Quantum Inf Process (2017) 16:19
DOI 10.1007/s11128-016-1460-3

The postprocessing of quantum digital signatures

Tian-Yin Wang[1,2,3] · **Jian-Feng Ma**[4] · **Xiao-Qiu Cai**[2]

Received: 29 March 2016 / Accepted: 27 October 2016 / Published online: 18 December 2016

Abstract Many novel quantum digital signature proposals have been proposed, which can effectively guarantee the information-theoretic security of the signature for a singe bit against forging and denying. Using the current basic building blocks of signing a single bit, we give a new proposal to construct an entire protocol for signing a long message. Compared with the previous work, it can improve at least 33.33% efficiency.

Keywords Quantum digital signature · Integrity · Forgery attack · Authentication

1 Introduction

Digital signature (DS) is a fundamental cryptographic primitive, which can effectively guarantee both the authenticity and transferability of messages. Nowadays, DS is widely used in electronic transactions, software distribution and other cases where it is vital to guarantee the security of a signed message against forging and denying.

✉ Xiao-Qiu Cai
xiaoqiucai@aliyun.com

Tian-Yin Wang
wangtianyin79@163.com

Jian-Feng Ma
jfma@mail.xidian.edu.cn

1 School of Computer Science and Technology, Xidian University, Xi'an 710071, China

2 School of Mathematical Science, Luoyang Normal University, Luoyang 471934, China

3 Start Travel Collaborative Innovation Center of Zhongyuan Economic Area, Luoyang Normal University, Luoyang 471934, China

4 School of Network and Information Security, Xidian University, Xi'an 710071, China

Nevertheless, the security of traditional digital signature schemes are generally based on difficult mathematical problems and therefore is facing serious challenges with the rapid development of computing technology, especially the appearance of fast quantum algorithms [1,2]. Fortunately, quantum digital signature (QDS) was introduced by Gottesman and Chuang [3], whose security is based on the fundamental principles of quantum mechanics. The early proposals [3–5] require preparing complex quantum states, performing quantum computation on these states and storing them in quantum memory, which make these proposals impractical. Subsequently, novel QDS proposals [6–8] were presented, in which quantum memory were not needed any longer. In addition, these proposals can be realized with standard quantum-optical techniques, and some of them have been demonstrated in experiments [6,9,10]. Nevertheless, there is an impractical assumption that authenticated quantum channels between participants are necessary in security analysis. Recently, two practical QDS schemes [11,12] were independently proposed by removing the requirement of authenticated quantum channels, respectively. Furthermore, the feasibility of experimental implementing QDS over a distance of more than one hundred kilometers had been given in [12].

However, the previous works are not sufficient to define an entire and practical QDS protocol. First, none of them has been explicitly generalized to more than three participants, and their security goals have not been formally defined. Second, a security framework for QDS schemes that includes rigorous definitions of security suitable for multiparty QDS protocols has not yet been proposed [13]. Finally, how to sign a long message has not been considered. Therefore, there still must be an additional set of rules which stipulate how disputes are resolved, and how validity of a long message is proven and so on.

Arrazola et al. [13] firstly introduced the rigorous security definitions by extending the security definitions of unconditionally secure signature (USS) given by Swanson and Stinson [14]. Furthermore, they provided a full security framework for QDS schemes and proved several properties that USS must satisfy. Additionally, they generalized a QDS protocol in [8] to multiparty case, proving its security against forging, repudiation and non-transferability.

Two of us firstly proposed a way to define an entire protocol for signing a long message with the current basic building blocks of signing a single bit [15]. In this work, we reconsider this problem and give a new proposal to deal with it. Compared with the previous work [15], the new proposal is also by the way of message tagging and using protected codewords, but it can reduce at least 33.33% classical and quantum resources.

2 The proposed proposal

In this section, we will give a new proposal to design an entire protocol with the current building blocks of signing a single bit, which includes three stages: the initial stage, the signing stage and the verifying stage. At the same time, a signer Alice, a trusted third party (TTP) Joe, who judges the validity of signatures and gives a fair decision when disputes appear, and several recipients Bob, Charlie, David and so on are also involved in this protocol. Specifically, this proposal can be described as follows.

