Unconditionally secure multi-party quantum commitment scheme *

Mingqiang Wang, Xue Wang, and Tao Zhan

Key Laboratory of Cryptologic Technology and Information Security,
Ministry of Education, School of Mathematics, Shandong University

wangmingqiang@sdu.edu.cn, wangxue715862303@163.com, zhantao@moe.edu.cn

Abstract

A new unconditionally secure multi-party quantum commitment is proposed in this paper by encoding the committed message to the phase of a quantum state. Multi-party means that there are more than one recipient in our scheme. We show that our quantum commitment scheme is unconditional hiding and binding, and hiding is perfect. Our technique is based on the interference of phase-encoded coherent states of light. Its security proof relies on the no-cloning theorem of quantum theory and the properties of quantum information.

Keywords: Photodetection; Phase; Quantum commitment; Binding; Hiding

1 Introduction

Commitment scheme is a fundamental cryptographic primitive that allows one to commit to a chosen value or statement while keeping it hidden from others, with the ability to open the commitment later, and has important applications in a number of cryptographic protocols, including coin tossing [1], zero-knowledge proofs [2], oblivious transfer [3] and secure two-party computation [4]. Unconditionally secure bit commitment was thought to be impossible [5] until recent theoretical protocols [6] that combine with quantum mechanics and relativity were shown to elude previous impossibility proofs.

Informally speaking, commitment scheme is to think of a sender as putting a message in a locked box, and giving the 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 (QC) 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.

*The author is supported by National 973 Grant 2013CB834205 and NSFC Grant 61672019 and The Fundamental Research Funds of Shandong University Grant 2016JC029

1.1 Related work

In 1984, the first quantum bit commitment scheme was introduced by Bennett [1]. In 1993, Brassard et al.[4] presented an information-theoretically secure commitment scheme using quantum communication. In 1997, Mayers [5] claimed that information-theoretically secure quantum bit commitment schemes are impossible. The scope of this general impossibility proof was analyzed in [6], and showed that the impossibility proof cannot work as it stands. Two unconditionally secure bit commitment schemes utilizing anonymous quantum states and decoy states were presented in [6]. In 2011, an unconditionally secure bit commitment with flying qudits was proposed in [7]. Based on Minkowski causality and the properties of quantum information, Kent [8] gave a new unconditionally secure bit commitment scheme. In 2014, Liu et al. [9] designed an experiment to implement unconditionally secure bit commitment, this experiment demonstrates the experimental feasibility of quantum communication with relativistic quantum communication. In 2016, Unruh [11] gave the collapse-binding definition and showed how to construct statistical hiding and collapse-binding commitments in the random oracle model, later he [12] constructed collapse-binding commitment in the standard model without the use of random oracles. Also, many other quantum bit commitment schemes were presented in [10, 13].

1.2 Our contributions

In this paper, we propose an unconditionally secure QC scheme of classical messages. Our scheme is implemented with quantum mechanism, its commit and reveal stages consist of classical messages.

First, We give a two-party QC scheme. And then we extend this scheme to a multi-party one. Multi-party means that there are more than one recipient. What's more, this scheme guarantees that all recipients share the same coherent quantum state through a multiport. In this work, we cite the techniques from the quantum digital signature in [14, 15].

In our scheme, the sender randomizes a message m and encodes it to the phase of coherent state $\mathrm{QuantCom}_m$. By interfering the phase-encoded coherent states of light, the recipient can authenticate the commitment $\mathrm{QuantCom}_m$ in the reveal stage. We show that our QC scheme is unconditional hiding and binding, and hiding is perfect.

The security proof of our scheme is based on the quantum mechanisms and mathematical tools. For the hiding property of our QC scheme, the phase of coherent state $\mathrm{QuantCom}_m$ can not be measured. So none can get the message m without the opening information $\mathbf{r}$, this ensures that our commitment scheme is unconditional hiding. If the recipient gets the information $(m, \mathbf{r})$, then he can verify the commitment. First, the recipient generates coherent quantum state $\rho_{\mathbf{r}} \bigotimes \rho_{m,\mathbf{r}}$. Then he interferes them individually with the coherent quantum state $\mathrm{QuantCom}_m$. If the number of photodetection events on his signal null-port arm is below the threshold value, the recipient accepts the message, otherwise rejects it. For the binding property of our QC scheme, our key observation is that if $m' \not\equiv m \bmod p$, where p is a prime, the following two equations

$$r' \equiv r \bmod p, \quad m'r' \equiv mr \bmod p \tag{1.1}$$

can not hold concurrently. This ensures that our commitment scheme is unconditional binding.

