Cheating Sensitive Security Quantum Bit Commitment with Security Distance Function

Weicong Huang[1(✉)], Qisheng Guang[1], Dong Jiang[2], and Lijun Chen[1(✉)]

[1] State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210046, People's Republic of China
huangwc@smail.nju.edu.cn, chenlj@nju.edu.cn
[2] School of Internet, Anhui University, Hefei 230039, China

Abstract. Quantum bit commitment (QBC) aims to provide a secure commitment between two mutually suspicious parties. This paper presents a new quantum bit commitment protocol by introducing security distance function. Theoretical analysis shows that our protocol can guarantee the qubit commitment process is secure and has better performance than existing protocols in robustness. Since our protocol is simpler and more practical, it is feasible with current technologies.

Keywords: Quantum bit commitment · Security distance function · Cheat sensitive

1 Introduction

The rapid development of quantum computing poses a huge threat to classical cryptographic protocols which rely their security on computational complexity. This also facilitates the growth of quantum cryptography as its security is guaranteed by quantum mechanics, which provides unconditional security. Many classical cryptographic protocols have their quantum counterparts to promote security against both external eavesdropping and internal cheating. Bit commitment, which is first presented by Blum [1], is one of the most fundamental issues in modern cryptography. Since it is associated with many basic concepts in modern cryptography, including coin flipping [1,2], obvious transfer [3,4], and zero-knowledge proof [5–7], and is widely applied in real systems, such as business negotiation, electronic voting, and electronic currency, it has attracted intensive study. The process of bit commitment is generally divided into two phases, namely bit committing phase and unveiling phase. In first phase, the sender Alice chooses a bit c which she wants to commit to the receiver Bob;

W. Huang and Q. Guang—These authors contributed equally to this work.

P. Gladyshev et al. (Eds.): ICDF2C 2021, LNICST 441, pp. 127–138, 2022.
https://doi.org/10.1007/978-3-031-06365-7_8

then she encrypts this bit and sends it to Bob. In the second phase, Alice provides Bob with additional information for decoding, so that Bob gets all the information about c. A good bit commitment protocol should simultaneously satisfy the crucial property of concealing and binding. These two property are core principle of bit commitment protocols. The former means that Bob can't obtain any knowledge about the commit bit c before the unveiling phase. The later signifies that Alice can't modify c after the bit is committed to Bob.

Quantum bit commitment (QBC) protocol was first mentioned by Bennett and Brassard in 1984 [8], in the same article where they put forward the well-known BB84 quantum key distribution protocol. They did not realize their quantum tossing protocol implicated the idea of QBC. However, the protocol has a huge security loophole; that is, Alice can cheat Bob without being detected once she possesses quantum memory. Therefore, several QBC protocols [9,10] have been raised to address this problem. Unfortunately, Mayers *et al.* [11] and Lo and Chau *et al.* [12] respectively proved that unconditionally secure QBC does not exist in 1997. Later the same conclusion was also drawn by Kitaev *et al.* [13] and D'Arian *et al.* [14].

Although absolutely secure QBC does not exist in a general sense, studies over QBC are still favored by researchers. Two mainstream sub-fields have emerged from original QBC: relativistic QBC (RQBC) [15–18] and cheat sensitive QBC (CSQBC) [21–25]. RQBC protocols enhance security by introducing extra physical conditions, i.e., the theory of relativity, among which the most representative one was proposed by Kent in 1998 [15]. Afterwards, many other protocols based on the theory of relativity are discussed [16–18], following experimental demonstrations [19,20]. Though RQBC theoretically achieves unconditional security, it requires strict space-time factors, which are hardly satisfied in real systems, thus impeding the large-scale practical applications of RQBC.

Different from RQBC, CSQBC [21–25] offers a probability model of QBC. Specifically, the other can detect it with non-zero probability when one participant cheats, i.e., any cheating behavior risks will be discovered. Compared with RQBC, CSQBC does not require strict conditions, and consequently is highly practical. As a result, we mainly put our focus on CSQBC. In this paper we put forward a new CSQBC protocol which outperforms state-of-art protocols mainly in the following three aspects. First, the proposed protocol is very subtle, which can detect cheating through the raising of error rate. Second, our protocol is easily implemented by current optical devices, and can withstand certain system defects (there is no need for perfect single photon source, noiseless channel and quantum memory). Third, our protocol is more secure compared with existing CSQBC protocols [21–25]. As is shown in the security analysis, Alice's cheating would induce Bob's measurement error rate increasing by 12.5%, enabling Bob to judge Alice's cheating behavior effectively.

