Quantum bit commitment with cheat sensitive binding and approximate sealing

Yan-Bing Li\textsuperscript{1,2,3}, Sheng-Wei Xu\textsuperscript{2}, Wei Huang\textsuperscript{1} and Zong-Jie Wan\textsuperscript{2}

\textsuperscript{1} State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, People's Republic of China
\textsuperscript{2} Beijing Electronic Science and Technology Institute, Beijing, 100070, People's Republic of China
\textsuperscript{3} Department of Electrical Engineering and Computer Science, Northwestern University, Evanston, IL 60208, USA

E-mail: liyanbing1981@gmail.com

Received 25 July 2014, revised 11 February 2015
Accepted for publication 12 February 2015
Published 12 March 2015

Abstract

This paper proposes a cheat-sensitive quantum bit commitment scheme based on single photons, in which Alice commits a bit to Bob. Here, Bob’s probability of success at cheating as obtains the committed bit before the opening phase becomes close to \( \frac{1}{2} \) (just like performing a guess) as the number of single photons used is increased. And if Alice alters her committed bit after the commitment phase, her cheating will be detected with a probability that becomes close to 1 as the number of single photons used is increased. The scheme is easy to realize with present day technology.

Keywords: quantum bit commitment, cheat sensitive, error correcting, sealing, binding

(Some figures may appear in colour only in the online journal)

1. Introduction

Bit commitment (BC) is a cryptographic task performed by two participants, which has a lot of applications in crucial cryptographic protocols including interactive zero-knowledge proof [1–4], coin flipping [5–7], oblivious transfer [8, 9], multi-party secure computation [10–13], and so on.

Generally, BC mainly consists of two phases: the commitment phase and the opening phase. In the commitment phase, Alice chooses a bit \( b \) \((b = 0 \text{ or } 1)\) which she wants to commit to Bob, and gives him some encrypted information about the bit, which cannot be decrypted.
by him before the opening phase. Later, in the opening phase, Alice announces some information for decrypting $b$ and the value of $b$. After decryption, Bob obtains an output $b'$. The commitment will be accepted by Bob if $b' = b$. Otherwise, the commitment will be rejected (if $b' \neq b$). Bit commitment must meet the following needs. Correctness. Bob should always accept for $b' = b$ if both participants are honest. Sealing. Before the opening phase, Bob cannot know $b$. Binding. Alice cannot change the value of $b$ after the commitment phase.

There are several quantum approaches [5, 14] that have been considered for guaranteeing unconditional security of quantum BC (QBC) protocols, such as quantum key distribution (QKD) protocols [15, 16]. Unfortunately, it was concluded that unconditionally secure QBC can never be achieved in principle; this was referred to as the Mayers–Lo–Chau (MLC) no-go theorem [17–19]. Although unconditionally secure QBC protocols are nonexistent, there are several schemes satisfying special security model requirements, such as the cheat-sensitive protocol and the relativistic protocol, that have been proposed [20–30]. Among these, an important class is that of the cheat-sensitive QBC (CSQBC) protocols, first proposed by Hardy and Kent [20]. In CSQBC, assuming that the commitment will eventually be opened, Alice cannot alter the committed bit after the commitment phase without risking detection by Bob, and Bob cannot extract information about the committed bit before the opening phase without risking detection by Alice. In other words, cheat sensitivity means that all of the cheating strategies should be detected with nonzero probability in the protocol.

In the first CSQBC scheme [20], a singlet state is used to perform a stage ‘challenge’, giving Alice and Bob chances with equal probabilities $\frac{1}{2}$ of performing their detection strategies. Also, quantum memory is needed to store a single photon representing the committed bit from the commitment phase before going to the opening phase. This opened up a new field in quantum cryptography, but is not a feasible scheme at present, as long-term quantum memory is difficult to realize with present day technology, and single-photon states are easily disturbed in practical settings.

