Cheat-sensitive commitment of a classical bit coded in a block of $m \times n$ round-trip qubits

Kaoru Shimizu,[1,*] Hiroyuki Fukasaka,[1,†] Kiyoshi Tamaki,[1,2] and Nobuyuki Imoto[3]

[1]*NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan*

[2]*National Institute of Information and Communications Technology (NICT), 4-2-1 Nukui-kitamachi, Koganei, Tokyo 184-8795, Japan*

[3]*Graduate School of Engineering Science, Osaka University, 1-3 Machikaneyama-cho, Toyonaka, Osaka 560-8531, Japan*

(Received 17 February 2011; published 4 August 2011)

This paper proposes a quantum protocol for a cheat-sensitive commitment of a classical bit. Alice, the receiver of the bit, can examine dishonest Bob, who changes or postpones his choice. Bob, the sender of the bit, can examine dishonest Alice, who violates concealment. For each round-trip case, Alice sends one of two spin states $|S\pm\rangle$ by choosing basis S at random from two conjugate bases X and Y. Bob chooses basis $C \in \{X,Y\}$ to perform a measurement and returns a resultant state $|C\pm\rangle$. Alice then performs a measurement with the other basis R ($\neq S$) and obtains an outcome $|R\pm\rangle$. In the opening phase, she can discover dishonest Bob, who unveils a wrong basis with a faked spin state, or Bob can discover dishonest Alice, who infers basis C but destroys $|C\pm\rangle$ by setting R to be identical to S in the commitment phase. If a classical bit is coded in a block of $m \times n$ qubit particles, impartial examinations and probabilistic security criteria can be achieved.

DOI: 10.1103/PhysRevA.84.022308 PACS number(s): 03.67.Dd, 03.67.Mn, 03.65.Ud

I. INTRODUCTION

As exhibited by the fruitful research activities undertaken since 1984 [1], quantum cryptography has attracted the attention of both physicists and information scientists. The most successful area of research has been quantum key distribution (QKD), where the laws of quantum mechanics, including the uncertainty principle, make it possible for two distant cooperative parties, Alice and Bob, to share secure random numbers [2].

In addition to QKD, several two-party computation protocols [3], such as bit commitment (BC) [4–7], oblivious transfer (OT), and coin flipping (CF) [8], have been studied in the quantum cryptography field. The difficulties in the above tasks are attributed to the assumption that Alice and Bob do not trust each other. Unlike QKD, quantum mechanics seems not to provide us with a security solution to those tasks beyond the computational complexity argument [3]. In fact, it has been proven that unconditionally secure BC and OT are impossible even if information is processed with a quantum object. The only exception is quantum weak or biased coin flipping, which is claimed to be unconditionally secure [9–12].

Our interest in this work is focused on a BC task that we describe below. In the commitment phase of BC, Bob chooses the bit u and computes the function $f = F(u;K)$ of u with the key K. He only informs Alice of f so that u can be concealed from her (concealment). In the subsequent opening phase, he notifies her of K so that she can compute u inversely. Here u must be bound to f (binding) so that Bob cannot change u from the initial value by notifying Alice of a different key K'. The no-go theorem of quantum BC relies on the fact that perfect concealment requiring $\rho_0 = \rho_1$ results in complete violation of the binding [4–7], where ρ_u ($u = 0,1$) denotes the density matrix relevant to the commitment bit value u. There have been some other quantum protocols proposed for two-party computation [13–15].

Nevertheless, there is still an open question as regards the possibility of realizing quantum protocols for cheat-sensitive BC (CSBC) [16,17]. The CSBC protocol abandons guaranteed concealment. However, this protocol enables honest Bob to detect violation of the concealment with an arbitrarily high probability. With regard to binding, Alice can detect dishonest Bob if (i) he changes u from its initial value or (ii) he postpones deciding u until the opening phase such that he can choose u in a deterministic way to be profitable for him. As the CSBC protocol does not require the condition $\rho_0 = \rho_1$, the no-go theorem of quantum BC tells us nothing about CSBC.

It has been claimed [11] that secure CSBC is possible through the combined use of a quantum bit escrow and quantum weak coin flipping (WCF) [16]. The bit escrow protocol provides one of two different examination cases. Case (I): Alice detects dishonest Bob with a finite probability P_A when he tries to violate the binding of u. Case (II): Bob detects dishonest Alice with a finite probability P_B when she attempts to violate the concealment of u.