2.1 The initial stage

For each possible message bit $k_i = 0$ and $k_i = 1$ in the future, $i = 1, 2, \ldots, N$, where the integer N is sufficiently large, Alice generates its signing key S_{k_i} and the corresponding verification key V_{k_i}, respectively, of which all the verification keys $\{V_{k_1}, V_{k_2}, \ldots, V_{k_N}\}$ are distributed to TTP and each recipient. This stage can be easily completed by one of the ways in [6–12]. It should be noted that all the signing keys and verification keys are labeled and sequential, and the key S_{k_i} used to sign 0 or 1 is predetermined, that is, if $k_i = 0$, it shall be used to sign a bit 0; otherwise, it shall be used to sign bit 1. Furthermore, the verification key V_{k_i} distributed to TTP and each recipient may be different, which depends on the adopted way in [6–12], but their functions are the same to verify the validity of a signature generated by the corresponding signing key S_{k_i}, and therefore, here we do not distinguish them with different notations any longer.

2.2 The signing stage

Without loss of generality, suppose that the recipient Bob wants the signer Alice to sign a classical message $M = m_1||m_2||\cdots||m_n, m_i \in \{0, 1\}, i = 1, 2, \ldots, n$, where $||$ denotes the concatenation between bits.

(1) Bob sends the message M to Alice via a classical authenticated channel.
(2) When receiving the message M, Alice firstly checks whether it is within the border delimited in advance. If it is not so, she rejects it. Otherwise, for each bit $m_i, i = 1, 2, \ldots, n$, if it is 0, she encodes it with the codeword 00; if it is 1, she encodes it with the codeword 01. After that, she adds a special codeword 11 to both the start and the end of the codeword sequence. In this way, the message M is transformed to a bit sequence $\widehat{M}$ whose length is $2n + 4$, i.e., $\widehat{M} = \widehat{m}_1||\widehat{m}_2||\cdots||\widehat{m}_{2n+4}$, here $\widehat{m}_1 = \widehat{m}_2 = \widehat{m}_{2n+3} = \widehat{m}_{2n+4} = 1$ and $\widehat{m}_j \in \{0, 1\}, j = 3, 4, \ldots, 2n + 2$.
(3) Alice firstly chooses $2n+4$ signing keys $S_{k_{l+1}}, S_{k_{l+2}}, \ldots, S_{k_{l+2n+4}}$ in sequence with $k_{l+j} = \widehat{m}_j, j = 1, 2, \ldots, 2n + 4$. Second, for each bit $\widehat{m}_j, j = 1, 2, \ldots, 2n + 4$, she signs it with the corresponding key $S_{k_{l+j}}$, here the signature for the bit $\widehat{m}_j$ is denoted as $Sig_{S_{k_{l+j}}}(\widehat{m}_j)$. Finally, she sends the resulting message-signature pair $(M, Sig(M), l)$ to Bob via a classical authenticated channel, where M is the original message, l is the sequence number of the first signing key in the whole, and

$$\begin{aligned} Sig(M) = {} & Sig_{S_{k_{l+1}}}(\widehat{m}_1)||Sig_{S_{k_{l+2}}}(\widehat{m}_2) \\ & ||\cdots||Sig_{S_{k_{l+2n+4}}}(\widehat{m}_{2n+4}) \end{aligned} \tag{1}$$

(4) When Bob receives the message-signature pair $(M, Sig(M), l)$, he transforms the message M to $\widehat{M}$ by the same way as Alice does in the step (2). Then he checks whether each signature $Sig_{S_{k_{l+j}}}(\widehat{m}_j)$ is true or not by using the corresponding verification key $V_{k_{l+j}}$. If each bit-signature pair $(\widehat{m}_j, Sig_{S_{k_{l+j}}}(\widehat{m}_j))$ can pass the

verification, he confirms that the message-signature pair $(M, Sig(M), l)$ comes from Alice and the message M has not been tampered with. Otherwise, he rejects it.

2.3 The verifying stage

When other recipient say Charlie receives the resulting message-signature pair $(M, Sig(M), l)$ forwarded by Bob via a classical authenticated channel, he can verify their validity by using the similar way as Bob does in step (4), i.e., if each bit-signature pair $(\widehat{m}_j, Sig_{S_{k_{l+j}}}(\widehat{m}_j))$ $(j = 1, 2, \ldots, 2n+4)$ matches with the verification key $V_{k_{l+j}}$ distributed by Alice in the initial stage, Charlie confirms the authenticity of the message M; otherwise, he thinks that the message M does not come from Alice or it has been tampered with.

