Quantum Information Processing (2018) 17:275
https://doi.org/10.1007/s11128-018-2047-y

An efficient quantum digital signature for classical messages

Ming-Qiang Wang[1] · Xue Wang[1] · Tao Zhan[1]

Received: 9 November 2017 / Accepted: 30 August 2018 / Published online: 6 September 2018

Abstract
Quantum digital signature offers an information theoretically secure way to guarantee the identity of the sender and the integrity of classical messages between one sender and many recipients. The existing unconditionally secure protocols only deal with the problem of sending single-bit messages. In this paper, we modify the model of quantum digital signature protocol and construct an unconditionally secure quantum digital signature protocol which can sign multi-bit messages at one time. Our protocol is against existing quantum attacks. Compared with the previous protocols, our protocol requires less quantum memory and becomes much more efficient. Our construction makes it possible to have a quantum signature in actual application.

Keywords Quantum digital signature · Quantum commitment · Photodetection event

1 Introduction

Quantum digital signature (QDS) offers a secure means to send classical messages, and the protocol cannot be forged or repudiated. In contrast to classical digital signature [1,2], the security of QDS depends on quantum mechanics, so QDS is secure against quantum attacks.

Formally, the protocol of QDS has two stages: the distribution stage and the messaging stage.

– In the distribution stage, the sender needs to generate all signatures for any possible message and sends them to all recipients. The recipients perform some types of

The author is supported by MMJJ20180210, NSFC: 61832012, NSFC Grant 61672019 and The Fundamental Research Funds of Shandong University Grant 2016JC029.

✉ Ming-Qiang Wang
wangmingqiang@sdu.edu.cn

[1] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, School of Mathematics, Shandong University, Jinan, China

nondemolition comparison [3] or symmetrization [4,5] of their states and store the outcomes.
– In the messaging stage, the sender signs a message by sending the private key of this message to all recipients, and recipients need to confirm that it is compatible with their stored information.

Intuitively, in the distribution stage, the sender makes a one-to-one correspondence between messages and signatures; then, he sends all signatures to recipients. In the messaging stage, the sender just sends the private key which generates the corresponding signature to recipients. In general, the distribution stage and the messaging stage are independent. The distribution stage restricts the length of the signed message, because the required quantum memory increases exponentially as the length of the signed message increases. To my knowledge, all presented QDS protocols only deal with the problem of signing single-bit classical messages, while signing a multi-bit message, one needs to iterate the single-bit signing procedure, which is rather impractical in reality.

1.1 Related work

There are two categories of quantum signature (QS) according to the type of the signed messages, i.e. QS for quantum messages and QS for classical messages.

For quantum messages, in 2002, based on the Greenberger–Horne–Zeilinger (GHZ) triplet states [6] and quantum one-time pads [7], Zeng et al. [8] proposed an arbitrated quantum signature (AQS) protocol, and this protocol has many merits such as it can sign both known and unknown quantum states. In 2009, Li et al. [9] presented an AQS protocol using two-particle entangled Bell states instead of GHZ states. This protocol can preserve the merits in [8] while providing a higher efficiency in transmission and reducing the complexity of implementation. In 2010, Zou et al. [10] showed that the above AQS protocols can be repudiated by the receiver. To conquer this shortcoming, they constructed an AQS protocol using a public board. In particular, this protocol does not utilize entangled states and preserves the merits in the existing AQS protocols. In 2012, Luo et al. [11] suggested a QDS with weak arbitrator, and this weak arbitrator is required only when there is a dispute between the signer and the verifier. However, in 2014, Zou et al. [12] showed that the above suggestion can counterfeit a valued signature by employing several known attacks.

For classical messages, in 2001, the QDS protocol presented by Gottesman and Chuang [3] is based on a quantum analogue of a one-way function, and this protocol requires a general SWAP test to perform nondestructive quantum state comparison on the quantum signatures and needs long-term quantum memory which is currently impractical in experiment. In 2006, Andersson et al. [13] presented an easily reliable method for quantum states comparison, and this method has a higher success probability and is experimentally feasible as the only required components are beam splitters and photon detectors. Then Clarke et al. [4] provided a novel QDS protocol by using Andersson et al.'s method to perform quantum states comparison instead of the SWAP test, and this protocol is based on the interference of phase-encoded coherent states of light, but it also needs a long-term quantum memory. In 2014, Dunjko et al. [14] gave

a QDS protocol without the requirement of quantum memory in which the quantum signatures are converted to classical information through quantum measurements during the distribution stage, and then, the procedures of authentication and verification only process classical data during the messaging stage. In 2015, Amiri et al. [15] constructed a new QDS protocol without secure quantum channels. In [15], the sender sends different signatures to recipients instead of the same signature, which improves efficiency, and the noise threshold is less strict.