In this paper, we propose a variant CSQBC scheme based on single photons. Unlike for the first CSQBC scheme, entangled states and quantum memory are not used here. In order to conceal the committed bit and to overcome the loss and noise in practical settings, an error correcting code (ECC) is used. In the scheme, the cheating sensitivity is a one-way process, which is only available in the binding. If Alice alters her committed bit, her cheating will be detected with a probability becoming close to 1 as the number of single photons used is increased. As for the sealing, Bob can only cheat as regards the committed bit with probability $\frac{1}{2} + \varepsilon$, where $\varepsilon$ becomes close to 0 as the number of single photons used is increased. When $\varepsilon = 0$, the one-way CSQBC is more secure than the two-way CSQBC, as the full sealing is more secure than cheat-sensitive sealing. However, since the MLC no-go theorem indicated that $\varepsilon = 0$ is impossible, we were only able to search for $\varepsilon \to 0$ in one-way CSQBC.

This paper is organized as follows. Section 2 shows the one-way CSQBC scheme. In section 3, we prove that the scheme is sensitive to cheating in binding and approximate sealing. And the protocol’s practicability is also analyzed. Finally, section 4 gives a short conclusion.

2. The quantum bit commitment scheme

In this protocol, Alice will commit a bit $b$ to Bob. Single photons will be used, each of which is prepared as one of the four states $\{ |0\rangle, |1\rangle, |+\rangle, |-\rangle \}$ randomly, where $|0\rangle$ and $|1\rangle$ are the two eigenstates of the Pauli operator $\sigma_z$, and $|+\rangle$ and $|-\rangle$ are the two eigenstates of the Pauli operator $\sigma_x$. For cheating sensitivity in binding and approximate sealing, an error
correcting code (ECC) will be used here. The specific steps of the protocol (shown in figure 1) are described as follows.

**[The pre-commitment phase]**

1. Alice and Bob agree on an ECC, the \((n, k, d)\)-code \(C\) \([31]\), which uses an \(n\)-bit codeword to encode a \(k\)-bit word, and the distance between any two codewords is \(d\).
2. Alice chooses a nonzero random \(n\)-bit string \(r = (r_1, r_2, \ldots, r_n)\), where \(r_i \in \{0, 1\}\), and announces it to Bob. Alice uses it to divide all the \(n\)-bit codewords \(C = (c_1 c_2 \ldots c_n)\) in \(C\) into two subsets \(C_0 = \{c \in C | c \oplus r = 0\}\) and \(C_1 = \{c \in C | c \oplus r = 1\}\), where \(c \oplus r \equiv \bigoplus_{i=1}^{n} c_i \land r_i\).
3. Bob prepares an ordered \(n\)-photon sequence \(s = (s_1, s_2, \ldots, s_n)\), in which each \(s_i\) is randomly in one of the four states \((|0\rangle, |1\rangle, |+\rangle, |-\rangle)\). Then Bob sends the photon sequence \(s\) to Alice.

**[The commitment phase]**

4. According to the commitment bit \(b\), Alice chooses a codeword \(c\) from \(C_b\) randomly.
5. When \(c_i = 0\), Alice measures the \(i\)-th photon \(s_i\) in basis \(Z\). Otherwise, when \(c_i = 1\), Alice measures the \(i\)-th photon \(s_i\) in basis \(X\). Then she obtains the outcomes \(o = (o_1, o_2, \ldots, o_n)\), where \(o_i \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}\).
6. When \(o_i \in \{|0\rangle, |+\rangle\}\), Alice sets \(o'_i = 0\). When \(o_i \in \{|1\rangle, |-\rangle\}\), Alice sets \(o'_i = 1\). Then Alice announces \(o' = (o'_1, o'_2, \ldots, o'_n)\) to Bob.

**[The opening phase]**

7. Alice announces the committed bit \(b\), and \(o\) and \(c\), to Bob.
(8) Bob checks whether $o$ is right or not. The rule is that when $o_i' = 0$ (or 1), one should have $o_i \in \{|0\}, |+\rangle\}$ (or $\{|1\}, |-\rangle\}$). Then Bob checks whether $c \otimes r = b$ or not. If both of them are right, he accepts the committed bit. Otherwise, he rejects the committed bit.