If no dispute appears, this protocol has been completed so far; otherwise, if there is a dispute, for example, the signer Alice denies her signature or a recipient doubts the authenticity of a message-signature pair $(M, Sig(M), l)$, in this case, they send the message-signature pair $(M, Sig(M), l)$ to TTP via a classical authenticated channel. Once receiving the request, TTP firstly verifies the validity of the message-signature pair $(M, Sig(M), l)$ in the same way as Bob does in the step (4) of Sect. 2.2 and then gives an objective decision according to the verification outcome, that is to say, if the signature can pass his verification, he judges the message M comes from Alice and it has not been tampered with; otherwise, he accepts Alice's appeal that the signature is not generated by her.

2.4 The security analysis

It has been proven that the signature for a single bit is unconditionally secure against forging and denying in [6–12], that is to say, nobody can forge a valid bit-signature pair $(\widehat{m}_i, Sig_{S_{k_{l+i}}}(\widehat{m}_i))$ except with a negligible probability even if he/she has infinite resources including computing, storing and so on. Obviously, the presented protocol is based on the basic building blocks of signing a single bit, which means that nobody can generate a valid message-signature pair $(M, Sig(M), l)$ by the way of forging a new $(\widehat{m'}_i, Sig_{S_{k_{l+i}}}(\widehat{m'}_i))$ except the signer Alice. Therefore, this way is not valid to the presented protocol, and the other way is recombining the bit-signature pair $(\widehat{m}_j, Sig_{S_{k_{l+j}}}(\widehat{m}_j))$ to form a valid message-signature pair $(M', Sig(M'), l')$ by using known message-signature pair $(M, Sig(M), l)$, i.e., choosing some bits from known messages and their signatures to recombine a new message-signature pair $(M', Sig(M'), l')$, which has been shown by forgery attacks 1 and 2 in [15]. Nevertheless, it is also not feasible to this protocol even if an opponent Eve has gained access to a lot of valid message-signature pairs $(M_1, Sig(M_1), l_1), (M_2, Sig(M_2), l_2), \ldots, (M_T, Sig(M_T), l_T)$.

First, the label of verification key for each message bit 0 or 1 is predetermined and sequential, which requires the bit-signature pairs chosen from known message-signature pairs must be also in sequence.

Second, it can be seen that every legal signature

$$\begin{aligned} Sig(M) &= Sig_{S_{k_{l+1}}}(\widehat{m}_1)||Sig_{S_{k_{l+2}}}(\widehat{m}_2)|| \\ &\quad \cdots ||Sig_{S_{k_{l+2n+3}}}(\widehat{m}_{2n+3})||Sig_{S_{k_{l+2n+4}}}(\widehat{m}_{2n+4}) \\ &= Sig_{S_{k_{l+1}}}(1)||Sig_{S_{k_{l+2}}}(1)||Sig_{S_{k_{l+3}}}(\widehat{m}_3)|| \\ &\quad \cdots ||Sig_{S_{k_{l+2n+3}}}(1)||Sig_{S_{k_{l+2n+4}}}(1) \end{aligned} \tag{2}$$

are tagged with $Sig_{S_{k_{l+1}}}(1)||Sig_{S_{k_{l+2}}}(1)$ and $Sig_{S_{k_{l+2n+3}}}(1)\,||Sig_{S_{k_{l+2n+4}}}(1)$ at the start and the end, i.e., both the start and the end of a valid signature $Sig(M)$ must be a signature on the special codeword 11. Therefore, in order to forge a valid message-signature pair, it is necessary to find two signatures on the special codeword 11.

Finally, it can be seen from both the signing stage and the verification stage that except the first two bit signatures and the last two in a legal signature $Sig(M)$, all the other bit signatures are on the bit sequence consisted of the codewords 00 and 01.