In this paper, we focus on the QS for classical message. The above QDS protocols only deal with the problem of signing single-bit messages, while signing a multi-bit message, one needs to iterate the single-bit signing procedure. In 2015, Wang et al. [5] found two kinds of truncation attacks and proved that iterating the single-bit signing procedure cannot resist the truncation attacks. In order to resist these attacks, Wang et al. designed a special encode way to tag the start and the end of the signed message and claimed that this method can guarantee the integrity of the signed message.

1.2 Our results and techniques

Our main result in this paper is that we construct an unconditionally secure QDS protocol which can sign multi-bit classical messages efficiently at one time. Our QDS protocol is secure against forging and repudiation, and our protocol is also secure against existing quantum attacks.

The existing QDS protocols only deal with the problem of signing single-bit messages, while signing a multi-bit message, one needs to iterate the single-bit signing procedure. Wang et al. [5] presented two algorithms to attack this iteration and designed a QDS protocol which can sign multi-bit message at one time. Compared with the protocol [5], our protocol can resist the two forgery attacks presented in [5]. Moreover, our protocol need less quantum memory and is more efficient.

In the key distribution stage, the sender sends all signatures for each possible bit message to recipients; each signature represents specific location information and bit information. Thus, the quantum memory we require is polynomial, not exponential. To ensure the integrity of signed message, our technique is that the sender commits the signed message and sends it to the recipient.

Our QDS protocol is secure against forging and repudiation. Our QDS protocol is secure against forging; the key observation is that if $m' \not\equiv m \bmod p$, where p is a prime, the following two equations

$$r' \equiv r \bmod p, \quad m'r' \equiv mr \bmod p \tag{1}$$

cannot hold concurrently. That is to say, if we encode the signed message to the phase of the quantum commitment, there is a great difference between the phases of the true and forged quantum commitment. Thus, the recipients can detect this discrepancy by counting the number of the photodetection events on the recipient's signal null-port arm. Our QDS protocol is secure against repudiation, the key is to use the multi-port, and each recipient saves the symmetric output states in their quantum memory. That is to say, the cost matrix $\mathbf{C}$ (Appendix A) that describes the probability of registering

a photodection event on recipients' signal null-port arm is symmetric. So the sender cannot make recipients disagree on the validity of any signed message. Also, the last recipient can be a judge, and he can prevent the sender from denying that she has sent the signed message.

2 Preliminaries

In this section, we introduce some necessary preliminaries to construct an unconditionally secure QDS protocol for classical messages.

In this paper, we use $[p]$ to denote the set $\{1, 2, \ldots, p\}$ and we use $\|$ to denote the concatenation of bits or bit strings. A coherent state $|\beta\rangle$ is a quantum state, which closely resembles a classical electromagnetic wave, and β is a complex number. The multi-port is made of four 50:50 beam splitters. The input states to the 50:50 beam splitter are $|\alpha\rangle$ and $|\beta\rangle$, and the output states are $|(\alpha - \beta)/\sqrt{2}\rangle$ and $|(\alpha + \beta)/\sqrt{2}\rangle$. This simple operation forms the basis of the multi-port signature comparison system. The output states of the multi-port are symmetric with respect to each recipient.

The following simple lemmas are useful for the proof of our unconditionally secure QDS protocol.

Lemma 1 *Let p be a prime and $(a, p) = 1$, for any $b \in Z$, and the following equation*

$$ax \equiv b \bmod p \tag{2}$$

has only one solution modulo p.

Lemma 2 [16] *Let $X_1, \ldots, X_L$ be independent random variables, and each attains values 0 or 1. Let $\bar{X} = 1/L \sum X_i$ be the empirical mean of the variables, and let $E(\bar{X})$ be the expectancy of the empirical mean. Then we have*

$$P(\bar{X} - E(\bar{X}) \geq t) \leq \exp(-2t^2 L), \tag{3}$$

$$P(|\bar{X} - E(\bar{X})| \geq t) \leq 2\exp(-2t^2 L). \tag{4}$$

The above inequalities are called the Hoeffding's inequalities. It is noted that the inequalities also hold when the $\{X_1, X_2, \ldots, X_L\}$ has been obtained using sampling without replacement; in this case, the random variables are not independent anymore.

2.1 Quantum commitment scheme

Informally speaking, commitment scheme is like a sender putting a message in a locked box and giving this box to a recipient. The message in the box is hidden from the recipient who cannot open the lock himself. Since the recipient has the box, the message inside cannot be changed, merely revealed if the sender chooses to give them the key at some later time.

The scheme of quantum commitment has two stages: the commit stage and the reveal stage.

– In the commit stage, the sender transmits information related to a message in such a way that the recipient learns nothing about the message (hiding property); at the same time, the sender cannot change his mind later about this message (binding property).
– In the reveal stage, the sender reveals the message and proves that this is indeed the message that he had in mind earlier.