The rest of the paper is organized as follows. In Sect. 2, the definition and construction method of the security distance function is introduced. In Sect. 3, our proposed CSQBC protocol is given. In Sect. 4, the security of the protocol is

analyzed. In Sect. 5, a detailed comparison and evaluation is provided. Finally, a brief conclusion is given.

2 Preliminaries

In order to guarantee the fairness of both parties involved in QBC process, we introduce the definition and construction method of security distance function, which is essential to our protocol.

2.1 Definition of Security Distance Function

Definition 1. *Security distance function.*
Function $f : \{0,1\}^n \to \{0,1\}^n$, $X, Y \in \{0,1\}^n$,

$$f(X) = Y. \tag{1}$$

If for any $X_1, X_2 \in \{0,1\}^n$ $(X_1 \neq X_2)$, *and* $f(X_1) = Y_1, f(X_2) = Y_2$, *we have*

$$d(X_1, X_2) + d(Y_1, Y_2) \geq m, \tag{2}$$

where $d(X, Y)$ *represents the Hamming distance between two binary string* X *and* Y[1], *the function* f *is called as* m*-level security distance function(SDF).*

The SDF is to guarantee a secure distance between different function inputs and outputs. However, in practical applications, due to channel noise, most of the optical pulses may be lost. Based on this, we extend the formal definition of the SDF, so that it can better conform to actual systems.

Definition 2. *Expanded security distance function.*
Function $g : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, $X, Y \in \{0,1\}^n, l \in Z$,

$$g(X, Y) = l. \tag{3}$$

If for any $X_1, X_2 \in \{0,1\}^n$ $(X_1 \neq X_2)$, *and* $g(X_1, Y_1) = g(X_2, Y_2)$, *we have*

$$d(X_1, X_2) + d(Y_1, Y_2) \geq m. \tag{4}$$

The function g *is called as* m*-level expanded security distance function (ESDF).*

[1] Hamming distance between two binary string X and Y is the number of ones in $X \oplus Y$.

2.2 Construction of Security Distance Function

After defining SDF, the next issue is finding an approach to construct SDF. Herein, we introduce how to construct SDF by linear block code (n, k, d), which uses n-bits codeword to encode k-bits message, and the Hamming distance between any two codewords is d.

First, we introduce the construction process of the (n, k) linear block code [28]. Denoting the input message bits by $X = (x_1, x_2, ..., x_k)$, and the encoded block code (output of linear block code) by $Y = (y_1, y_2, ...y_n)$, the block-code bits y_i is calculated by the following equation:

$$y_i = g_{1i}x_1 + g_{2i}x_2 + \cdots + g_{ki}x_k, \tag{5}$$

where $g_{lm}(l = 1, 2, ..., k; m = 1, 2, ..., n)$ are binary coefficients. This definition can be put into a vector-matrix product:

$$Y = (y_1, y_2, ..., y_n) = (x_1, x_2, ..., x_k) \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{pmatrix} = X\tilde{G}. \tag{6}$$

The matrix $\tilde{G}$ is called the generator matrix and

$$\tilde{G} = \left[I_k \middle| P \right] = \left(\begin{array}{cccc|cccc} 1 & 0 & \cdots & 0 & p_{11} & p_{12} & \cdots & p_{1m} \\ 0 & 1 & \cdots & 0 & p_{21} & p_{22} & \cdots & p_{2m} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & p_{k1} & p_{k2} & \cdots & p_{km} \end{array} \right), \tag{7}$$

where I_k is the $k \times k$ identity matrix and P is the $k \times m$ matrix $(m = n - k)$. Defining Y_m as the last m-bit code of Y, i.e. $Y_m = (y_{k+1}, ..., y_n)$, we know

$$Y = \left(X \middle| Y_m \right) = \left(XI_k \middle| XP \right), \tag{8}$$

then we have $Y_m = XP$. Now we can construct a $(2n, n, n/2)$ linear block code according to the construction process of the above linear block code. Suppose the input message is $X = (x_1, x_2, ..., x_n)$, and the encoded block code (output of linear block code) is $Y = (y_1, y_2, ..., y_{2n})$, we can get $Y = X\tilde{G} = X\left(I_n \middle| P_n \right) = \left(X \middle| Y_n \right)$. According to definition of SDF, we define a SDF as

$$Y_n = XP_n, \tag{9}$$

where X is n-bit input, Y_n is n-bit output, and security distance would be $n/2$. A notable example is the Golay code, which is a $(23, 12, 7)$ linear block code with 12 information bits and 11 checking bits. We can extend its check bits to construct $(24, 12, 7)$, with $d \geq \frac{n}{2} = 6$, satisfying the requirement for subsequent security analysis.