As a result, if an opponent Eve wants to forge a message-signature pair $(M', Sig(M'), l')$ (here the length of the message M' is n') that can pass the verification, she must make the forged signature

$$\begin{aligned} Sig(M') &= Sig_{S_{k_{l'+1}}}(\widehat{m'}_1)||Sig_{S_{k_{l'+2}}}(\widehat{m'}_2)|| \\ &\quad \cdots ||Sig_{S_{k_{l'+2n'+4}}}(\widehat{m'}_{2n'+4}) \end{aligned} \tag{3}$$

satisfy the following three requirements:

(1) $m'_1 m'_2 = 11, m'_{2n'+3} m'_{2n'+4} = 11$;
(2) $m'_{2j+1} m'_{2j+2} \in \{00, 01\}$, $j = 1, 2, \ldots, n'$;
(3) each bit-signature pair $(\widehat{m}_i, Sig_{S_{k_{l'+i}}}(\widehat{m}_i))$, $i = 1, 2, \ldots, 2n' + 4$ matches the corresponding verification key $V_{k_{l'+i}}$, that is to say, all of them must pass the verification.

However, it is impossible to recombine such a message-signature pair $(M', Sig(M'), l')$ no matter how many valid message-signature pairs $(M_1, Sig(M_1), l_1)$,$(M_2, Sig(M_2), l_2)$, …,$(M_T, Sig(M_T), l_T)$ Eve has gained access to. To prove the conclusion, some necessary preliminaries should be given firstly.

Theorem 1 *Suppose that $C = c_1||c_2||\cdots||c_t$, $c_i \in \{00, 01\}, i = 1, 2, \ldots, t$, is a bit sequence, i.e., C is a codeword sequence consisted of 00 and 01, then we can get $11 \notin C$.*

Proof By simple analysis, it can be obtained that there are only four cases 00||00, 00||01, 01||00 and 01||01 between the concatenation of 00 and 01. In addition, the codeword sequence C just includes the two codewords 00 and 01. Therefore, three kinds of codewords 00, 01 and 10 can be found in the sequence C, but it is impossible to find a codeword 11 no matter how large t is, that is $11 \notin C$.

Noted that this theorem is simple, but it implies that if each bit 0(1) of a message M is encoded by the codeword 00(01), then it is impossible to find a codeword 11 in the corresponding encoding sequence. For example, let a message $M = 001011$, then

the message M is transformed to the bit sequence $C = 000001000101$, in which it is impossible to find such a codeword 11. □

Theorem 2 *Suppose that* $C = 11||c_1||c_2||\cdots||c_t||11$, $c_i \in \{00, 01\}$, $i = 1, 2, \ldots, t$, *is a bit sequence, it is impossible to find a sequence* $C' = 11||c'_1||c'_2||\cdots||c'_k||11$ *with* $c'_i \in \{00, 01\}$, $i = 1, 2, \ldots, k$ *such that* $C' \subseteq C$ *except* $C' = C$. *Noted that here all the codewords in* C' *are in sequence.*

Proof To find a sequence $C' = 11||c'_1||c'_2||\cdots||c'_k||11$ with $c'_i \in \{00, 01\}, i = 1, 2, \ldots, k$ such that $C' \subseteq C$, we must find two codewords 11 in the sequence C at first. Nevertheless, we know $11 \notin c_1||c_2||\cdots||c_t$ according to Theorem 1, which means that it is impossible to find a codeword sequence $C' = 11||c'_1||c'_2||\cdots||c'_k||11$ with $c'_i \in \{00, 01\}, i = 1, 2, \ldots, k$ such that $C' \subseteq c_1||c_2||\cdots||c_t$. In addition, the first bit of both the legal codewords 00 and 01 is 0, and therefore, we cannot find a new codeword 11 in $11||c_1||c_2||\cdots||c_t$ except the start codeword 11. Therefore, to find a sequence $C' = 11||c'_1||c'_2||\cdots||c'_k||11$ with $c'_i \in \{00, 01\}, i = 1, 2, \ldots, k$ such that $C' \subseteq C$, we must choose the first codeword 11 of the sequence C as the start codeword of the sequence C', but the end codeword 11 of the sequence C' cannot be also chosen from the last codeword 11 of the sequence C because the bit sequences C' and C are the same in the case, i.e., $C' = C$. By simple deducing, it is not difficult to find that there is only one codeword 11 in the sequence C except the first and the last, that is, when the codeword c_t is 01, the last bit 1 of c_t and the first bit 1 of the end codeword 11 in the sequence C can be taken out to combine a new codeword 11. Nevertheless, the sequence C' is $11||c_1||c_2||\cdots||c_{t-1}|01|1 = 11||c_1||c_2||\cdots||c_{t-1}|0||11$ in this case. It is evident that it does not satisfy the requirement $C' = 11||c'_1||c'_2||\cdots||c'_k||11$ with $c'_i \in \{00, 01\}, i = 1, 2, \ldots, k$ for $0 \notin \{00, 01\}$.