Let us recall the basics of quantum commitment scheme. The following is taken verbatim from [17].

A commitment scheme consists of algorithms *Com* and *Verify*. $(\mathrm{C}, u) \leftarrow Com(1^{\lambda}, m)$ returns a commitment C and the opening information u for the message m. C alone is supposed not to reveal anything about m (hiding property). To open the commitment, the sender sends (m, u) to the recipient who checks whether $Verify(1^{\lambda}, \mathrm{C}, m, u) = 1$. *Com* has classical input and a well-defined message space $\mathcal{M}$ that depends on the security parameter λ (e.g. $\{0, 1\}^{\lambda}$).

Definition 1 Let (*Com*, *Verify*) be a commitment scheme, and we define

– *Completeness* For any $m \in \mathcal{M}$, the following probability declines exponentially in terms of the length of the quantum commitment

$$\Pr[Verify(1^{\lambda}, \mathrm{C}, m, u) \neq 1 : (\mathrm{C}, u) \leftarrow Com(1^{\lambda}, m)].$$

– *Unconditional binding* For any computationally unlimited adversary $\mathcal{A}$ and $m \in \mathcal{M}$, the following probability declines exponentially in terms of the length of the quantum commitment

$$\Pr[Verify(1^{\lambda}, \mathrm{C}, m, u) = 1 \wedge Verify(1^{\lambda}, \mathrm{C}, m', u') = 1 \wedge m \neq m' : (\mathrm{C}, m, u, m', u') \leftarrow \mathcal{A}(\lambda)].$$

– *Unconditional hiding* For any computationally unlimited adversary $\mathcal{A}$ and $m \in \mathcal{M}$, the following probability declines exponentially in terms of the length of the quantum commitment

$$|\Pr[m \leftarrow \mathcal{A}(1^{\lambda}, \mathrm{C}) : (\mathrm{C}, u) \leftarrow Com(1^{\lambda}, m)] - \frac{1}{|\mathcal{M}|}|.$$

Construction We introduce a quantum commitment scheme [18] and describe it as follows. For simplicity, we outline the case with one sender Alice and one recipient Bob.

1. Let p be a prime to be chosen later. To make a commitment of message $m \leq p$ to Bob, Alice chooses a sequence of $\mathbf{r} = (r_1, r_2, \ldots, r_L)$ from $[p]^L$ randomly and generates a sequence of coherent states

$$\rho_k = |e^{\frac{2r_k\pi i}{p}}\alpha\rangle\langle e^{\frac{2r_k\pi i}{p}}\alpha|, \ k = 1, \ldots, L, \tag{5}$$

$$\rho_k^m = |e^{\frac{2mr_k\pi i}{p}}\alpha\rangle\langle e^{\frac{2mr_k\pi i}{p}}\alpha|, \ k = 1, \ldots, L, \tag{6}$$

where α is a real positive amplitude and L is a polynomial of security parameter λ. Let

$$\rho_{\mathbf{r}} =: (\rho_1, \ldots, \rho_L),\ \ \rho_{m,\mathbf{r}} =: (\rho_1^m, \ldots, \rho_L^m). \tag{4}$$

The vector $\mathbf{r}$ is called the opening information and $\text{QuantCom}_m =: (\rho_{\mathbf{r}}, \rho_{m,\mathbf{r}})$ is called the commitment of message m. QuantCom_m is in $2L$ independent quantum registers, and each register does not interfere with each other. Then Alice sends QuantCom_m to Bob over an authenticated channel.

2. To open the commitment, Alice sends $(m, \mathbf{r})$ to Bob over an insecure channel. Bob generates coherent states $(\rho_{\mathbf{r}}, \rho_{m,\mathbf{r}})$ of amplitude α with the relative phase defined by $(m, \mathbf{r})$ and interferes them individually with the states QuantCom_m. He counts the number of photodetection events on his signal null-port arm and accepts this message m if the number of photodetection events is below $2s_v L$; otherwise, he rejects it. The parameter s_v is called the verification threshold which will be chosen later.

Intuitively, our commitment scheme is unconditionally secure, i.e. its security is independent of the ability of the adversary.

Theorem 1 *The above two-party quantum commitment scheme is unconditional hiding and binding.*

Proof This theorem is proved in [18], so we omit it. □

3 Quantum digital signature protocol

In this section, we modify the model of QDS protocol and give a new efficient QDS protocol. We outline the case with one sender Alice and two recipients Bob and Charlie.

3.1 Definition

The protocol of QDS has three stages: the key distribution stage, the signing stage and the verification stage.