3 Quantum Bit Commitment with Security Distance Function

In this section, we will describe the proposed QBC protocol in detail. SDF is employed in our protocol to generate sequence for verification. To improve the practicability of the protocol, we consider both ideal and defective cases.

3.1 QBC with SDF in Ideal Case

In ideal case, let's suppose that: a) Alice has perfect single photon source. b) Bob has infallible detecting devices. c) The transmission channel is noiseless.

The above ensures that any signal sent by Alice, including quantum signals and classic signals, can be accurately received and measured by Bob. Alice will choose a random basis sequence A, to encoded commit bit c, and generate checking string X according to basis sequence and SDF. The specific steps of our idea protocol are described as follows:

Phase 1: Committing Phase

(1) Alice and Bob determine the public security distance function f.
(2) Alice chooses her commit bit c, and selects a random basis string $A = \{a_1, a_2, ..., a_n\}$, which satisfies $c = a_1 \oplus a_2 \oplus ... \oplus a_n$, and $\oplus$ is the XOR operation.
(3) Alice calculates $X = f(A)$, where $X = \{x_1, x_2, ..., x_n\}$. Then she prepares photon sequence $|\phi_{a_i,x_i}\rangle$, where a_i and x_i respectively represent the bases and values of these photon sequence. The photons can be denoted as follows:

$$\begin{aligned} |\phi_{0,0}\rangle &= |0\rangle, \qquad |\phi_{0,1}\rangle = |1\rangle, \\ |\phi_{1,0}\rangle &= |-\rangle, \qquad |\phi_{1,1}\rangle = |+\rangle. \end{aligned} \tag{10}$$

(4) Alice sends $|\phi_{a_i,x_i}\rangle$ to Bob. Bob measures the photons in $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ basis, and records measurement bases as A' and the results as X' (or Bob stores the photons if he has quantum memory).

Phase 2: Unveiling Phase

(5) Alice sends A, X and c to Bob.
(6) Bob compares A' and A. If the bases are the same, the value of X' in corresponding position is identical to X; otherwise, the probability that the value of X' in corresponding position is identical to X is 50%. Or Bob uses basis sequence to measured the photons stored in quantum memory and records the result as X'. Finally, Bob will check whether $c = a_1 \oplus a_2 \oplus ... \oplus a_n$ and $f(A) = X$.
(7) If Alice passes all tests, Bob accepts commitment bit c. Otherwise, Bob judges Alice as a cheater and rejects her.

3.2 QBC with SDF in Defective Case

In actual implementation, due to the imperfection of the single-photon source and the decoherence of the photon propagation by the channel noise, Bob usually does not receive all the light pulses sent by Alice. Therefore, Bob will inform Alice the positions of the light pulses he received by classical channel (synchronized by the clock, e.g., GPS). Then, Alice calculates the commit bit $c = r_1 \oplus r_2 \oplus ... \oplus r_n$ according to the value of the basis in the photon sequence received by Bob. The specific steps of our improved protocol are described as follows:

Phase 1: Committing Phase

(1) Alice and Bob determine the public extended security distance function g.
(2) Alice selects random basis strings $A = \{ a_1, a_2, ..., a_l \}$, and $X = \{x_1, x_2, ..., x_l\}$ $(l >> n)$.
(3) Alice prepares photons $|\phi_{a_i,x_i}\rangle$,and send $|\phi_{a_i,x_i}\rangle$ to Bob.
(4) When Bob receives sufficient photons, he informs Alice the positions of the light pulses he detected.
(5) Alice discards invalid information and part of the data to ensure that the number of information bits is n. Then Alice calculates $c = r_1 \oplus r_2 \oplus ... \oplus r_n$ and $l_a = g(R, X_R)$ and sends l_a to Bob, where $R = \{r_1, r_2, ..., r_n\}$ is the base sequence of remaining photons filtered by Alice and Bob, X_R is the value of remaining photons prepared by Alice.
(6) Bob measures the photons, and records measurement bases as R' and the result as X'_R (or Bob stores the photons if Bob has quantum memory).