3. Analysis

In the protocol presented, in the absence of consideration of the noise in the quantum channels and equipment, Bob will always accept Alice’s committed bit, as $c \otimes r = b$, when both of them are honest.

However, in a quantum bit commitment protocol, Alice and Bob do not trust each other. Furthermore, one of them may be dishonest and perform some cheating strategies. So we will analyze the scheme’s security in the following two cases: (1) a dishonest Alice and an honest Bob; (2) a dishonest Bob and an honest Alice. Generally, the case where neither Alice nor Bob is honest will not be considered, since that will be quantum gambling.

And the real-life setting will present some problems to the protocol. In this section, we will analyze the protocol’s practicability in the ideal setting, following this with a security analysis of it.

3.1. Cheat-sensitive binding

In the scheme, the EC $(n, k, d)$-code $C$ is used, in which the distance between any two codewords is $d$. This means that Alice should change $d$ bits in $c$ if she wants to alter the committed bit $b$ to $b'$, where $b, b' \in \{0, 1\}$ and $b \neq b'$. Further, Alice could use the slyest strategy, in which she first commits a bit $b''$ other than 0 or 1, i.e., she chooses a bit string $c'$ which is contained in neither $C(0)$ nor $C(1)$, and has the Hamming distance between $c'$ and any one of $C(0)$ and $C(1)$ be $d/2$. Then she only needs to change $d/2$ bits in $c'$ to cheat with $b = 0$ or $b = 1$.

When Alice announces $o'$, it means that she had committed something, regardless of whether she has measured the photons or not. In the opening phase, what she should do is to make $o$ and $c$ tally with $o'$ and her wanted $b$. For instance, if she wants to cheat with $b = 0$, $c$ should be in the set $C(0)$. We know that both $o_i = \{0\}$ and $|+\rangle$ ($o_i = \{1\}$ and $|-\rangle$) are possible when $o_i' = 0$ (or $o_i' = 1$), so $2^n$ different cases of $o$ are legal corresponding to one $o'$. Then the cheating strategy degenerates to a simpler form: Bob sends a photon in one of the states $\{|0\}, |1\rangle\}$ to Alice. Alice could do anything in response to this, but she should say whether the state is in the set $\{|0\}, |+\rangle\}$ or the set $\{|1\}, |-\rangle\}$. If she is right, she could cheat successfully with probability 1 as the states in the set are always legal. But if she is wrong, her cheating will be detected with probability 1/2, as she can avoid having her cheating detected when her announced basis is wrong but it will be detected with certainty when her announced basis is right.

Now we analyze how Alice can distinguish the single photon from the sets $\{|0\}, |+\rangle\}$ and $\{|1\}, |-\rangle\}$. Since the photon is always held in Alice’s hand, she would not use any ancilla states, but would measure the photon directly. We suppose that the measurement basis is $\{|n_0\}, |n_1\rangle\}$, where $|n_0\rangle = \cos \theta |0\rangle + \sin \theta |1\rangle$ and $|n_1\rangle = \sin \theta |0\rangle - \cos \theta |1\rangle$. It should be the case that

$$
|0\rangle = \cos \theta |n_0\rangle + \sin \theta |n_1\rangle,
$$

(1a)
\[ |1\rangle = \sin \theta |n_0\rangle - \cos \theta |n_1\rangle, \quad (1b) \]

\[ |+\rangle = \cos \left( \frac{\pi}{4} - \theta \right) |0\rangle - \sin \left( \frac{\pi}{4} - \theta \right) |1\rangle \quad (1c) \]

\[ |−\rangle = \sin \left( \frac{\pi}{4} - \theta \right) |0\rangle + \cos \left( \frac{\pi}{4} - \theta \right) |1\rangle. \quad (1d) \]