- In the key distribution stage, Alice generates all signatures for each possible bit message and sends them to two recipients. Then recipients perform symmetrization of their states and store the outcomes.
- In the signing stage, Alice sends the quantum commitment of the signed message m to Charlie; then, for each bit of the signed message $m = m_1 \parallel m_2 \parallel \cdots \parallel m_n$, she sends the corresponding private key pair $(j, \text{Privkey}_j^{m_j})$ to two recipients.
- In the verification stage, Charlie verifies the commitment QuantCom_m according to the pair $(m, \mathbf{r})$. If fails, the protocol has to be aborted. Otherwise, two recipients continue to verify the signature.

The QDS protocol is required to resist two kinds of malicious activities: forging and repudiation. The protocol being secure against forging means that any recipient will

reject any message that is not sent by the sender. The protocol being secure against repudiation means that the sender cannot make recipients disagree on the validity of any signed message. Formally we have the following definitions of the secure QDS protocol:

- We say that a protocol of QDS is robust if the probability of the signed message being rejected is declining exponentially in terms of the length of the quantum signature when all parties are honest.
- We say that a protocol of QDS is secure against forging if the probability in the following case is declining exponentially in terms of the length of the quantum signature; the case is that any adversary generates a private key of a message that will pass verification of other recipients without receiving it from the sender.
- We say that a protocol of QDS is secure against repudiation if the probability in the following case is declining exponentially in terms of the length of the quantum signature; the case is that a signature of the signed message fails verification with one recipient once it has already passed authentication with the other.

3.2 Construction

In this subsection, we describe our QDS protocol.

1. *The key distribution stage*

   (a) Let n be the length of the message to be signed. For each jth bit, $j = 1, 2, \ldots, n$, Alice chooses two sequences of $\text{PrivKey}_j^0 = (r_{j,1}^0, r_{j,2}^0, \ldots, r_{j,L}^0)$ and $\text{PrivKey}_j^1 = (r_{j,1}^1, r_{j,2}^1, \ldots, r_{j,L}^1)$ from $[p]^L$ randomly; then, she generates coherent states

   $$\rho_{j,k}^0 =: |e^{\frac{2r_{j,k}^0\pi i}{p}}\alpha\rangle\langle e^{\frac{2r_{j,k}^0\pi i}{p}}\alpha|,\ k = 1, \ldots, L, \tag{7}$$

   $$\rho_{j,k}^1 =: |e^{\frac{2r_{j,k}^1\pi i}{p}}\alpha\rangle\langle e^{\frac{2r_{j,k}^1\pi i}{p}}\alpha|,\ k = 1, \ldots, L, \tag{8}$$

   where α is a real positive amplitude, L is polynomial of the security parameter λ, and p is a prime depending on the properties of practical implementation. Let

   $$\text{QuantSig}_j^0 =: (\rho_{j,1}^0, \ldots, \rho_{j,L}^0),\ \text{QuantSig}_j^1 =: (\rho_{j,1}^1, \ldots, \rho_{j,L}^1). \tag{9}$$

   The vector PrivKey_j^μ with $\mu = 0, 1$ is called jth private key of message μ, and the sequence of such coherent states QuantSig_j^ν with $\nu = 0, 1$ is called jth quantum signature of message ν.

   (b) Alice generates two copies of these sequences of coherent states QuantSig_j^0 and QuantSig_j^1. For $\mu = 0, 1$ and $j = 1, 2, \ldots, n$, Alice sends one copy of the quantum signature pair $(j, \mu, \text{QuantSig}_j^\mu)$ to Bob and the other to Charlie by an authenticated channel. Then Bob and Charlie send each sequence of QuantSig_j^0

and QuantSig_j^1 through a multi-port, respectively, saving the output states in quantum memory and noting which quantum signature corresponds to message 0 of jth bit and which to 1 of jth bit.

2. *The signing stage*

(a) To sign a message $m = m_1 \parallel m_2 \parallel \cdots \parallel m_n \in [p]$, Alice makes commitment of this message m to Charlie. She chooses a sequence of $\mathbf{r} = (r_1, r_2, \ldots, r_L)$ from $[p]^L$ randomly and generates a sequence of coherent states

$$\rho_k = |e^{\frac{2r_k\pi i}{p}}\alpha\rangle\langle e^{\frac{2r_k\pi i}{p}}\alpha|,\ k = 1, \ldots, L, \tag{10}$$

$$\rho_k^m = |e^{\frac{2mr_k\pi i}{p}}\alpha\rangle\langle e^{\frac{2mr_k\pi i}{p}}\alpha|,\ k = 1, \ldots, L. \tag{11}$$

Let

$$\rho_{\mathbf{r}} =: (\rho_1, \ldots, \rho_L),\ \rho_{m,\mathbf{r}} =: (\rho_1^m, \ldots, \rho_L^m), \tag{12}$$

where the vector $\mathbf{r}$ is called the opening information and $\text{QuantCom}_m = (\rho_{\mathbf{r}}, \rho_{m,\mathbf{r}})$ is called the quantum commitment of message m. Then Alice sends QuantCom_m to Charlie by an authenticated channel and sends the pair $(m, \mathbf{r})$ to Bob over an insecure channel.