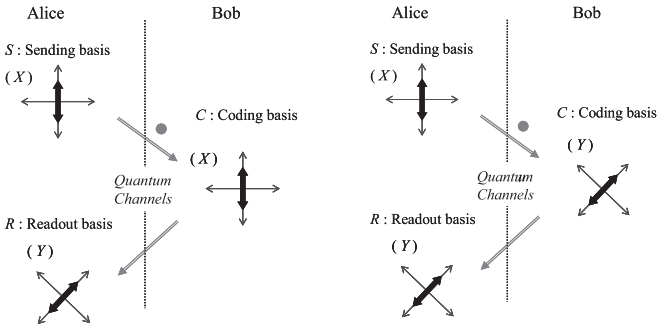
Although the two examination cases are mutually exclusive, they can determine an examiner and an examinee in an impartial way by employing the quantum WCF protocol [9–12]. Recently, however, a security loophole has been claimed for the above framework unless the bit escrow protocol is independent of the WCF protocol [18]. To avoid such loopholes, we must take a different approach to ensure Alice's and Bob's impartiality.

This paper proposes an alternative CSBC framework based on $m \times n$ repetitions of an appropriate quantum bit escrow protocol with a round trip of a qubit particle. We also study the probabilistic security against some cheating strategies.

This paper is organized as follows. Section II proposes the quantum bit escrow protocol, which is the building block of our CSBC protocol. Section III describes the minimal CSBC protocol. Section IV analyzes security aspects of the CSBC protocol in a more general framework considering the entanglement-assisted operations of Bob and Alice. It provides us with a suggestion that the security might be attributed

*shimizu.kaoru@lab. ntt.co.jp.

†Present affiliation: Accenture Technology Solution Co., Ltd.



(a) $S = C \neq R$ case (b) $S \neq C = R$ case

FIG. 1. Legitimate arrangements for sending (S) and readout basis (R), and subsequent changes in the qubit spin state.

to the complementary relationships between the spin angular momentum of a composite system and that of the individual particle. Finally, Sec. V is devoted to a summary.

II. BIT ESCROW PROTOCOL WITH A ROUND-TRIP QUBIT

In this section, we propose the bit escrow protocol that is the building block of our CSBC protocol, where $X = \{|X+\rangle,|X-\rangle\}$ and $Y = \{|Y+\rangle,|Y-\rangle\}$ indicate a pair of conjugate bases that are related with each other through $|Y\pm\rangle = \{(1 \pm i)|X+\rangle + (1 \mp i)|X-\rangle\}/2$. First, Alice sends one of two spin states $|S\pm\rangle$ by choosing basis S at random from two conjugate bases X and Y. Next, Bob decides basis $C \in \{X,Y\}$ to perform a projection measurement and returns a resultant state $|C\pm\rangle$. Alice then performs a projection measurement with the other basis R ($\neq S$) and obtains an outcome $|R\pm\rangle$. Figure 1 illustrates our basic idea, in which Alice always sets the readout basis R being conjugate to the sending basis S. As shown in Fig. 1, the different arrangements in the sending (S) and readout (R) bases afford her no information on his chosen basis C. If Bob's coding basis C is the same as S, his resultant coded state $|B_C\rangle$ is identical to her transmitted state $|A_S\rangle$. If Bob's coding basis C is the same as R, his coded state $|B_C\rangle$ is identical to her measurement outcome $|A_R\rangle$. Thus Alice can always specify Bob' coded state $|B_C\rangle$ after Bob opened his coding basis C.

We detail the protocol in the following:

A. Commitment phase

Step 1. Alice prepares a carrier particle b of a qubit. She selects a sending basis $S \in \{X,Y\}$ at random and then randomly chooses a spin state $|A_S\rangle \in \{|S+\rangle,|S-\rangle\}$. She records the state choice in a classical register, and then sends particle b to Bob.

Step 2. Bob decides his commitment bit $u \in \{0,1\}$. Before measuring particle b, he assigns a coding basis $C \in \{X,Y\}$ in accordance with their consensus that $u = 0$ and 1 correspond to $C = X$ and Y, respectively. With the coding basis C, Bob performs the projection measurement and obtains one of the measurement outcomes $|B_C\rangle \in \{|C+\rangle,|C-\rangle\}$. He defines $|B_C\rangle$ as his coded state and then returns particle b to Alice.

Step 3. Alice performs a projection measurement for particle b with a certain readout basis $R \in \{Y,X\}$, which must be different from the sending basis S ($R \neq S$). She records the result $|A_R\rangle \in \{|R+\rangle,|R-\rangle\}$ in her register.