When the photon is \(|0\rangle\) or \(|1\rangle\), Alice can distinguish the two sets successfully with probability \(\cos^2 \theta\). When the photon is \(|+\rangle\) or \(|−\rangle\), Alice will distinguish the two sets successfully with probability \(\cos^2 \left( \frac{\pi}{4} - \theta \right)\). So the total probability of Alice distinguishing the two sets successfully is

\[
P = \frac{\cos^2 \theta + \cos^2 \left( \frac{\pi}{4} - \theta \right)}{2} = \frac{2 + \sin 2\theta + \cos 2\theta}{4} = \frac{2 + \sqrt{2} \cos \left( \frac{\pi}{4} - 2\theta \right)}{4}. \quad (2)\]

It should be the case that \(\frac{2 - \sqrt{2}}{4} \leq P \leq \frac{2 + \sqrt{2}}{4}\). If Alice distinguishes the sets unsuccessfully, Bob will detect the cheating when his basis is the same as what Alice announced. So Alice’s cheating will be detected with at least the probability \(1 - \left( \frac{1 - \left( \sqrt{2} \frac{\pi}{4} \right)}{2} \right)^d\), after she has cheated as regards one photon. As she must cheat as regards at least \(d/2\) photons, her cheating will be detected with probability \(1 - \left( \frac{1 - \left( \sqrt{2} \frac{\pi}{4} \right)}{2} \right)^d\), for altering the committed bit. With increasing value of \(d\), the probability will become close to 1. Since \(d\) increases with increasing value of \(n\) normally, this means that Alice’s cheating will be detected with probability becoming close to 1 with increasing number of single photons used if she alters the committed bit.

In a QSQBC, cheating sensitivity in binding means that Bob is sensitive to all of Alice’s cheating actions. Suppose a dishonest Alice will be detected by Bob with probability \(P_{\text{cheat}} (0 \leq P_{\text{cheat}} \leq 1)\) after she has performed an effective cheating strategy to alter her committed bit. When \(P_{\text{cheat}} > 0\), the QBC protocol is sensitive to cheating in binding. Obviously, under the same cheating strategy, a QBC protocol is better with bigger \(P_{\text{cheat}}\). As \(P_{\text{cheat}} \leq 1\), the QBC presented has a good capability for cheating sensitivity in binding, as the value is close to 1.

### 3.2. Approximate sealing

Before the opening phase, a dishonest Bob might cheat on Alice’s committed bit with the states that he sent and Alice’s announcement.

**Cheating method I.** Without any additional processing, a curious Bob could obtain some information about \(o_i\). When the \(i\)th photon that Bob sent is \(|0\rangle\), he can guess that the basis that Alice used is \(Z\) if Alice said that her measurement outcome is in the set \(|0\rangle, |+\rangle\}. Otherwise, if Alice said that her measurement outcome is in the set \(|1\rangle, |−\rangle\)}, he can guess that the basis that Alice used is \(X\). In this way, he will have success with probability \(3/4\) in obtaining \(o_i\) before the opening phase. However, since the distance between any two
codewords in $C(0)$ and $C(1)$ is $d$, Bob must obtain more than $n - d$ bits to extract valid committed information. So Bob could cheat successfully with probability $\left(\frac{1}{2}\right)^{n-d}$. When $n - d \geq 3$, the probability will be less than $1/2$, which means that the cheating strategy is not better than guessing.

**Cheating method II.** Bob has a more effective cheating strategy. Instead of sending a single photon to Alice, Bob could cheat by sending one particle of an entangled state to Alice. After she has measured it, he measures his particle for analyzing $o_i$. The best thing for him is obtaining the same state as Alice has, i.e., obtaining a photon in state $|0\rangle$ (or $|1\rangle$, or $|+\rangle$, or $|-\rangle$) when $o_i = |0\rangle$ (or $|1\rangle$, or $|+\rangle$, or $|-\rangle$). Then according to $o_i$, he calculates $o_i$ and $c_i$. For these purposes, he should measure the state which is one of $|0\rangle$, $|+\rangle$ to make sure what state it is.