Our quantum commitment scheme is unconditional hiding and binding, and hiding is perfect. Compared with the existing unconditionally secure quantum commitment schemes, our scheme allows that there are more than one recipient, and the length of the committed message is more than one bit.

1.3 Organization and notations

In section 1, we give an introduction of this paper. In section 2, we present a definition of QC commitment and we construct an unconditionally secure two-party QC scheme. In section 3, we construct an unconditionally secure three-party QC scheme. In Section 4, we compare our scheme with the related protocols. In section 5, we conclude this work.

In this paper, we use λ to denote the security parameter, we use $[p]$ to denote the set $\{0, 1, 2, \cdots, p-1\}$, and we use $\otimes$ to denote the tensor product of two quantum states.

2 Two-party Quantum Commitment

In this section, first we present a definition of QC commitment, and then we construct an unconditionally secure two-party QC scheme of classical messages, this scheme is implemented with quantum mechanism, the commit and the reveal stages consist of classical messages.

2.1 Definition of QC commitment

First, we recall the basics of QC scheme. The following is taken verbatim from [11].
Commitment. A commitment scheme consists of algorithms *Com* and *Verify*. $(\mathrm{C}, \mathrm{u}) \leftarrow \mathit{Com}(1^\lambda, m)$ 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, we send (m, u) to the recipient who checks whether $\mathit{Verify}(1^\lambda, \mathrm{C}, \mathrm{m}, \mathrm{u}) = 1$. *Com* has classical input, and a well-defined message space $\mathcal{M}$ that depends on the security parameter λ (e.g., $\{0,1\}^\lambda$). Furthermore, for technical reasons, we assume that it is possible to find triples $(\mathrm{C}, \mathrm{m}, \mathrm{u})$ with $\mathit{Verify}(1^\lambda, \mathrm{C}, \mathrm{m}, \mathrm{u}) = 1$ with overwhelming probability.

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

- ◇ **Completeness:** *for any $m \in \mathcal{M}$, the following probability is declining exponentially in terms of the length of the QC*

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

- ◇ **Unconditional binding:** *for any computationally unlimited adversary $\mathcal{A}$ and $m \in \mathcal{M}$, the following probability is declining exponentially in terms of the length of the QC*

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

- ◇ **Unconditional hiding:** *for any computationally unlimited adversary $\mathcal{A}$ and $m \in \mathcal{M}$, the following probability is declining exponentially in terms of the length of the QC*

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

2.2 Our construction

In this subsection, we present an unconditionally secure two-party QC scheme with one sender Alice and one recipient Bob, and we describe it as following.

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

$$\rho_k = |e^{\frac{2r_k\pi i}{p}}\alpha >< e^{\frac{2r_k\pi i}{p}}\alpha|,\ k = 1, \cdots, L, \tag{2.1}$$

$$\rho_k^m = |e^{\frac{2mr_k\pi i}{p}}\alpha >< e^{\frac{2mr_k\pi i}{p}}\alpha|,\ k = 1, \cdots, L. \tag{2.2}$$

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

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

   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, 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 photodection events is below $2s_aL$, otherwise rejects it. The parameter s_a is called the authentication threshold which will be chosen later.

Intuitively, our commitment protocol is unconditionally secure, i.e. it's security is independent of the ability of the adversary. The following simple lemmas are useful for the proof of our commitment.

Lemma 1. *Let p be a prime. For any a and b, the following equation*

$$ax \equiv b \bmod p \tag{2.3}$$

has at most one solution modulo p.

Lemma 2. *[16] Let $X_1, ..., X_L$ be independent random variables each attaining 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*

$$P(\bar{X} - E(\bar{X}) \geq t) \leq \exp(-2t^2L), \tag{2.4}$$

$$P(|\bar{X} - E(\bar{X})| \geq t) \leq 2\exp(-2t^2L). \tag{2.5}$$

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

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

Proof. We divide our proof into three parts: completeness, unconditional hiding and unconditional binding.