Table I summarizes the relationships between Alice's registration patterns ($|A_S\rangle,|A_R\rangle$) with $S \neq R$ and Bob's coded states $|B_C\rangle$ with basis $C \in \{X,Y\}$.

B. Opening phase

There are two exclusive cases in the opening phase. In case (I), Alice is an examiner and Bob is an examinee. In case (II), Bob is an examiner and Alice is an examinee. In the description of the protocol below, we assume that both parties are honest unless otherwise stated. First, we describe case (I).

1. Opening phase, case (I): Alice is an examiner

Step 4a. Bob decides a bit $v \in \{0,1\}$ that is identical to u and takes basis $\tilde{C} \in \{X,Y\}$ in such way that $v = 0$ and 1 correspond to $\tilde{C} = X$ and Y, respectively. He first unveils v ($=u$), that is, $\tilde{C}(=C)$.

Step 5a. Alice temporally considers Bob's coded state to be $|\mathrm{A}_{\tilde{C}}\rangle$, which is identical to $|A_S\rangle$ or $|A_R\rangle$ when $\tilde{C} = S$ ($\neq R$) or $\tilde{C} = R$ ($\neq S$).

Step 6a. Bob then opens his state $|\mathrm{B}_{\tilde{C}}\rangle(=|B_C\rangle)$.

Step 7a. If Alice can confirm the coincidence $|\mathrm{B}_{\tilde{C}}\rangle = |\mathrm{A}_{\tilde{C}}\rangle$, she accepts the unveiled bit v to be identical to the commitment bit u. Otherwise, she rejects v.

As Table I shows, when Bob opens his selected basis C, Alice can assert his state $|C\pm\rangle$ correctly. Hence he can always pass the examination in step 7a.

TABLE I. Alice's assertion for Bob's spin state $|\pm\rangle$ depending on his notification of the coding basis C.

				Bob's notification of the basis C coding basis $C \in \{X,Y\}$	
	Alice's or Bob's state $\|\pm\rangle$	Alice's transmitted spin state $\|\pm\rangle$	Alice's readout spin state $\|\pm\rangle$ ($R \neq S$)	When Bob was notified of the X basis	When Bob was notified of the Y basis
Alice's registration patterns	P	$\|Y+\rangle$	$\|X+\rangle$	+	+
	q	$\|Y-\rangle$	$\|X-\rangle$	−	−
	r	$\|Y-\rangle$	$\|X+\rangle$	+	−
	s	$\|Y+\rangle$	$\|X-\rangle$	−	+
	p'	$\|X+\rangle$	$\|Y+\rangle$	+	+
	q'	$\|X-\rangle$	$\|Y-\rangle$	−	−
	r'	$\|X+\rangle$	$\|Y+\rangle$	+	−
	s'	$\|X-\rangle$	$\|Y-\rangle$	−	+

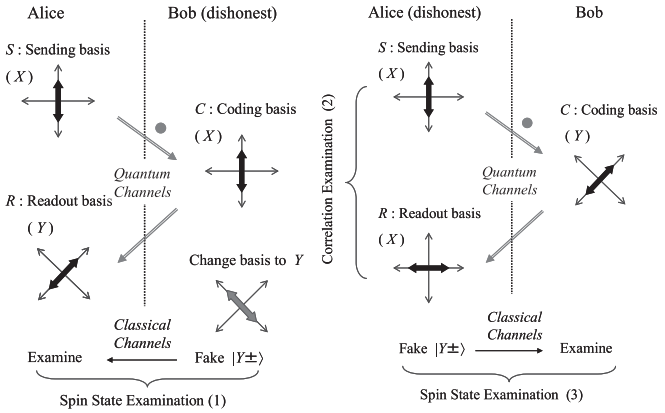


FIG. 2. Schematic diagram showing the detection of a dishonest party. (1) Alice can detect dishonest, Bob who changes the basis (C) from Y to X. (2) Dishonest Alice can find Bob's coding basis as Y. (3) Dishonest Alice fails to answer the spin state $|C\pm\rangle$.

However, if Bob dishonestly changes his mind ($\tilde{C} \neq C$) and fakes the spin state when he reveals $|\mathrm{B}_{\tilde{C}}\rangle$ in step 4a, Alice can detect him with a $1/2$ probability. This point is apparent from Table I and Fig. 2(a). Suppose that (i) he obtains $|X+\rangle_b$ and returns it in step 2, (ii) he changes his mind and announces a Y basis in step 4a, and (iii) he notifies her of $|Y+\rangle_b$ in step 6a. From (i), he can surely narrow down Alice's eight registration patterns to four patterns p, r, p', and r' in Table I. Nevertheless, he cannot specify the correct pattern that she obtained in the commitment phase. If she obtained r or r', he is detected in step 7a.