Phase 2: Unveiling Phase

(7) Alice sends R, X_R and c to Bob.
(8) Bob compares R' and R. When the basis is same, the values of X in corresponding positions are same, otherwise the probability that X_R is the same is 1/2, or Bob uses basis sequence to measured the photons stored in quantum memory, and records the results as X'_R. Bob will check that whether $c = r_1 \oplus r_2 \oplus ... \oplus r_n$ and $g(R, X_R) = l_a$.
(9) If Alice passes all tests, Bob accepts commitment bit c. Otherwise, Bob rejects Alice and judges Alice as a cheater.

4 Security Analysis

Generally speaking, Bob will always accept the committed bit c, as Bob's checking results are $f(R, X_R) = l_a$, and $X_R = X'_R$, when both Alice and Bob are honest. In fact, quantum bit commitment with SDF is a spacial case of QBC with ESDF. The difference between the two protocols is the method of creating connection between the checking sequence and bases sequence. In QBC with SDF, Alice can determine the checking sequence based on the basis sequence

before sending her photons to Bob. But this checking sequence will be inaccurate when the signal is lost. QBC with ESDF solves this problem. Following we analyze the security of our protocols from two perspectives, concealing and binding.

4.1 Concealing

In concealing stage, we calculated the amount of information obtained by Bob before unveiling phase to analyze concealing of our protocol. For X_R, there is $\frac{1}{2}$ probability for the photon state to be the $|0\rangle$ or $|-\rangle$ if x_i is 0. The density matrix is

$$\rho_0 = \frac{1}{2}(|0\rangle\langle 0| + |-\rangle\langle -|) = \frac{1}{2}\begin{bmatrix} \frac{3}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{bmatrix}. \tag{11}$$

The state will be $|1\rangle$ or $|+\rangle$ with $\frac{1}{2}$ probability if x_i is 1. The density matrix is

$$\rho_1 = \frac{1}{2}(|1\rangle\langle 1| + |+\rangle\langle +|) = \frac{1}{2}\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{3}{2} \end{bmatrix}. \tag{12}$$

Then,

$$\rho = \frac{1}{2}(\rho_0 + \rho_1) = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{13}$$

The Von Neumann entropy (VN entropy) is $S(\rho) = -\rho log_2(\rho) = 1$, and $S(\rho_0) = S(\rho_1) = 0.5983$. The mutual information is

$$H(X_R; X'_R) \leq S(\rho) - \sum_x p_x \rho_x = 0.4017. \tag{14}$$

Therefore, the Holevo bound is 0.4017 and the mutual information $H(X_R; X'_R)$ is bounded by it. Similarly, for R, the state will be $|0\rangle$ or $|1\rangle$ with $\frac{1}{2}$ probability if r_i is 0. The density matrix is

$$\rho_0 = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{15}$$

The state will be $|+\rangle$ or $|-\rangle$ with $\frac{1}{2}$ probability if r_i is 1. The density matrix is

$$\rho_1 = \frac{1}{2}(|+\rangle\langle +| + |-\rangle\langle -|) = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{16}$$

Then,

$$\rho = \frac{1}{2}(\rho_0 + \rho_1) = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{17}$$

The Von Neumann entropy (VN entropy) is $S(\rho) = -\rho log_2(\rho) = 1$, and $S(\rho_0) = S(\rho_1) = 1$. The mutual information is

$$H(R; R') \leq S(\rho) - \sum_x p_x \rho_x = 0. \tag{18}$$

Bob can use positive-operator valued measurement (POVM) to get 40% information of X_R, and 0% for R. Now, we assume that Bob uses POVM to measure Alice's photons, and records measurement results as X'_R. Then he calculates $R' = g^{-1}(X'_R, l_a)$. According to equation (3), for any $R \neq R'$, $g(R, X_R) = g(R', X'_R)$. Due to definition of security distance function, we have

$$d(R, R') + d(X_R, X'_R) \geq m. \tag{19}$$

If $X_R = X'_R$, then $d(X_R, X'_R) = 0$ and $d(R, R') \geq m$; if $X_R \neq X'_R$, then the measurement basis chosen by Alice and Bob must be different, and R must not be equal to R'. Therefore, Bob cannot obtain more information about basis sequence R by using POVM.