(b) For the message $m = m_1 \parallel m_2 \parallel \cdots \parallel m_n \in [p]$, Alice sends the corresponding private key pairs $(j, \text{PrivKey}_j^{m_j})$, $j = 1, 2, \ldots n$, to Bob over an insecure channel.

3. *The verification stage*

(a) To authenticate this signature, Bob generates coherent states of amplitude α with each relative phase defined by the declared $\text{PrivKey}_j^{m_j}$, $j = 1, 2, \ldots n$ and interferes them individually with the states $\text{QuantSig}_j^{m_j}$ he has in his quantum memory one by one. For each state $\text{QuantSig}_j^{m_j}$, he counts the number of photodetection events on his signal null-port arm and authenticates this state if the number of photodetection events is below $s_a L$. The parameter s_a is the authentication threshold. If there is a state which cannot be authenticated, Bob rejects the message m.

(b) Bob sends $(m, \mathbf{r})$ to Charlie; then, Charlie generates coherent states of amplitude α with the relative phase defined by $(m, \mathbf{r})$ and interferes them individually with the states QuantCom_m. He counts the number of photodetection events on his signal null-port arm; if the number of photodetection events is not below $2s_v L$, where s_v is called the verification threshold, the protocol is aborted.

(c) To prove to Charlie that he received the message m from Alice, Bob sends the corresponding private key pairs $(j, \text{PrivKey}_j^{m_j})$, $j = 1, 2, \ldots n$ to Charlie. Charlie then performs an analogous procedure as Bob and he verifies the signature of bit message m_j if the number of photodetection events is below $s_v L$, with $0 < s_a < s_v < 1$. If there is a state which cannot be verified, Charlie rejects this message m.

If any of the thresholds are breached, the protocol has to be aborted.

Remark Charlie's responsibility is the judge. When Alice and Bob are controversial, the step (c) in the verification stage can prevent Alice from denying that she has sent the signed message to Bob.

Lemma 3 [4] *For any bit message $m_j,\ j = 1, 2, \ldots n$, the probability of Alice repudiating successfully is*

$$\Pr(\text{repudiation}\, m_j) \leq 2^{-(s_v - s_a)L}. \tag{13}$$

Theorem 2 *Our quantum digital signature protocol is secure.*

Proof We divide our proof into three parts: robust, security against forging and security against repudiation.

For any integer $0 \leq a, b \leq p-1$, let $c_{a,b}$ denote the probability that causes a photodetection event on the recipient's signal null-port arm when the phase angle of the state he has in his quantum memory is $\frac{2a\pi}{p}$ and what the sender declared is $\frac{2b\pi}{p}$. Let $\bar{X}_1 = \frac{1}{L}X$, $\bar{X}_2 = \frac{1}{2L}X$. X denotes the total number of photodetection events on recipient's signal null-port arm and $E(\bar{X}_i)$ denotes the expectancy of the variable $\bar{X}_i$, where $i = 1, 2$. Also, we let

$$c = \max_{a\in[p]}\{c_{a,a}\},\ \widehat{c}_{p_1,p_2} = p_1 \min_{a\in[p]}\{c_{a,a}\} + p_2 \min_{a,b\in[p],a\neq b}\{c_{a,b}\}. \tag{14}$$

And we let $g = \widehat{c}_{\frac{1}{2},\frac{1}{2}} - c$, by the experiment in Appendix A; we have that $g > 0$. We set $s_a = c + \frac{g}{3}$, $s_v = \widehat{c}_{\frac{1}{2},\frac{1}{2}} - \frac{g}{3}$. □

Robust For any bit message $m_j,\ j = 1, 2, \ldots n$, if the three parties in this protocol are honest, we have

$$E(\bar{X}_1) \leq \max_{a\in[p]}\{c_{a,a}\} = c. \tag{15}$$

Then the probability that the signature of bit message m_j cannot be authenticated is

$$\Pr(\text{Bob rejects}\, m_j) = \Pr(\bar{X}_1 > s_a) \leq \Pr(\bar{X}_1 - E(\bar{X}_1) > \frac{g}{3}) \leq \exp(-\frac{2}{9}g^2 L). \tag{16}$$