The problem of optimal state estimation has been studied in great detail previously [32] by Helstrom, and in particular the optimal measurement for discriminating between two density operators [33] is well known. Using Helstrom’s optimal measurement, the maximum probability of Bob estimating $c_i$ is

$$p_{\text{max}} = \frac{1}{2} + \frac{1}{4} \text{Tr} \left| \rho_{|0\rangle} - \rho_{|1\rangle} \right| = \frac{1}{2} + \frac{\sqrt{2}}{4}, \quad (3)$$

where $|\rho_{|0\rangle} - \rho_{|1\rangle}|^2 = \left(\rho_{|0\rangle} - \rho_{|1\rangle}\right)^\dagger \left(\rho_{|0\rangle} - \rho_{|1\rangle}\right)$ is the Hermitian conjugate or adjoint of the $\left(\rho_{|0\rangle} - \rho_{|1\rangle}\right)$ matrix. So Bob could obtain $c_i$ with success probability $\frac{1}{2} + \frac{\sqrt{2}}{4}$. Since the distance between any two codewords is $d$, Bob needs to know more than $n - d$ bits to obtain valid information. The probability of obtaining the committed bit correctly is $\left(\frac{1}{2} + \frac{\sqrt{2}}{4}\right)^{n-d}$. When $n - d \geq 5$, the probability will be less than $1/2$, which means that the cheating strategy is no better than guessing.

**Cheating method III.** Bob has another strategy, using conclusive measurement or unambiguous state discrimination (USD) [34, 35]. These measurements have three possible outcomes: $|0\rangle'$, $|+\rangle'$ and $?'$, the latter being called the inconclusive outcome. Whenever the outcome $|0\rangle$ or $|+\rangle$ is obtained, it is guaranteed that the measured state was indeed $|0\rangle$ or $|+\rangle$. Conclusive measurement can distinguish $|0\rangle$ and $|+\rangle$ with conclusive outcome probability $1 - \frac{\sqrt{2}}{2} \approx 29\%$. This means that Bob could obtain about $29n\%$ correct bits from the $n$ states, which could be used to extract the committed bit. Here Bob could also use more than $n - d$ bits to obtain valid information, using an approach like that used in methods I and II. So one should have $\frac{d}{n} < \frac{\sqrt{2}}{2}$ for security. On the other hand, since the outcome bit is correct unambiguously, which is not the same situation as in the cheating methods I and II, Bob could use them to make a judgment efficiently: in the same orders, if the conclusive bits are all the same as a codeword $c'$, he calculates the committed bit with $c' \otimes r$. As the amount of codewords in $C$ is $2^k$, $2^{k-(1-\frac{k}{2})n}$ codewords have the same $29n\%$ bits in the same orders on average. When $k$ is less than or close to $(1 - \frac{\sqrt{2}}{2})n$, the judgment will be effective. But with increasing value of $k - (1 - \frac{\sqrt{2}}{2})n$, Bob’s cheating success probability becomes close to $\frac{1}{2}$.

In a QBC, Bob’s cheating capability is represented as his cheating success probability $\frac{1}{2} + \varepsilon$ where $0 \leq \varepsilon \leq \frac{1}{2}$. Generally, the scheme’s capability of sealing is better with smaller $\varepsilon$. When $\varepsilon = 0$, the QBC protocol is complete sealing, as Bob can only distinguish the committed bit with probability $\frac{1}{2}$ before the opening phase, which is just like guessing. However, as the MLC no-go theorem said that $\varepsilon = 0$ is impossible, we can only design a CSQBC scheme with $\varepsilon \rightarrow 0$. Here, we say that a QBC protocol has approximate sealing if $\varepsilon \rightarrow 0$.
(namely, Bob can only distinguish the committed bit before the opening phase with probability close to \(
\frac{1}{2}
\), which is like guessing, approximately). In the proposed CSQBC, \(\epsilon\) becomes close to 0 with increasing value of \(k - (1 - \frac{\sqrt{2}}{2})n\) under the constraints \(n - d \geq 5\) and \(\frac{d}{n} < \frac{\sqrt{2}}{2}\). Since \(k - (1 - \frac{\sqrt{2}}{2})n\) increases with increasing value of \(n\) normally, this means that Bob can only cheat on the committed bit with probability becoming close to \(\frac{1}{2}\) (i.e., \(\epsilon\) is close to 0) with increasing number of single photons used. In other words, to Bob the QBC presented is approximate sealing.