For any integer $0 \leq a, b \leq p-1$, let $c_{a,b}$ denote the probability that causes a photodection event on Bob'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 Alice declare is $\frac{2b\pi}{p}$. Let $\bar{X} = \frac{1}{2L}X$, X denotes the total number of photodetection events on Bob's signal null-port arm and $E(\bar{X})$ denotes the expectancy of the variable $\bar{X}$. Also, we let

$$c = \max_{a\in[p]}\{c_{a,a}\}, \tag{2.6}$$

$$\widehat{c}_{p_1,p_2} = p_1 \min_{a\in[p]}\{c_{a,a}\} + p_2 \min_{a,b\in[p],a\neq b}\{c_{a,b}\}. \tag{2.7}$$

And let $g_1 = \widehat{c}_{\frac{1}{2},\frac{1}{2}} - c$, by the experiment in Appendix A, we have that $g_1 > 0$. Then we set $s_a = \widehat{c}_{\frac{1}{2},\frac{1}{2}} - \beta g_1$, where $0 < \beta < 1$.

Completeness. If the two parties in this protocol are honest, by the experiment in Appendix A, we have that

$$E(\bar{X}) \leq \max_{a\in[p]}\{d_{a,a}\} = c. \tag{2.8}$$

It is easy to say that

$$\Pr[\mathit{Verify}(1^\lambda, \mathrm{C}, \mathrm{m}, \mathrm{u}) \neq 1 : (\mathrm{C}, \mathrm{u}) \leftarrow \mathit{Com}(1^\lambda, m)] = \Pr(\text{Bob rejects}) = \Pr(\bar{X} > s_a), \tag{2.9}$$

then we can bound the probability that the committed message is rejected as

$$\Pr(\bar{X} > s_a) = \Pr(\bar{X} > c + (1-\beta)g_1) \leq \Pr(\bar{X} > E(\bar{X}) + (1-\beta)g_1) \leq \exp(-4(1-\beta)^2 g_1^2 L). \tag{2.10}$$

Unconditional hiding. None can get any extra information about the phase of a quantum commitment by measuring. So for any adversary $\mathcal{A}$, we have the following probability

$$\Pr[m \leftarrow \mathcal{A}(1^\lambda, \mathrm{C}) : (\mathrm{C}, \mathrm{u}) \leftarrow \mathit{Com}(1^\lambda, m)] = 1/|\mathcal{M}|. \tag{2.11}$$

Hence, the commitment scheme is perfect hiding.

Unconditional binding. In order to prove that our QC scheme is unconditional binding, we need to show that for any $m' \neq m$ and $\mathbf{r}' = (r'_1, \cdots, r'_L)$, the probability of $\mathit{Verify}(\mathrm{QuantCom}_m, m', \mathbf{r}') = 1$ is declining exponentially in terms of the length of the QC.

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

$$r' \equiv r \bmod p, \tag{2.12}$$

$$m'r' \equiv mr \bmod p \tag{2.13}$$

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

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

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

$$r'_i \equiv r_i \bmod p, \quad m'r'_i \equiv mr_i \bmod p, \quad 1 \leq i \leq L, \tag{2.14}$$

is at least L.

By the above discussions, we have

$$\begin{aligned} E(\bar{X}) &= \frac{1}{2L}E(X) \\ &\geq \frac{1}{2L}(L\min_{a\in[p]}\{c_{a,a}\} + L\min_{\substack{a,b\in[p]\\ a\neq b}}\{c_{a,b}\}) \\ &= \frac{1}{2}\min_{a\in[p]}\{c_{a,a}\} + \frac{1}{2}\min_{\substack{a,b\in[p]\\ a\neq b}}\{c_{a,b}\}. \end{aligned} \tag{2.15}$$

It is easy to say that

$$\Pr[\mathit{Verify}(\mathrm{QuantCom}_m, m', \mathbf{r}') = 1] = \Pr[\text{Bob accepts}] = \Pr[\bar{X} \leq s_a]. \tag{2.16}$$

By Lemma 2, we get

$$\Pr[\bar{X} \leq s_a] \leq \Pr[\bar{X} - E(\bar{X}) \leq -\beta g_1] \leq \Pr[|\bar{X} - E(\bar{X})| \geq \beta g_1] \leq 2\exp(-4\beta^2 g_1^2 L). \tag{2.17}$$

This probability is declining exponentially in terms of the length of the QC. Therefore, we complete the proof of this Theorem. What's more, the binding property guarantees that our scheme also can resist forgery attack. ■

3 Multi-party Quantum Commitment

In this section, we construct a QC scheme with one sender Alice and two recipients Bob and Charlie, and this can be extended to multi-party QC scheme trivially. Charlie is the trusted third party who can resist repudiation of other participants. The technique in this construction comes from quantum digital signature [14]. It is required that the quantum channels between the sender and the recipients are secure to ensure that the states won't be tempered over these channels by any external adversary.