Therefore, it is impossible to find a sequence $C' = 11||c'_1||c'_2||\cdots||c'_k||11$ with $c'_i \in \{00, 01\}, i = 1, 2, \ldots, k$ such that $C' \subseteq C$ except $C' = C$. For example, let $C = 110000010111$, clearly, there is no codeword 11 in the middle of the bit sequence C, and therefore, it is impossible to find a sequence $C' = 11||c'_1||c'_2||\cdots||c'_k||11$ with $c'_i \in \{00, 01\}, i = 1, 2, \ldots, k$ such that $C' \subseteq 110000010111$ except $C' = 110000010111$. □

Theorem 3 *Suppose that* $C_j = c_1^j||c_2^j||\cdots||c_{n_j}^j$, $c_1^j = c_{n_j}^j = 11$, $c_i^j \in \{00, 01\}, i = 2, 3, \ldots, n_j - 1$, $j = 1, 2, \ldots, l$, *it is impossible to find a sequence* $C' = c'_1||c'_2||\cdots||c'_{n'}$ *with* $c'_1 = c'_{n'} = 11$ *and* $c'_i \in \{00, 01\}, i = 2, 3, \ldots, n' - 1$ *such that* $C' \subseteq C_1||C_2||\cdots||C_l$ *except* $C' = C_j$, $j = 1, 2, \ldots, l$.

Proof When $l = 1$, Theorem 3 reduces to Theorem 2, and hence, the conclusion is obviously right.

When $l = 2$,

$$C_1||C_2 = c_1^1||c_2^1||\cdots||c_{n_1-1}^1||c_{n_1}^1||c_1^2||c_2^2||\cdots||c_{n_2-1}^2||c_{n_2}^2. \tag{4}$$

To find a sequence $C' = c'_1||c'_2||\cdots||c'_{n'}$ with $c'_1 = c'_{n'} = 11$ and $c'_i \in \{00, 01\}, i = 2, 3, \ldots, n' - 1$ such that $C' \subseteq C_1||C_2||\cdots||C_l$, it is necessary to find at least one

new codeword 11. By Theorem 2 and Formula (4), the new codeword 11 can be only chosen from $c^1_{n_1-1}||c^1_{n_1}||c^2_1$ or $c^2_{n_2-1}||c^2_{n_2}$.

(1) When $c^1_{n_1-1} = c^2_{n_2-1} = 00$, $c^1_{n_1-1}||c^1_{n_1}||c^2_1 = 00||11||11$ and $c^2_{n_2-1}||c^2_{n_2} = 00||11$, we can choose the new codeword 11 only from $c^1_{n_1}||c^2_1 = 11||11$. Nevertheless, if we choose $c^1_{n_1}$ as the end codeword of the sequence C', we must choose c^1_1 as the start codeword, in the case $C' = C_1$; if we choose $c^1_{n_1}$ as the start codeword of the sequence C', we must choose $c^2_{n_2}$ as the end codeword, i.e., $C' = c^1_{n_1}||c^2_1||c^2_2||\cdots||c^2_{n_2-1}||c^2_{n_2}$, in the case $c^2_1 = 11 \notin \{00, 01\}$; if we choose the last bit of $c^1_{n_1}$ and the first bit of c^2_1 as the end codeword of the sequence C', we must choose c^1_1 as the start codeword, i.e., $C' = 11||c^{'}_2||\cdots||c^{'}_{n'-1}||11 = c^1_1||c^1_2||\cdots||c^1_{n_1-1}||11||1$, in the case there must exist at least one codeword c'_i ($c'_i \in C'$) such that $c'_i \notin \{00, 01\}$; if we choose the last bit of $c^1_{n_1}$ and the first bit of c^2_1 as the start codeword of the sequence C', we must choose $c^2_{n_2}$ as the end codeword, i.e., $C' = 11||c^{'}_2||\cdots||c^{'}_{n'-1}||11 = 1||11||c^2_2||\cdots||c^2_{n_2-1}||11$, in the case there also must exist at least one codeword c'_i ($c'_i \in C'$) such that $c'_i \notin \{00, 01\}$; if we choose c^2_1 as the end codeword of the sequence C', we must choose c^1_1 as the start codeword, i.e., $C' = c^1_1||c^1_2||\cdots||c^1_{n_1-1}||c^1_{n_1}||c^2_1$, in the case $c^1_{n_1} = 11 \notin \{00, 01\}$; if we choose c^2_1 as the start codeword of the sequence C', we must choose $c^2_{n_2}$ as the end codeword, in the case $C' = C_2$. Therefore, when $c^1_{n_1-1} = c^2_{n_2-1} = 00$, it is impossible to find a sequence $C' = c^{'}_1||c^{'}_2||\cdots||c^{'}_{n'}$ with $c^{'}_1 = c^{'}_{n'} = 11$ and $c^{'}_i \in \{00, 01\}$, $i = 2, 3, \ldots, n'-1$ such that $C' \subseteq C_1||C_2$ except $C' = C_j$, $j = 1, 2$.