Hence, the probability that the signature of message $m = m_1 \parallel m_2 \parallel \cdots \parallel m_n$ cannot be authenticated is

$$\begin{aligned} \Pr(\text{Bob rejects}\, m) &= 1 - \Pr(\text{Bob accepts}\, m) \\ &= 1 - [\Pr(\text{Bob accepts}\, m_j)]^n \\ &= 1 - [1 - \Pr(\text{Bob rejects}\, m_j)]^n \\ &\leq 1 - [1 - \exp(-\tfrac{2}{9}g^2 L)]^n \leq n\exp(-\tfrac{2}{9}g^2 L). \end{aligned} \tag{17}$$

Similarly, we have

$$\Pr(\text{Charlie rejects } m) \leq 1 - \left[1 - \exp(-\frac{2}{9}g^2 L)\right]^n \leq n \exp(-\frac{2}{9}g^2 L). \quad (18)$$

Security against forging First we assume that only Bob is dishonest. Because the quantum commitment scheme in Sect. 2 is unconditional binding, once Bob sends forged message $m' \neq m$ to Charlie, no matter how Bob chooses $\mathbf{r}' = (r'_1, \ldots, r'_L)$; the probability that this protocol is aborted declines exponentially in terms of the length of the quantum signature.

By Lemma 1, if $m' \not\equiv m \bmod p$, the following two equations

$$r' \equiv r \bmod p, \ m'r' \equiv mr \bmod p \quad (19)$$

cannot hold concurrently. Hence, if $m' \not\equiv m \bmod p$, no matter how Bob chooses the random sequence vector $\mathbf{r}' = (r'_1, \ldots, r'_L)$; there are at least L different entries modulo p between the following two vectors

$$(r'_1, \ldots, r'_L, m'r'_1, \ldots, m'r'_L), \ (r_1, \ldots, r_L, mr_1, \ldots, mr_L).$$

In other words, the number of the following $2L$ equations that do not hold

$$r'_i \equiv r_i \bmod p, \ \ m'r'_i \equiv mr_i \bmod p, \ \ 1 \leq i \leq L, \quad (20)$$

is at least L.

By the above discussions, we have

$$\begin{aligned} E(\bar{X}_2) &= \tfrac{1}{2L} E(X_2) \\ &\geq \tfrac{1}{2L}(L \min_{a\in[p]}\{c_{a,a}\} + L \min_{\substack{a,b\in[p]\\ a\neq b}}\{c_{a,b}\}) \\ &= \tfrac{1}{2}\min_{a\in[p]}\{c_{a,a}\} + \tfrac{1}{2}\min_{\substack{a,b\in[p]\\ a\neq b}}\{c_{a,b}\} \\ &= \widehat{c}_{\frac{1}{2},\frac{1}{2}}. \end{aligned} \quad (21)$$

Hence, we have

$$\Pr[\text{Charlie accepts } m'] = \Pr[\bar{X}_2 \leq s_v]. \quad (22)$$

By Lemma 2, we get

$$\begin{aligned} \Pr\left[\bar{X}_2 \leq s_v\right] &\leq \Pr\left[\bar{X}_2 - E(\bar{X}_2) \leq -\frac{g}{3}\right] \\ &\leq \Pr\left[|\bar{X}_2 - E(\bar{X}_2)| \geq \frac{g}{3}\right] \leq 2\exp(-\frac{4}{9}g^2 L). \end{aligned} \quad (23)$$

This probability declines exponentially in terms of the length of the quantum signature.
Security against repudiation First, we assume that the multi-port is ideal and Alice is only dishonest. In this attack, Alice wants to forward a message–signature pair that will pass Bob's authentication, but will be rejected by Charlie. From Lemma 3, we known that, for any bit message m_j, $j = 1, 2, \ldots n$, the probability of Alice repudiating successfully is

$$\Pr(\text{repudiation } m_j) \leq 2^{-(s_v - s_a)L}. \tag{24}$$

In the same way, for the signed message $m = m_1 \parallel m_2 \parallel \cdots \parallel m_n$, we can bound the probability of Alice repudiating successfully as

$$\Pr(\text{repudiation } m) \leq 1 - [1 - 2^{-(s_v - s_a)L}]^n \leq n2^{-(s_v - s_a)L}. \tag{25}$$

4 Compared with the previous work

In this section, we compare our protocol with the main existing QDS protocols. Compared with the previous works, our advantages can be showed in three aspects: the length of the signed message, quantum memory and efficiency. Specifically, our protocol can sign multi-bit messages at one time, and our protocol needs less quantum memory and is more efficient.