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

- ◇ In the commit stage, Alice sends the commitment C of the signed message m to Bob and Charlie. Then two recipients perform symmetrisation of their states through the multiport and store the outcomes.
- ◇ In the reveal stage, Alice sends m and opening information u to Bob, Bob authenticates the commitment C. If fails, the protocol has to be aborted. Otherwise, Bob sends (m, u) to Charlie, then Charlie performs an analogous procedure as Bob to verify the commitment C.

Now, we describe multi-party quantum commitment scheme as following.

1. **The commit stage.**
   (a) To commit to a message $m \in [p]$, first Alice chooses sequence $\mathbf{r} = (r_1, r_2, ..., r_L)$ from $[p]^L$ randomly and generates two sequences of coherent states

$$\rho_k = |e^{\frac{2r_k\pi i}{p}}\alpha >< e^{\frac{2r_k\pi i}{p}}\alpha|,\ k = 1, \cdots, L, \tag{3.1}$$

$$\rho_k^m = |e^{\frac{2mr_k\pi i}{p}}\alpha >< e^{\frac{2mr_k\pi i}{p}}\alpha|,\ k = 1, \cdots, L. \tag{3.2}$$

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

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

The vector $\mathbf{r}$ is called the opening information of message m.

(b) Alice generates two copies of a sequence of coherent states $\text{QuantCom}_m = (\rho_{\mathbf{r}}, \rho_{m,\mathbf{r}})$. The sequence of such coherent states QuantCom_m is called a commitment of message m. QuantCom_m is in $2L$ independent quantum registers, each register does not interfere with each other. She sends one copy of this commitment to Bob and the other to Charlie over an authenticated channel.

(c) Bob and Charlie send the sequence of QuantCom_m through a multiport, saving the output states in quantum memory.

2. **The reveal stage.**

(a) Alice sends the corresponding pair $(m, \mathbf{r})$ to Bob over an insecure channel. To authenticate the commitment, Bob generates coherent states of amplitude α with the relative phase defined by the declared $(m, \mathbf{r})$, and interferes them individually with the states he has in his quantum memory. He counts the number of photodetection events on his signal null-port arm and authenticates this commitment if the number of photodection events is below $2s_aL$. The parameter s_a is the authentication threshold .

(b) To prove to Charlie that he received the message m from Alice, Bob sends $(m, \mathbf{r})$ to Charlie. Charlie then performs an analogous procedure as Bob, and he verifies this commitment if the number of photodection events is below $2s_vL$, where s_v is called the verification threshold, with $0 < s_a < s_v < 1$.

If any of the thresholds is breached, the protocol has to be aborted.
The following Lemma is useful for the proof of the security of our three-party QC scheme.

Lemma 3. *In the QC scheme, we assume that Alice sends the same coherent quantum state σ corresponding to $(m, \mathbf{r})$ to the adversary $\mathcal{A}$ and Charlie. In the commit stage, the adversary changes his input through a multiport, then suppose the adversary $\mathcal{A}$ and Charlie share a quantum state σ' corresponding to a vector*

$$(a_1, a_2, ..., a_L, b_1, b_2, ..., b_L).$$

After getting $(m, \mathbf{r})$, no matter how the adversary $\mathcal{A}$ chooses $m' \not\equiv m \bmod p$ and $\mathbf{r}'$, The probability of the following case is negligible: there are more than $3L/2$ identical entries modulo p between the following two vectors

$$(a_1, a_2, ..., a_L, b_1, b_2, ..., b_L),\ (r'_1, r'_2, \cdots, r'_L, m'r'_1, m'r'_2, \cdots, m'r'_L).$$

Proof. Before changing his input through a multiport, Bob has no idea about the original information $(m, \mathbf{r})$. Therefore the vector $(a_1, a_2, ..., a_L, b_1, b_2, ..., b_L)$ is random to Bob. It is easy to see that, the probability of the adversary $\mathcal{A}$ making each a_i, b_i with $m' \not\equiv m \bmod p$ satisfy that $m'a_i \equiv b_i \bmod p$ is $\frac{1}{p}$.