3.3. Practicability

In the protocol presented, only BB84 states with \(X\) and \(Y\) basis measurements are used, all of which can be implemented with present day technology. In a QBC, the period between the commitment phase and the opening phase may be very long. If quantum states have to be stored during this period, the protocol will be difficult to realize with present day technology. Here, quantum storage is not needed in the proposed QBC. So compared with some protocols in which long-term quantum memories are used, our protocol is more practicable.

Multi-photons present an important problem, which has caused trouble in some practical quantum protocols. Now we analyze the effect on the QBC presented here. In a photon number splitting (PNS) attack [36], Alice uses a quantum non-demolition (QND) measurement to obtain the amount of photons included in the \(i\)th pulse. When the amount is 1, she proceeds with honest processing. But when the amount is no less than 2, she measures one photon in the basis \(X\) and the other (or one of the others) in the basis \(Z\). If the two outcomes happen to be \([0,|+\rangle]\) or \([1,|-\rangle]\), she can cheat as regards \(c_i = 0\) and \(c_i = 1\) easily by announcing \(o_i' = 0\) or \(o_i' = 1\) at step (6) and announcing her wanted \(c\) at step (7). However, if the two outcomes happen to be \([0,|-\rangle]\) or \([1,|+\rangle]\), Alice cannot perform this cheating. Namely, to cheat successfully as regards one orderly pulse, she might perform the cheating on two pulses including multi-photon ones on average. For successful cheating, Alice needs to change \(d/2\) bits in \(c\) at least. So if the multi-photon rate \(\eta_m\) is less than \(\frac{d}{2} \times 2 \times \frac{1}{n} = \frac{d}{n}\), she could not cheat successfully by performing only the PNS attack. For security, Bob should set the multi-photon rate of his source at a small enough value.

Next, we analyze the effect derived from loss, error and the ECC. The loss and error appearing in quantum channels and devices are also important problems in practical quantum protocols. We consider a realistic scenario with the loss rate \(\eta_l\) and the error rate \(\eta_e\). In the protocol, the ECC is used to deal with the error and loss effects. The EC \((n, k, d)\)-code \(C\) uses an \(n\)-bit codeword to encode a \(k\)-bit word, and the distance between any two codewords is \(d\).

We suppose that the ECC can correct \(t\) error bits, where \(t \leq \frac{d-1}{2}\). When loss happens, participants would use random bits to fill the corresponding orders. So each loss bit yields a 1/2 error bit; consequently, the ECC parameter should be set as

\[
    t \geq \left(\frac{\eta_l}{2} + \eta_e\right)n. \tag{4}
\]

Dishonest Alice could take advantage of the redundancy arising from the ECC to extract the committed bit by (i) replacing the channels and devices with loss-free and error-free channels and devices first and (ii) then performing some attacks, which will yield some error bits. The cheating will not be detected when the amount of error bits is no more than \(t\), as the error will be corrected by the ECC.

Now we consider the attack strategy proposed in subsection 3.1, as an example. We consider the worst case, i.e., Alice has the most cheating success probability and there is the
least probability of her cheating being detected. To cheat on one photon, Alice could distinguish the two sets $\{|0\rangle, |+\rangle\}$ and $\{|1\rangle, |-\rangle\}$ successfully with probability at most $\frac{2 + \sqrt{2}}{4} \approx 0.8536$. And her cheating will be detected with probability at least $\frac{1 - (\frac{2 + \sqrt{2}}{4})}{2} \approx 0.0732$ as she distinguished the two sets unsuccessfully. That is, the mutual information that she obtained is $1 - h(0.8536) \approx 0.3992$ bit, where $h(p) = -p \log_2 p - (1 - p) \log_2(1 - p)$ is the binary entropy function. Suppose Alice performed this attack on $r$ states; the information that she obtained was $\frac{\eta_m}{2} n + 0.3992 r$ combined with the information obtained from the PNS attack. We could also use binary entropy to measure the error yielded by the attack. The mutual information of $o_i$ announced by dishonest Alice and its real value is $h(0.0732) \approx 0.3775$. So the error information in $o_i$ will be $0.3775 r$.