4.2 Binding

In binding stage, we will calculate the probability of Alice's successful cheating. Theoretically, Bob cannot guess correct commit bit before unveiling phase in our protocol, but there also exists another question that is how to detect Alice's cheating behavior. Now, we assume that Alice is dishonest and Bob is honest, and analyze how our protocol detects dishonest Alice in a noisy channel.

Any of Alice's cheating methods will be seen as being implemented during the unveiling phase, as any action Alice does during the committing phase is considered a commitment process. We only need to ensure that Bob holds signal states $|\phi_{R,X_R}\rangle$ and connection parameter l_a when the committing phase is completed, where $R = \{r_1, r_2, ..., r_n\}$, $X_R = \{x_1, x_2, ..., x_n\}$ and $l_a = g(R, X_R)$.

Alice prepares $|\phi_{a_i,x_i}\rangle$ and sends to Bob, we assume that Alice's commit bit $c = a_1 \oplus a_2 \oplus ... \oplus a_n = 0$. Now Alice want to modify commit bit c to 1. In fact, Alice can achieve her purpose by modifying odd numbers of basis bits. We denote $k(0 \leq k \leq n)$ as number of basis bits that Alice wants to modify after committing phase. Alice prepares k entangled states as following.

$$|\phi_{AB}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \tag{20}$$

The remaining $n - k$ photons are also single photon pulses. For the entangled states, if Alice and Bob choose the same measurement basis, then the results of the measurement are the same. Defining Alice's and Bob's final basis sequence as R and R', we have $c_0 = \oplus_{i=1}^{n} R_i = 0$, $c_1 = \oplus_{i=1}^{n} R'_i = 1$. Then, we have

$$d(R, R') \leq k. \tag{21}$$

According to definition of ESDF,

$$d(R, R') + d(X_R, X'_R) \geq m, \tag{22}$$

$$d(X_R, X'_R) \geq m - k. \tag{23}$$

When $k < \frac{m}{2}$, we have $d(X_R, X'_R) \geq \frac{m}{2} > k$. Alice's control of k bits will introduce errors more than k bits. Therefore, the probability of Alice being discovered is 1. When $k \geq \frac{m}{2}$, we have

$$min\{d(X_R, X'_R)\} \leq \frac{m}{2}. \tag{24}$$

The probability of successful cheating is $P_A \leq \frac{1}{2^{\frac{m}{2}}}$. Also by calculating channel noisy error, we can get $P_A \leq \frac{1}{2^{\frac{m}{2}-ne_r}}$. Generally, we can set $m = \frac{n}{2}$, then we have $P_A \leq \frac{1}{2^{\frac{n}{4}-ne_r}}$.

4.3 Error Rate Introduced by Alice's Cheating

In the above, we have discussed the probability of Alice's successful cheating, but we did not consider the background noise of the channel. Channel noise can conceal some of Alice's cheating behavior, which is overlooked by some CSQBC protocols [15–18]. In our QBC protocol, Alice's cheating behavior will inevitably lead to an increase of the bit error rate. If the lower bound of Alice's bit error rate is greater than the upper bound of bit error rate induced by channel noise, any Alice's cheating behavior would be discovered. Therefore, we will calculate the lower bound of the bit error rate caused by Alice's cheating behavior.

We define N_x as the number of error bits in sequence X when Bob's measurement bases are equal to Alice's, N_r as the number of bits in sequence X when Bob's measurement bases are equal to Alice's, ans n as the number of information bits of the remaining photons. If Alice and Bob are honest, under the noiseless model, $\frac{N_x}{N_r} = 0$; under the noisy model, Er_{noisy} is defined as the upper bound of channel noise, $\frac{N_x}{N_r} \leq Er_{noisy}$. When Alice is dishonest, Alice prepares k entangled states to roughly cause $\frac{k}{2}$ error bits. When Bob performs the measurement, the probability that the bases same with Alice's is $\frac{1}{2}$. Therefore, the number of error bit N_x introduced by Alice is $\frac{k}{4}$. The number of bits N_r in sequence X is $\frac{n}{2}$. As the result, the error rate introduced by Alice is

$$Er_a = \frac{N_x}{N_r} = \frac{k/4}{n/2} = \frac{k}{2n}. \tag{25}$$

According to the conclusion in the above, the rate of successful cheating is the largest when $k = \frac{m}{2}$.

$$Er_a = \frac{k}{2n} \geq \frac{m}{4n} \tag{26}$$

When the parameter of ESDF is $m = \frac{n}{2}$, we have $Er_a \geq \frac{1}{8}$. Therefore, the error rate will increase by at least 12.5% when Alice cheats and this gives Bob sufficient conditions to judge Alice's legitimacy.