Let E_t be the events that there are more than t equations hold in the following L equations

$$m'a_i \equiv b_i \bmod p, \quad 1 \le i \le L. \tag{3.3}$$

It is not difficult to see

$$\begin{aligned}\Pr(E_t) &= \sum_{k=t}^{L} C_L^k (\frac{1}{p})^k (1-\frac{1}{p})^{L-k} \\ &\leq (\frac{1}{p})^t \sum_{k=0}^{L} C_L^k (1-\frac{1}{p})^{L-k} \\ &\leq \frac{2^L}{p^t}.\end{aligned} \tag{3.4}$$

Take $t = \frac{L}{2}$, we have $\Pr(E_{\frac{L}{2}}) \leq (\frac{2}{\sqrt{p}})^L$, which completes the proof of this Lemma. ■

Besides the requirement of completeness, unconditional hiding and binding, the three-party QC scheme needs to resist Bob's cheating. Now, we state our main result.

Theorem 2. *The three-party quantum commitment scheme is unconditionally secure.*

Proof. The proof of this Theorem is divided into four parts: completeness, unconditional hiding, security against cheating of sender, security against cheating of recipients.

For any integer $0 \leq a, b \leq p-1$, let $c_{a,b}$ denote the probability that causes a photodection 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 $\bar{X} = \frac{1}{2L}X$, X denotes the total number of photodetection events on the recipient's signal null-port arm, and $E(\bar{X})$ denotes the expectancy of the variable $\bar{X}$. Also, we let

$$c = \max_{a\in[p]}\{c_{a,a}\}, \tag{3.5}$$

$$\widehat{c}_{p_1,p_2} = p_1 \min_{a\in[p]}\{c_{a,a}\} + p_2 \min_{a,b\in[p],a\neq b}\{c_{a,b}\}. \tag{3.6}$$

And $g_1 = \widehat{c}_{\frac{1}{2},\frac{1}{2}} - c$, $g_2 = \widehat{c}_{\frac{3}{4},\frac{1}{4}} - c$, by the experiment in Appendix A, we have that $g_1 > 0$, $g_2 > 0$. We set $s_a = \widehat{c}_{\frac{1}{2},\frac{1}{2}} - \beta g_1$, $s_v = \widehat{c}_{\frac{3}{4},\frac{1}{4}} - \gamma g_2$, where β, γ must satisfy that $s_a < s_v$ and $0 < \gamma < \beta < 1$.

Completeness. If the three parties in this protocol are honest, by the experiment in Appendix A, we have that

$$E(\bar{X}) \leq \max_{a\in[p]}\{c_{a,a}\} = c. \tag{3.7}$$

It is easy to say that

$$\Pr[\mathit{Verify}(1^\lambda, \mathrm{C}, \mathrm{m}, \mathrm{u}) \neq 1 : (\mathrm{C}, \mathrm{u}) \leftarrow \mathit{Com}(1^\lambda, m)] = \Pr(\text{the recipient rejects}) = \Pr(\bar{X} > s_a), \tag{3.8}$$

then we can bound the probability that the commitment is not be authenticated as

$$\Pr(\text{Bob rejects}) = \Pr(\bar{X} > c + (1-\beta)g_1) \leq \Pr(\bar{X} > E(\bar{X}) + (1-\beta)g_1) \leq \exp(-4(1-\beta)^2 g_1^2 L). \tag{3.9}$$

Also, we can bound the probability that the commitment is not be verified as

$$\Pr(\text{Charlie rejects}) = \Pr(\bar{X} > s_v) \leq \Pr(\bar{X} > s_a) \leq \exp(-4(1-\beta)^2 g_1^2 L). \tag{3.10}$$

Unconditional hiding. No one can get any extra information about the phase of a commitment by measuring. So for any adversary $\mathcal{A}$, we have the following probability

$$\Pr[m \leftarrow \mathcal{A}(1^\lambda, \mathrm{C}) : (\mathrm{C}, \mathrm{u}) \leftarrow \mathit{Com}(1^\lambda, m)] = 1/|\mathcal{M}|. \tag{3.11}$$

Hence, the commitment scheme is perfect hiding.

Security against cheating of sender. The proof of this part is the same as the proof of unconditional binding in Theorem 1.