(2) When $c^1_{n_1-1} = 01$ and $c^2_{n_2-1} = 00$, $c^1_{n_1-1}||c^1_{n_1}||c^2_1 = 01||11||11$ and $c^2_{n_2-1}||c^2_{n_2} = 00||11$, we can choose the new codeword 11 only from $c^1_{n_1-1}||c^1_{n_1}||c^2_1 = 01||11||11$. Nevertheless, if we choose the last bit of $c^1_{n_1-1}$ and the first bit of $c^1_{n_1}$ as the end codeword of the sequence C', we must choose c^1_1 as the start codeword, i.e., $C' = 11||c^{'}_2||\cdots||c^{'}_{n'-1}||11 = c^1_1||c^1_2||\cdots||c^1_{n_1-2}||01||1$, in the case there must exist at least one codeword c'_i ($c'_i \in C'$) such that $c'_i \notin \{00, 01\}$; if we choose the last bit of $c^1_{n_1-1}$ and the first bit of $c^1_{n_1}$ as the start codeword of the sequence C', we can choose c^2_1 or $c^2_{n_2}$ as the end codeword, if we choose c^2_1, i.e., $C' = 1||c^1_1||c^1_2 = 11111$, it is obviously contradictory to the requirement $c^{'}_i \in \{00, 01\}$, but if we choose $c^2_{n_2}$, i.e., $C' = 11||c^{'}_2||\cdots||c^{'}_{n'-1}||11 = 1||11||c^2_1||c^2_2||\cdots||c^2_{n_2-1}||11$, in the case there also must exist at least one codeword c'_i ($c'_i \in C'$) such that $c'_i \notin \{00, 01\}$; if we choose $c^1_{n_1}$, c^2_1 or the last bit of $c^1_{n_1}$ and the first bit of c^2_1 as the start codeword or the end one, we will face the similar difficulty. Therefore, when $c^1_{n_1-1} = 01$ and $c^2_{n_2-1} = 00$, it is impossible to find a sequence $C' = c^{'}_1||c^{'}_2||\cdots||c^{'}_{n'}$ with $c^{'}_1 = c^{'}_{n'} = 11$ and $c^{'}_i \in \{00, 01\}$, $i = 2, 3, \ldots, n'-1$ such that $C' \subseteq C_1||C_2$ except $C' = C_j$, $j = 1, 2$.