Proposition 1 *Our unconditionally secure QDS protocol can sign multi-bit messages at one time. If the length of the signed message is n, we need to generate* $2n + 1$ *coherent states and iterate n times single-bit signing procedure.*

Compared with our protocol, the existing unconditionally secure QDS protocols, i.e. [4,14,15], only can sign single-bit messages at one time except the protocol [5]. If the length of the signed message is n, the protocol [5] needs to generate $6n + 12$ coherent states and iterate $3n + 6$ times single-bit signing procedure. And there is time delay in verification stage of the protocol [5]. Suppose that Bob is dishonest, he sends a forged message to Charlie. In the protocol [5], Charlie needs to verify each signature of the signed message bits; only when he find a state which cannot be verified, he can reject this forged message, while in our protocol, Charlie can reject this forged message only by verifying a quantum commitment. The reason for this difference is that we encode the signed message to the phase of the quantum commitment, and we take the signed message as a whole. Any alteration of the signed message will be detected by verifying this quantum commitment, instead of verifying validity of each signed message bit.

In order to be more image and specific, we build a table with columns and rows to compare and analyse as follows.

	Quantum memory	Iteration	Length	Time delay
[4,14,15]	1	1	Single-bit	No
[5]	$6n+12$	$3n+6$	Multi-bit	Yes
Our protocol	$2n+1$	n	Multi-bit	No

Appendix A

Bob's optimal strategy is to minimize the probability of causing a photodetection event, with the cost matrix $\mathbf{C}$ with elements $c_{\phi,\theta}$. In the cost matrix $\mathbf{C}$, the diagonal elements represent the cases when recipient uses the same phase as sender, and the off-diagonal elements represent the cases when recipient uses the phase different from sender. In the specific experimental operation, to make our protocol to be secure against forging, a practical requirement is that the probabilities of registering a photodetection event on Charlie's signal null-port arm are greatly different between the above two cases. If so, Charlie can register distinctly more photodetection events than threshold value when Bob (or other external party) attempts to forge a message. That is to say, Charlie is capable of detecting a discrepancy between the true and forged messages. To achieve this requirement, the choice of the number of possible phase encodings p cannot be large. Clarke et al. [4] presents us a practical experimental data, they use 8 different phase states, and the average photon number per pulse is $|\alpha^2| = 0.16$. In this experimental setup, the cost matrix is given by

$$\mathbf{C} = \begin{pmatrix} 3.89 & 4.40 & 5.24 & 5.95 & 6.35 & 6.00 & 5.29 & 4.39 \\ 4.56 & 3.88 & 4.43 & 5.29 & 6.04 & 6.39 & 6.02 & 5.20 \\ 5.28 & 4.60 & 3.89 & 4.42 & 5.29 & 6.02 & 6.37 & 5.95 \\ 5.68 & 5.22 & 4.58 & 3.90 & 4.40 & 5.24 & 5.91 & 6.30 \\ 6.36 & 5.68 & 5.27 & 4.59 & 3.89 & 4.43 & 5.24 & 6.01 \\ 5.62 & 6.36 & 5.66 & 5.23 & 4.57 & 3.89 & 4.41 & 5.30 \\ 5.26 & 5.68 & 6.40 & 5.70 & 5.22 & 4.60 & 3.88 & 4.40 \\ 4.61 & 5.24 & 5.65 & 6.36 & 5.68 & 5.22 & 4.56 & 3.88 \end{pmatrix} \times 10^{-3}. \quad (26)$$

Appendix B

Lemma 4 *For any bit message m_j, $j = 1, 2, \ldots, n$, the probability of Alice repudiating successfully is*

$$Pr(\text{repudiation}\, m_j) \leq 2^{-(s_v - s_a)L}. \quad (1)$$

Proof For this purpose, Alice needs to forward different quantum signatures to Bob and Charlie, or more generally, the most general state Alice prepares is

$\pi_{A,B_1,C_1,B_2,C_2,\ldots,B_L,C_L}$, which is a general $2L+1$-partite state. Subsystem A Alice keeps and sends partitions $B_1,\ldots,B_L$ to Bob and $C_1,\ldots,C_L$ to Charlie. If Alice is honest, there is no subsystem A, B_i and C_i are identical coherent states with a complex phase known to Alice alone, as specified by the protocol.

There are two cases of this attack: security against individual repudiation and security against coherent repudiation.

At first, we show that our protocol is secure against individual repudiation. We assume that the system A is disentangled from the rest of Alice's state, and the subsystems (B_kC_k) and (B_lC_l) are not entangled with each other for $k \neq l$. However, we allow the partitions B_k and C_k to be mutually entangled. This type of an attack we refer to as an individual attack. According to the protocol specifications, Bob and Charlie will individually run the pairs of states in the systems through the multi-port and commit to quantum memory whatever comes out on their signal outputs of the multi-port. For the purpose of showing security against repudiation, we can assume that they ignore the measurement outcomes on the multi-port null-ports.