Security against cheating of recipients. Now, we assume that Bob is dishonest. First, we draw a clear distinction between passive attack and active attack. In passive attack, Bob behaves honestly until the reveal stage in above three-party QC scheme. In active attack, Bob behaves dishonestly throughout the whole stages, specifically he can tamper with his part of states that he sends to Charlie throughout the multiport.

To forge a message, Bob has to generate a new opening information that can pass Charlie's verification. Because Bob had received the true $(m, \mathbf{r})$ from Alice, the best way of forging for Bob is to find a suitable $(m', \mathbf{r}')$ that can cause the number of photodetection events on Charlie's signal null-port arm is below $2s_vL$.

In the passive attack, we need to prove that

$$\Pr[\,\mathit{Verify}(\mathrm{QuantComm}_m, m', \mathbf{r}') = 1 : (m', \mathbf{r}') \leftarrow \mathit{Bob}]$$

is declining exponentially in terms of the length of the QC. The property of unconditional binding guarantees that our QC scheme resists passive attack.

In the active attack, we need to prove that

$$\Pr[\,\mathit{Verify}(\mathrm{QuantComm}'_m, m', \mathbf{r}') = 1 : (m', \mathbf{r}') \leftarrow \mathit{Bob}]$$

is declining exponentially in terms of the length of the QC. In this attack, Bob is allowed to alter the states he sends to Charlie throughout the multiport, which modifies the states that Charlie stored in his quantum memory. This means that Bob and Charlie share a new coherent quantum state corresponding to a vector

$$(a_1, a_2, ..., a_L, b_1, b_2, ..., b_L).$$

Before changing his input through a multiport, Bob has no idea about the original information $(m, \mathbf{r})$. Therefore the vector $(a_1, a_2, ..., a_L, b_1, b_2, ..., b_L)$ is random to Bob.

From Lemma 3, we know that no matter how Bob chooses the random sequence vector $\mathbf{r}' = (r'_1, \cdots, r'_L)$ and $m' \neq m$, except a negligible probability, there are at least $L/2$ different entries modulo p between the following two vectors

$$(a_1, a_2, ..., a_L, b_1, b_2, ..., b_L),\ (r'_1, \cdots, r'_L, m'r'_1, \cdots, m'r'_L).$$

Hence, we have

$$\begin{aligned} E(\bar{X}) &\geq \frac{1}{2L}\left(\frac{3L}{2}\min_{a\in[p]}\{c_{a,a}\} + \frac{L}{2}\min_{a,b\in[p],a\neq b}\{c_{a,b}\}\right) \\ &= \frac{3}{4}\min_{a\in[p]}\{c_{a,a}\} + \frac{1}{4}\min_{a,b\in[p],a\neq b}\{c_{a,b}\}. \end{aligned} \tag{3.12}$$

It is easy to see that

$$\Pr[\,\mathit{Verify}(\mathrm{QuantComm}'_m, m', \mathbf{r}') = 1 : (m', \mathbf{r}') \leftarrow \mathit{Bob}] = \Pr[\bar{X} \leq s_v]. \tag{3.13}$$

Then we have

$$\Pr[\bar{X} \leq s_v] = \Pr[\bar{X} \leq \widehat{c}_{\frac{1}{4},\frac{3}{4}} - \gamma g_2] \leq \Pr[|\bar{X} - E(\bar{X})| \geq \gamma g_2] \leq 2\exp(-4\gamma^2 g_2^2 L). \tag{3.14}$$

This probability is declining exponentially in terms of the length of the QC, so we complete the proof of this Theorem.■

4 Compared with the Related Work

In this section, we compare our scheme with the main existing unconditionally secure commitment schemes. Intuitively, the most important advantages of our scheme can be showed in two aspects: efficiency and function.

In 1993, Brassard et al.[4] presented a bit commitment scheme using quantum communication and claimed that the scheme is information-theoretically secure. Unfortunately, in 1997, Mayers [5] proved that the bit commitment scheme in [4] is not correct. Based on the existence of quantum one-way functions by fundamental principles of quantum physics, in 2004, Lu et al. [13] proposed the first unconditionally bit commitment scheme. Later, many unconditionally secure bit commitment schemes were presented [7, 8, 10] by applying different laws of quantum physics.

In this work, we provide the first unconditionally secure multiple bits commitment scheme based on the interference of phase-encoded coherent states of light. Our method is to encode the committed message to the phase of the commitment. Compared with the above schemes, our scheme allows that there are more than one recipient and the length of the committed message is not limited to one bit. To ensure that each recipient saves the symmetric output states in quantum memory, we use the multiport.