(3) When $c^1_{n_1-1} = 00$ and $c^2_{n_2-1} = 01$, $c^1_{n_1-1}||c^1_{n_1}||c^2_1 = 00||11||11$ and $c^2_{n_2-1}||c^2_{n_2} = 01||11$, we can choose the new codeword 11 from $c^1_{n_1}||c^2_1 = 11||11$ or $c^2_{n_2-1}||c^2_{n_2} = 01||11$. Nevertheless, if we choose $c^1_{n_1}$ as the end codeword of the sequence C', we must choose c^1_1 as the start codeword, in the case $C' = C_1$; if we choose $c^1_{n_1}$ as the start codeword of the sequence C', we can choose the last bit of $c^2_{n_2-1}$ and the first bit of $c^2_{n_2}$ or $c^2_{n_2}$ as the end codeword, in both cases $c^2_1 = 11 \notin \{00, 01\}$; if we choose the last bit of $c^1_{n_1}$ and the first bit of c^2_1 as the end codeword, we also must choose c^1_1 as the start codeword, in the case $C' = 11||c^{'}_2||\cdots||c^{'}_{n'-1}||11 = 11||c^1_2||\cdots||c^1_{n_1-1}||11||1$, there must exist at least one codeword c'_i ($c'_i \in C'$) such that $c'_i \notin \{00, 01\}$; if we choose the last bit of $c^1_{n_1}$ and the first bit of c^2_1 as the start codeword, we can choose the last bit of $c^2_{n_2-1}$ and the first bit of $c^2_{n_2}$ or $c^2_{n_2}$ as the end codeword, i.e., $C' = 11||c^{'}_2||\cdots||c^{'}_{n'-1}||11 = 1||11||c^2_2||\cdots||c^2_{n_2-2}||01||1$ or $C' = 11||c^{'}_2||\cdots||c^{'}_{n'-1}||11 = 1||11||c^2_2||\cdots||c^2_{n_2-2}||01\ ||11$, in both cases there must exist at least one codeword c'_i ($c'_i \in C'$) such that $c'_i \notin \{00, 01\}$; if we choose c^2_1, the last bit of $c^2_{n_2-1}$ and the first bit of $c^2_{n_2}$ or $c^2_{n_2}$ as the new codeword, we will face the similar difficulty. Therefore, when $c^1_{n_1-1} = 00$ and $c^2_{n_2-1} = 01$, it is impossible to find a sequence $C' = c^{'}_1||c^{'}_2||\cdots||c^{'}_{n'}$ with $c^{'}_1 = c^{'}_{n'} = 11$ and $c^{'}_i \in \{00, 01\}$, $i = 2, 3, \ldots, n' - 1$ such that $C' \subseteq C_1||C_2$ except $C' = C_j$, $j = 1, 2$.

(4) When $c^1_{n_1-1} = 01$ and $c^2_{n_2-1} = 01$, $c^1_{n_1-1}||c^1_{n_1}||c^2_1 = 01||11||11$ and $c^2_{n_2-1}||c^2_{n_2} = 01||11$, we can choose the new codeword 11 from $c^1_{n_1-1}||c^1_{n_1}||c^2_1 = 01||11||11$ or $c^2_{n_2-1}||c^2_{n_2} = 01||11$. Nevertheless, no matter how to choose the sequence $C' = c^{'}_1||c^{'}_2||\cdots||c^{'}_{n'} = 11||c^{'}_2||\cdots||\ c^{'}_{n'-1}||11$, there must exist at least one codeword c'_i ($c'_i \in C'$) such that $c'_i \notin \{00, 01\}$. □

Therefore, when $l = 2$, the conclusion is also right.

Suppose that when $n = l - 1$, this conclusion is right. When $n = l$, let $C = C_1||C_2||\cdots||C_{l-1}$, by the former assumption, it is impossible to find a sequence $C' = c^{'}_1||c^{'}_2||\cdots||c^{'}_{n'}$ with $c^{'}_1 = c^{'}_{n'} = 11$ and $c^{'}_i \in \{00, 01\}$, $i = 2, 3, \ldots, n' - 1$ such that $C' \subseteq C$ except $C' = C_j$, $j = 1, 2, \ldots, l - 1$. By similar analysis as $l = 2$, we can conclude that it is impossible to find a sequence $C' = c^{'}_1||c^{'}_2||\cdots||c^{'}_{n'}$ with $c^{'}_1 = c^{'}_{n'} = 11$ and $c^{'}_i \in \{00, 01\}$, $i = 2, 3, \ldots, n' - 1$ such that $C' \subseteq C||C_l$ except $C' = C_j$, $j = 1, 2, \ldots, l$, which means this conclusion is also right when $n = l$.

All in all, it is impossible to find a sequence $C' = c^{'}_1||c^{'}_2||\cdots||c^{'}_{n'}$ with $c^{'}_1 = c^{'}_{n'} = 11$ and $c^{'}_i \in \{00, 01\}$, $i = 2, 3, \ldots, n' - 1$ such that $C' \subseteq C_1||C_2||\cdots||C_l$ except $C' = C_j$, $j = 1, 2, \ldots, l$.