For the kth signature element, the joint system of Bob and Charlie which they store into memory is state $\pi^{\text{out}}_{B_kC_k}$, which is symmetric under permutations of Bob's and Charlie's subsystems as we now show. Let

$$\pi^{\text{in}}_{B_kC_k} = \int_{C^2} P(\alpha,\beta)|\alpha><\alpha| \otimes |\beta><\beta| d^2\alpha d^2\beta \tag{28}$$

be any general two mode state given in the P representation. Then the stored output state (when the null-port subsystems have been traced out) is

$$\begin{aligned}\pi^{\text{out}}_{B_kC_k} = \int_{C^2} & P(\alpha,\beta)|(\alpha+\beta)/\sqrt{2}><(\alpha+\beta)/\sqrt{2}| \\ & \otimes|(\alpha+\beta)/\sqrt{2}><(\alpha+\beta)/\sqrt{2}| d^2\alpha d^2\beta,\end{aligned} \tag{29}$$

which is symmetric in the sense given above. From [4], we know that the signature states Bob and Charlie end up with are symmetric under the swap of their systems and the probability matrix describing a priori occurrence of photodection events on Bob's and Charlie's signal null-port arm is symmetric. So for every possible state $\pi^{\text{out}}_{B_kC_k}$, the probability of getting event outcomes (0, 1) (only Charlie registers a photodection event) and (1, 0) (only Bob registers a photodection event) is the same and is no more than $\frac{1}{2}$. Specifically, if Alice succeeds in repudiating that Bob accepted the message sent by Alice, but Charlie rejected, Charlie needs to register more photodection events than Bob, so we can bound the probability of Alice repudiating successfully as

$$\Pr(\text{repudiation}) \leq 2^{-(s_v-s_a)L}. \tag{30}$$

The security against coherent repudiation of our protocol is rather obviously. In a coherent attack, the entanglement of the states Alice may use is unrestricted. From [4], we know that using globally entangled states cannot help Alice repudiate her signed

message, that is to say

$$\Pr(\text{Alice cheats}|\ \text{individual attack}) \geq \Pr(\text{Alice cheats}|\ \text{coherent attack}). \quad (31)$$

□

References

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. Gottesman, D., Chuang, I.: Quantum digital signatures. Quantum Phys., Preprint at arXiv:quant-ph/0105032 (2001)
4. Clarke, P.J., Collins, R.J., Dunjko, V., Andersson, E., Jeffers, J., Buller, G.S.: Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light. Nat. Commun. **3**(6), 1174 (2012)
5. Wang, T.Y., Cai, X.Q., Ren, Y.L., Zhang, R.L.: Security of quantum digital signatures for classical messages. Sci. Rep. **5**, 9231 (2015)
6. Greenberger, D.M., Horne, M.A., Zeilinger, A.: Bells theorem, quantum theory, and conceptions of universe. Physics **58**, 1131 (1990)
7. Boykin, P.O., Roychowdhury, V.: Optimal encryption of quantum bits. Phys. Rev. A **67**, 042317 (2003)
8. Zeng, G., Keitel, C.H.: Arbitrated quantum-signature scheme. Phys. Rev. A **65**, 042312 (2002)
9. Li, Q., Chan, W.H., Long, D.Y.: Arbitrated quantum signature scheme using Bell states. Phys. Rev. A **79**, 054307 (2009)
10. Zou, X., Qiu, D.: Security analysis and improvements of arbitrated quantum signature schemes. Phys. Rev. A **82**(4), 042325 (2010)
11. Luo, M.X., Chen, X.B., Yun, D., Yang, Y.X.: Quantum signature scheme with weak arbitrator. Int. J. Theor. Phys. **51**, 2135–2142 (2012)
12. Zou, X., Qiu, D., Yu, F., Mateus, P.: Security problems in the quantum signature scheme with a weak arbitrator. Int. J. Theor. Phys. **53**(2), 603–611 (2014)
13. Andersson, E., Curty, M., Jex, I.: Experimentally realiable quantum comparison of coherent states and its applications. Phys. Rev. A **74**(2), 022304-1–022304-11 (2006)
14. Dunjko, V., Wallden, P., Andersson, E.: Quantum digital signatures without quantum memory. Phys. Rev. Lett. **112**(4), 040502 (2014)
15. Amiri, R., Wallden, P., Kent, A., Andersson, E.: Secture quantum signatures using insecure quantum channels. Phys. Rev. A **93**(3), 032325 (2016)
16. Hoeffding, W.: Probability inequalities for sums of bounded random variables. J. Am. Stat. Assoc. **58**(301), 13–30 (1963)
17. Unruh, D.: Computationally binding quantum commitments. In: Advances in Cryptology-EUROCRYPT 2016, LNCS 9666, pages, pp. 497–527, Springer (2016)
18. Wang, M.Q., Wang, X., Zhan, T.: Unconditionally secure multi-party quantum commitment scheme. Quantum Inf. Process. **17**(2), 31 (2018)