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

	hiding	binding	the number of the recipient	whether the agent is required	the length of the committed message
[7]	perfect	unconditional	one	no	one bit
[8]	perfect	unconditional	one	yes	one bit
[11]	perfect	unconditional	one	no	one bit
[13]	perfect	statistical	one	no	one bit
our scheme	perfect	unconditional	more than one	no	multiple bits

5 Conclusion

In this paper, we construct an unconditionally secure multi-party QC scheme for classical messages. First, we present an unconditionally secure two-party QC scheme. Then we extend this scheme to an unconditionally secure multi-party QC scheme. After that, we show that our quantum commitment scheme is unconditional hiding and binding, and hiding is perfect. In addition, our technique is based on the interference of phase-encoded coherent states of light. Its security proof relies on the no-cloning theorem of quantum theory and the properties of quantum information.

Acknowledgement: We express our heartful thanks to reviewers for their useful comments which improve our manuscript greatly.

References

[1] Bennett C.H. and Brassard G. Quantum cryptography : Public key distribution and coin tossing. In Proc. IEEE International Conference on Computers Systems and Signal Processing, volume 560, pages 175-179, IEEE Computer Society, 1984.

[2] Watrous, J. Zero-knowledge against quantum attacks. SIAM J. Comput. 39(1), pages 25-58, 2009.

[3] Crpeau C., Dumais P., Mayers D., and Salvail L. Computational collapse of quantum state with application to oblivious transfer. In Theory of Cryptography, In TCC 2004, LNCS 2951, pages 374-393, Springer. 2004.

[4] Brassard G., Crepeau C., Jozsa R., and Langlois D. A quantum bit commitment scheme provably unbreakable by both parties. In Proc. FOCS 1993, pages 362-371, IEEE Computer Society, 1993.

[5] Mayers D. Unconditionally secure quantum bit commitment is impossible. Physical Review Letters, 78(17):3414-3417, 1997.

[6] Yuen H.P. Unconditionally secure quantum bit commitment is possible. Quantum Physics, 2005. arXiv:quant-ph/0505132v1.

[7] Kent A. Unconditionally secure bit commitment with flying qudits. New Journal of Physics, 13(11):113015-113029(15), 2011.

[8] Kent A. Unconditionally secure bit commitment by transmitting measurement outcomes. Physical Review Letters, 109(13):130501, 2012.

[9] Liu Y., Cao Y., Curty M., Liao S.K., Wang J., Cui K., Li Y.H., Lin Z.H., Sun Q.C., and Li D.D. Experimental unconditionally secure bit commitment. Physical Review Letters, 112(1):010504, 2014.

[10] Cheung C.Y. Unconditionally secure quantum bit commitment using neutron double-slit interference. Quantum Physics, 2010. arXiv:0910.2645v4.

[11] Unruh D. Computationally binding quantum commitments. In Advances in Cryptology-EUROCRYPT 2016, LNCS 9666, pages 497-527, Springer. 2016.

[12] Unruh D. Collapse-binding quantum commitments without random oracles. In Advances in Cryptology-ASIACRYPT 2016: Part II 22, LNCS 10032, pages 166-195, Springer. 2016.

[13] Lu X., Ma Z., and Feng D.G. An unconditionally secure quantum bit commitment scheme. Quantum Physics, 2004. arXiv:quant-ph/0403036v6.

[14] Clarke P.J., Collins R.J., Dunjko V., Andersson E., Jeffers J., and Buller G.S. Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light. Nature Communications, 3(6):1174, 2012.

[15] Gottesman, D. and Chuang, I. Quantum digital signatures. Preprint at http:// arxiv. org/ abs/ quant-ph/ 0105032, 2001.

[16] Hoeffding W. Probability inequalities for sums of bounded random variables. Journal of the American Statistical Association, 58(301):13-30, 1963.

Appendix A. Experimental data of interfering phase

In the cost matrix **C**, the diagonal elements represent the cases when recipient uses the same phase as sender, the off-diagonal elements represent the cases when recipient uses the phase different from sender. In 2012, Clarke et al. [14] presented us a practical experimental data, the cost matrix **C**

realised by experimental set-up using 8 different phase states and with average photon number of $|\alpha^2| = 0.16$ per pulse is given by

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