From Theorems 1, 2 and 3, it can be concluded that Eve cannot forge a new valid message-signature pair $(M', Sig(M'), l')$ by recombining the obtained bit-signature pairs even if she has a lot of valid message-signature pairs, and therefore if the basic building blocks of signing a single bit is unconditionally secure against forging, the presented protocol is also unconditionally secure against forging. Furthermore, a TTP

Joe is introduced in this protocol, where he can deal with disputes and prevent the possible repudiation of a valid signature.

As a result, if the basic building blocks of signing a single bit are unconditionally secure against forging and denying, the presented protocol is also unconditionally secure against forging and denying even in the model of adaptive chosen-message attacks [16].

3 Conclusion

Based on the current basic building blocks of signing a single bit, we give a new proposal to define an entire protocol for signing a long message by the way of tagging both the start and the end of a signed message. In the proposal, a valid message-signature pair $(M, Sig(M), l)$ is generated by the signer Alice, and it can be verified and transferred among the legal recipients Bob, Charlie, David and so on. Although a TTP is introduced, he does not participate in this protocol except when a dispute appears. Furthermore, the security analysis shows it is unconditionally secure against forging and denying. Therefore, the defined QDS protocol has the basic properties of transferability, verifiability, unforgeability and non-repudiation.

In the previous work [15], it will consume $3n$ signing keys to sign a message M consisted of n bits, but the protocol only consumes $2n$ signing keys to sign M. Furthermore, the participants transfer the message M instead of the encoding sequence $\widehat{M}$ in this protocol, which makes it reduce 66.7% classical communication. Therefore, this protocol can reduce at least 33.33% classical and quantum resources compared with the previous work. We hope this work shed some light on the next development of QDS.

Acknowledgements We are grateful to the anonymous referees for helpful comment and detailed suggestion on revisions. This work was supported by the National High Technology Research and Development Program (863 Program) (Grant No. 2015AA011704), the Key Program of NSFC Union Foundation (Grant Nos. U1135002, U1405255), the National Natural Science Foundation of China (Grant Nos. 61202317, 61572246, 61602232, 61472048), the Plan for Scientific Innovation Talents of Henan Province (Grant No. 164100510003), the Program for Science and Technology Innovation Talents in Universities of Henan Province (Grant No. 13HASTIT042) and the Key Scientific Research Project in Universities of Henan Province (Grant Nos. 16A520021, 16A120007).

References

1. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**, 1484–1509 (1997)
2. Wei, H.R., Deng, F.G.: Scalable quantum computing based on stationary spin qubits in coupled quantum dots inside double-sided optical microcavities. Sci. Rep. **4**, 7551 (2014)
3. Gottesman, D., Chuang, I.: Quantum digital signatures. arXiv:quant-ph/0105032 (2001)
4. Jrn, M.Q.: Quantum pseudosignatures. J. Mod. Opt. **49**, 1269–1276 (2002)
5. Lu, X., Feng, D.G.: Quantum digital signature based on quantum one-way functions. ICACT **1**, 514–517 (2005)
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. Wallden, P., Dunjko, V., Kent, A., et al.: Quantum digital signatures with quantum key distribution components. Phys. Rev. A **91**, 042304 (2015)
9. 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)
10. Donaldson, R.J., Collins, R.J., Kleczkowska, K., et al.: Experimental demonstration of kilometer-range quantum digital signatures. Phys. Rev. A **93**, 012329 (2016)
11. Amiri, R., Wallden, P., Kent, A., et al.: Secure quantum signatures using insecure quantum channels. Phys. Rev. A **93**, 032325 (2016)
12. Yin, H.L., Fu, Y., Chen, Z.B.: Practical quantum digital signature. Phys. Rev. A **93**, 032316 (2016)
13. Arrazola, J.M., Wallden, P., Andersson, E.: Multiparty quantum signature schemes. Quantum Inf. Comput. **6**, 0435 (2016)
14. Swanson, C.M., Stinson, D.R.: Unconditionally secure signature schemes revisited. Inf. Theor. Sec. **6673**, 100 (2011)
15. Wang, T.Y., Cai, X.Q., Ren, Y.L., et al.: Security of quantum digital signatures for classical messages. Sci. Rep. **5**, 9231 (2015)
16. Gao, F., Qin, S.J., Guo, F.Z., et al.: Cryptanalysis of the arbitrated quantum signature protocols. Phys. Rev. A **84**, 022344 (2011)