can give an example to show that. Let $S_1 = 111000000111$, $S_2 = 111000010111$, $S_3 = 111010010111$, then $S_1||S_2||S_3 = 111000000111111000010111$ 111010010111, from the bit sequence 111000000111111000010111111010010111, it can be seen that we cannot find a sequence $S' = 111\|s'_1\|s'_2\|\cdots\|s'_k\|111$, $s'_i \in \{000, 010\}$, $i = 1, 2, \ldots, k$ such that $S' \subseteq S_1||S_2||S_3$ except $S' = 111000000111$, 111000010111 or 111010010111.

From Lemmas 1, 2 and 3, we can conclude that even if an opponent has obtained a lot of message-signature pairs, he/she cannot forge a new valid message-signature pair by forgery attack 1 or forgery attack 2. It is noted that if the opponent can forge a bit-signature pair, he/she can forge a valid message-signature pair by forgery attack 1 or forgery attack 2 because he/she can forge a new codeword 111. Nevertheless, in C-proposal, it has been proven that the probability of forging a bit-signature pair is

$$\varepsilon_{\text{forging}} \leq 2\exp\left(-\frac{2}{9}g^2 L\right). \quad (6)$$

By simple computation, we can get that the probability of forging a signature for a new codeword 111 is not more than $\varepsilon_{\text{forging}}$. Furthermore, the probability $\varepsilon_{\text{forging}}$ is exponentially close to 0 with the increase of the parameter L. Consequently, if a large parameter L is chosen, the probability of forging a signature for a new codeword 111 is negligible.

Therefore, if the basic building blocks of dealing with the problem of sending single bit messages is secure against forging, our method can effectively guarantee the integrity of signed messages in the sense that it can prevent currently known attacks.

Finally, it should be noted that our method does not influence the security of QDS against repudiation, but it may be only one of several possibilities to guarantee the integrity of signed messages.

1. Rivest, R. L., Shamir, A. & Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21**, 120–126 (1978).
2. ElGamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory* **31**, 469–472 (1985).
3. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26**, 1484–1509 (1997).
4. Gottesman, D. & Chuang, I. Quantum digital signatures. Preprint at http://arxiv.org/abs/quant-ph/0105032 (2001).
5. Clarke, P. J. *et al.* Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light. *Nat. Commun.* **3**, 1174 (2012).
6. Dunjko, V., Wallden, P. & Andersson, E. Quantum digital signatures without quantum memory. *Phys. Rev. Lett.* **112**, 040502 (2014).
7. Collins, R. J. *et al.* Realization of quantum digital signatures without the requirement of quantum memory. *Phys. Rev. Lett.* **113**, 040502 (2014).
8. Dunjko, V., Wallden, P. & Andersson, E. Quantum digital signatures with quantum key distribution components. Preprint at http://arxiv.org/abs/1403.5551 (2014).
9. Gao, F., Qin, S. J., Guo, F. Z. & Wen, Q. Y. Cryptanalysis of the arbitrated quantum signature protocols. *Phys. Rev. A* **84**, 022344 (2011).
10. Goldwasser, S., Micali, S. & Rivest, R. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM J. Comput.* **17**, 281–308 (1988).

Acknowledgments

This work was supported by NSFC (Grant Nos. 61202317, 61272015, 61202367), HASTIT (Grant No. 13HASTIT042), HYKT (Grant No. 2012GGJS-157), NSFS (Grant No. 12ZR1443700), and IPSMEC (Grant No. 14YZ020).

Author contributions

T.Y. and R.L. analysed the security of C-proposal and proposed the forgery attacks. T.Y., X.Q. and Y.L. proposed the way to guarantee the integrity of signed messages. T.Y. and X.Q. wrote the main manuscript text. All authors reviewed the manuscript.

Additional information

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Wang, T.-Y., Cai, X.-Q., Ren, Y.-L. & Zhang, R.-L. Security of quantum digital signatures for classical messages. *Sci. Rep.* 5, 9231; DOI:10.1038/srep09231 (2015).