Alice should let $0.3775 r \leq t$ (we will consider the worst case of $r = \frac{t}{0.3775}$) to guarantee that her cheating could not be detected, i.e., the error yielded would be corrected by the ECC. So it should be the case that

$$\frac{\eta_m}{2} n + \frac{0.3992}{0.3775} t < \frac{d}{2} \quad (5)$$

to prevent a dishonest Alice from acting in a practical setting. Combining with equation (1d),

$$\frac{\eta_m}{2} n + \frac{0.3992}{0.3775} \left( \frac{1}{2} \eta_l + \eta_e \right) n < \frac{d}{2} \quad (6)$$

is obtained. Then a dishonest Alice could not use the redundancy arising from the ECC to perform her cheating effectively. We give some explanation for equation (3). It indicates that half of the distance ($\frac{d}{2}$) between any codewords should be more than the sum of $\frac{\eta_m}{2} n$ ($\eta_m n$ is the amount of multi-photons), $\frac{0.3992}{0.3775} \cdot \frac{1}{2} \eta_l n$ ($\eta_l n$ is the amount of lost photons) and $\frac{0.3992}{0.3775} \eta_e n$ ($\eta_e n$ is the amount of error photons). $\frac{d}{2}$ indicates that dishonest Alice needs to change $\frac{d}{2}$ bits in $c'$ to alter the committed bit. For each multi-photon, she could cheat on $\frac{1}{2}$ bits successfully without altering the original bits, which gives rise to the coefficient $\frac{1}{2}$. Besides the PNS attack, another cheating strategy, such as what was proposed in subsection 3.1, could be performed simultaneously. But some errors were introduced in the original bits, which gave rise to the coefficient $\frac{0.3992}{0.3775} \cdot \frac{1}{2}$. And the coefficient $\frac{1}{2}$ in front of $\eta_l$ arises from the fact that each loss bit yielded a $\frac{1}{2}$ error bit.

4. Conclusion

To summarize, in this paper, we have dealt with a quantum bit commitment protocol based on single photons. In our scheme, Alice commits a value by performing some measurements on the single photons which were sent from Bob. Bob can only cheat on the committed bit with probability becoming close to 0 as the number of single photons used is increased. On the other hand, if Alice alters her committed bit after the commitment phase, her action will be detected with probability becoming close to 1 as the number of single photons used is increased. This is easy to realize with present day technology.
Acknowledgments

This work was supported by the NSFC (Grant Nos 61272057, 61170270, 61370188, and 61103210) and Beijing Higher Education Young Elite Teacher Project (Grant Nos YETP0475, YETP0477), from the China scholarship council.