5 Comparison

Following we will compare our protocol with other CSQBC protocols [21–25] and show our protocol is superior to other CSQBC protocols.

The current CSQBC protocols have defects in theory or in practice. H.B *et al.*'s [21] protocol requires quantum memory and quantum computing to

implement, while others CSQBC protocols [22–24] need prefect single photon source, which are both hardly realized with current technologies. Meanwhile, G. He *et al.* [27] demonstrated that in some CSQBC protocols [21–24], Bob can obtain sufficient information before unveiling phase, and deduce the commit bit. However, as discussed in Sect. 4.1, Bob cannot obtain any information about the commit bit before unveiling phase, and he can only speculate it randomly. The probability Bob can correctly guess the commit bit yields 50%. Thus, the security problem does not exist and our protocol is secure.

Li *et al.* [25] also proposed CSQBC based on single photon, in which Bob's successful cheating probability roughly equals the probability that Bob successfully speculates the commit bit, while Alice's successful cheating probability drops with negative exponent, approaching zero when signal length expands. Nevertheless, it needs perfect single photon source as well as noiseless channel. Our protocol reaches Li's security standard, that is when $m = \frac{n}{2}$, the probability of Alice successful cheating is $P_A = \frac{1}{2^{(\frac{1}{4}-e_r)n}}$, and the probability of Bob successful cheating is $P_B = \frac{1}{2}$. Besides, in the case of channel noise and signal loss, our protocol is compatible to most QKD protocols.

Meanwhile, Zhou *et al.* [26] proposed CSQBC based on Bell states. Here, we address some problems in its security analysis. The lower-bound of P_B should be $\frac{1}{2}$; Bob can randomly guess the commit bit with probability $\frac{1}{2}$ even if Bob does not cheat. However, the P_B defined in Zhou *et al.*'s seems unfair for other CSQBC protocols. Moreover, the probability of Alice's successful cheating should be $\frac{1}{2}$; Alice can cheat Bob by randomly modifying any b_i.

Table 1 shows the comparisons between our protocol and other protocols in different aspects. According to it, we can conclude that our protocol outperforms others in security, robustness, and practicability.

Table 1. Comparison between our protocol and other protocols in different aspects. P_A: the probability of Alice successful cheating; P_B: the probability of Bob successful cheating; Signal: S, single state; B, Bell state. PC, need of perfect channel; SP, need of single photon source: Y, yes; N, no. OTR: other technical requirements: QM, quantum memory; QC, quantum computing.

Protocol	P_A	P_B	Signal	PC	SP	OTR
H. B et al.	–	≥ 0.5	S	Y	N	QM, QC
other CSQBC	–	≥ 0.5	–	Y	Y	–
Li et al.	$(\frac{6+\sqrt{2}}{8})^{\frac{n}{2}}$	≥ 0.5	S	–	Y	–
L. Zhou et al.	$\frac{1}{2^n}$	$\frac{1}{8^n}(\geq 0.5)$	B	Y	Y	–
Ours	$\frac{1}{2^{\frac{n}{4}-ne_r}}$	0.5	S	N	N	–

6 Conclusion

In this paper, we propose a quantum bit commitment protocol with security distance function, which is simpler and more secure than the existing quantum bit commitment protocols. Similar to the BB84 quantum key distribution protocol, our quantum bit commitment protocol utilizes the receiver's error rate to detect sender's cheating behavior. Theoretical analysis shows that our protocol can guarantee a secure quantum bit commitment process, and have better performance. Since our protocol has considered the ideal and the defective situations, it is robust and feasible with the current technologies.

Acknowledgments. This research is financially supported by the National Key Research and Development Program of China (Grant No. 2017YFA0303704), the Major Program of National Natural Science Foundation of China (Grants No. 11690030 and No. 11690032), the National Natural Science Foundation of China (Grant No. 61771236), the Natural Science Foundation of Jiangsu Province (Grant No. BK20190297) and Nanjing University Innovation Program for PhD candidate.