References

[1] Brassard G, Chaum D and Crépeau C 1988 Minimum disclosure proofs of knowledge J. Comput. Syst. Sci. 37 156–89
[2] Goldwasser S, Micali S and Rackoff C 1989 The knowledge complexity of interactive proof systems SIAM J. Comput. 18 186–208
[3] Goldreich O, Micali S and Wigderson A 1991 Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems J. ACM 38 691–729
[4] Nascimento J C D and Ramos R V 2010 Quantum protocols for zero-knowledge systems Quantum Inf. Proc 9 37–46
[5] Brassard C and Crépeau G 1991 Quantum bit commitment and coin tossing protocols Advances in Cryptology: Proc. Crypto ’90 (Lecture Notes in Computer Science vol 537) (Berlin: Springer) pp 49–61
[6] Nayak A and Shor P 2003 Bit-commitment-based quantum coin flipping Phys. Rev. A 67 012304
[7] Silman J, Chailloux A, Aharon N, Kerenidis I, Pironio S and Massar S 2011 Fully distrustful quantum bit commitment and coin flipping Phys. Rev. Lett. 106 220501
[8] Bennett C H, Brassard G, Crépeau C and Skubiszewska M H 1991 Advances in Cryptology: Proc. Crypto ’91 (Lecture Notes in Computer Science vol 576) (Berlin: Springer) pp 351–66
[9] He G P and Wang Z D 2006 Oblivious transfer using quantum entanglement Phys. Rev. A 73 012331
[10] Yao A C 1982 Protocols for secure computation Proc. 23rd Ann. IEEE Symp. (Foundations of Computer Science) (Washington, DC: IEEE Computer Society) p 160
[11] Goldreich O, Micali S and Wigderson A 1987 How to play ANY mental game STOC ’87: Proc. 19th Ann. ACM Symp. on Theory of Computing (New York: ACM) pp 218–29
[12] Yang Y G and Wen Q Y 2009 An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement J. Phys. A: Math. Theor. 42 055305
[13] Anders J and Browne D E 2009 Computational power of correlations Phys. Rev. Lett. 102 1–4
[14] Brassard G, Crépeau C, Jozsa R and Langlois D 1993 A quantum bit commitment scheme provably unbreakable by both parties Proc. 34th Ann. IEEE Symp. on Foundations of Computer Science (Los Alamitos, CA: IEEE) pp 362–71
[15] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing Proc. IEEE Int. Conf. on Computers Systems, and Signal Processing (Bangalore, India) (New York: IEEE) 17–179
[16] Lo H K and Chau H F 1999 Unconditional security of quantum key distribution over arbitrarily long distances Science 283 2050
[17] Mayers D 1997 Unconditionally secure quantum bit commitment is impossible Phys. Rev. Lett. 78 3414
[18] Lo H K and Chau H F 1997 Is quantum bit commitment really possible? Phys. Rev. Lett. 78 3410
[19] Li Q, Li C Q, Long D Y, Chan W H and Wu C H 2012 The impossibility of non-static quantum bit commitment between two parties Proc. Quantum Inf. 11 519–27
[20] Hardy L and Kent A 2004 Cheat sensitive quantum bit commitment Phys. Rev. Lett. 92 157901
[21] Shimizu K, Fukasaka H, Tamaki K and Imoto N 2011 Cheat-sensitive commitment of a classical bit coded in a block of m × n round-trip qubits Phys. Rev. A 84 022308
[22] Halvorson H 2004 Remote preparation of arbitrary ensembles and quantum bit commitment J. Math. Phys. 45 4920
[23] He G P 2006 Secure quantum bit commitment against empty promises Phys. Rev. A 74 022332
[24] Choi J W, Hong D, Chang K Y, Chi D P and Lee S 2009 Non-static quantum bit commitment arXiv:0901.1178 [quant-ph]
[25] Wolf S and Wullschleger J 2005 Bit commitment from weak non-locality arXiv:quant-ph/0508233
[26] He G P and Wang Z D 2008 Practically secure quantum bit commitment based on quantum seals arXiv:0804.3531 [quant-ph]
[27] He G P 2011 Quantum key distribution based on orthogonal states allows secure quantum bit commitment J. Phys. A: Math. Theor. 44 445305
[28] Adrian K 2011 Unconditionally secure bit commitment with flying qudits New J. Phys. 13 113015
[29] Yuen H P 2012 An unconditionally secure quantum bit commitment protocol arXiv:1212.0938v1
[30] Danan A and Vaidman L 2012 Practical quantum bit commitment protocol Quantum Inf. Proc 11 769–75
[31] MacWilliams F J and Sloane N J A 1983 The Theory of Error-Correcting Codes (Amsterdam: North-Holland)
[32] Helstrom C W 1976 Quantum Detection and Estimation Theory (New York: Academic)
[33] Fuchs C A 1998 Information gain vs. state disturbance in quantum theory Fortschr. Phys. 46 535–65
[34] Dieks D 1988 Overlap and distinguishability of quantum states Phys. Lett. A 126 303–6
[35] Peres A 1988 How to differentiate between non-orthogonal states Phys. Lett. A 128 19
[36] Huttner B, Imoto N, Gisin N and Mor T 1995 Quantum cryptography with coherent states Phys. Rev. A 51 1863