References

1. Blum, M.: Coin flipping by telephone a protocol for solving impossible problems. SIGACT News **15**(1), 23–27 (1983)
2. Kak, S.C.: A new method for coin flipping by telephone. Cryptologia **13**(1), 73–78 (1989)
3. Wei, C.Y., Cai, X.Q., Liu, B., Wang, T.Y., Gao, F.: A generic construction of quantum-oblivious-key-transfer-based private query with ideal database security and zero failure. IEEE Trans. Comput. **67**(1), 2–8 (2017)
4. Chou, Y.H., Zeng, G.J., Kuo, S.Y.: One-out-of-two quantum oblivious transfer based on nonorthogonal states. Sci. Rep. **8**(1), 15927 (2018)
5. Watrous, J.: Zero-knowledge against quantum attacks. SIAM J. Comput. **39**(1), 25–58 (2009)
6. Watrous, J.: Limits on the power of quantum statistical zero-knowledge. In: The 43rd Annual IEEE Symposium on Foundations of Computer Science, Proceedings, pp. 459–468. IEEE (2002)
7. Aharonov, D., Ta-Shma, A., Ta-Shma, A.: Adiabatic quantum state generation and statistical zero knowledge. In: Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing, pp. 20–29. ACM (2003)
8. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. Theor. Comput. Sci. **560**(12), 7–11 (2014)
9. Brassard, G., et al.: A quantum bit commitment scheme provably unbreakable by both parties. In: Symposium on Foundations of Computer Science (1993)
10. Brassard, G., Crpeau, C.: Quantum bit commitment and coin tossing protocols. Lect. Notes Comput. Sci. **537**, 49–61 (1990)
11. Mayers, D.: Unconditionally secure quantum bit commitment is impossible. Phys. Rev. Lett. **78**(17), 3414 (1997)
12. Lo, H.K., Chau, H.F.: Is quantum bit commitment really possible? Phys. Rev. Lett. **78**(17), 3410 (1997)
13. Kitaev, A., Mayers, D., Preskill, J.: Superselection rules and quantum protocols. Phys. Rev. A **69**(5), 052326 (2004)

14. D'Ariano, G.M., et al.: Reexamination of quantum bit commitment: the possible and the impossible. Phys. Rev. A **76**(3), 032328 (2007)
15. Kent, A.: Unconditionally secure bit commitment. Phys. Rev. Lett. **83**(7), 1447 (1999)
16. Kent, A.: Unconditionally secure bit commitment by transmitting measurement outcomes. Phys. Rev. Lett. **109**(13), 130501 (2012)
17. Kent, A.: Unconditionally secure bit commitment with flying qudits. New J. Phys. **13**(11), 113015 (2011)
18. Kent, A.: Secure classical bit commitment using fixed capacity communication channels. J. Cryptol. **18**(4), 313–335 (2005)
19. Hardy, L., Kent, A.: Cheat sensitive quantum bit commitment. Phys. Rev. Lett. **92**(15), 157901 (2004)
20. Buhrman, H., et al.: Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment. Phys. Rev. **78**(2), 022316 (2008)
21. Li, Y.-B., Wen, Q.-Y., Li, Z.-C., Qin, S.-J., Yang, Y.-T.: Cheat sensitive quantum bit commitment via pre- and post-selected quantum states. Quantum Inf. Process. **13**(1), 141–149 (2013)
22. Shimizu, K., et al.: Cheat-sensitive commitment of a classical bit coded in a block of m × n round-trip qubits. Phys. Rev. A **84**(2), 022308 (2011)
23. Li, Y.B., et al.: Quantum bit commitment with cheat sensitive binding and approximate sealing. J. Phys. A Math. Theor. **48**(13), 135302 (2015)
24. Lunghi, T., et al.: Experimental bit commitment based on quantum communication and special relativity. Phys. Rev. Lett. **111**(18), 180504 (2013)
25. Liu, Y., et al.: Experimental unconditionally secure bit commitment. Phys. Rev. Lett. **112**(1), 010504 (2014)
26. Desurvire, E.: Classical and Quantum Information Theory. Science Press (2013)
27. He, G.P.: Security bound of cheat sensitive quantum bit commitment. Sci. Rep. **5**, 9398 (2015)
28. Zhou, L., et al.: Game theoretic security of quantum bit commitment. Inf. Sci. **479**, 503–514, 135302 (2019)