Next we describe case (II).

2. *Opening phase, case (II): Bob is an examiner*

Step 4b. Bob opens bit u with the corresponding basis C.

Step 5b. Alice deduces that Bob's coded state is $|A_C\rangle = |A_S\rangle$ if $C = S\ (\neq R)$ or $|A_C\rangle = |A_R\rangle$ if $C = R\ (\neq S)$.

Step 6b. Alice notifies Bob of $|A_C\rangle$.

Step 7b. Bob checks the coincidence $|A_C\rangle = |B_C\rangle$. If $|A_C\rangle \neq |B_C\rangle$, he aborts.

Honest Alice can always pass the examination, whereas she does not know u until he opens it.

However, Alice can dishonestly violate the concealment of u with a finite probability in the commitment phase if she sets illegitimately the readout basis R to be identical to the sending basis S ($R = S$) as shown in Fig. 2(b). If she finds an anticoincidence $|A_R\rangle \neq |A_S\rangle$ in the spin states, which occurs with a $1/4$ probability, she can assert that the coding basis C is different from the sending basis $[C \neq (S = R)]$ and specify the commitment bit u. However, she fails to pass step 7b with a finite probability. This is because her illegitimate access with the mismatched basis $R \neq C$ destroys Bob's coded state $|B_C\rangle$ and she must fake $|A_C\rangle$ in step 6b. The probability P_B that Bob detects dishonest Alice is $1/4$, which is the product of the probabilities of $C \neq (S = R)$ and $|B_C\rangle \neq |A_C\rangle$.

Even if dishonest Alice finds the coincidence $|A_R\rangle = |A_S\rangle$, she can guess $C = (S = R)$ with a $2/3$ $\{= (1/2)/[1-(1/4)])\}$ probability, where $1/2$ and $1/4$ indicate the probabilities of $C = (S = R)$ and $|A_R\rangle \neq |A_S\rangle$, respectively. When $C \neq (S = R)$ holds under the condition $|A_R\rangle = |A_S\rangle$, Bob can detect her failure with a $1/2$ probability. Hence P_B is estimated as $1/6$ $\{=(1/2) \times [1 - (2/3)]\}$ in the above case.

The proposed bit escrow protocol does not require any quantum memory for storing the quantum state. This feature is a great advantage from a practical point of view. It may be worth mentioning that the round-trip transmission is not the only possible implementation for our CSBC protocol. For example, the round trip of a qubit can be replaced with a pair of one-way quantum communications from Bob to Alice provided that (i) Bob prepares the spin states $|B_C\rangle$ of the first and second qubits such that they are identical, and (ii) Alice employs different readout bases for those two qubits.

III. MINIMAL CSBC PROTOCOL

A. Coding in a block of $m \times n$ qubit particles

This subsection describes how $m \times n$ repetitions of the quantum bit escrow protocol can provide impartiality between Alice and Bob when one examines the other. Suppose that Bob decides the commitment bit $Z \in \{0,1\}$ and then chooses m different subordinate bits u^i $(i = 1 \sim m) \in \{0,1\}$ in such a way that their parity corresponds to his commitment bit Z; $\oplus_{i=1}^{m} u^i = Z$. In this case, dishonest Alice must assert all m subordinate bits in order to determine Z in the commitment phase. This increases the number of incorrect answers caught by Bob in step 7b.

In the above scheme, however, dishonest Bob can violate the binding of Z by changing only one subordinate bit, and then Alice fails in detecting him with a $1/2$ probability. To improve Alice's probability P_A of detecting dishonest Bob in step 7a, we propose a protocol in which each subordinate bit u^i has to be coded by Bob with a sequence of n different qubits b^{ij} $(j = 1 \sim n)$. Here all n qubits belonging to the same ith sequence are measured by Bob with an identical coding basis $C^i = X$ or Y, depending on $u^i = 0$ or 1. This forces dishonest Bob to fake quantum states $|\mathrm{B}_{\tilde{C}}\rangle^{ij}$ of all n qubits b^{ij} $(j = 1 \sim n)$ in step 6a when he changes the subordinate bit from u^i to v^i $(\neq u^i)$. This increases the incorrect answers caught by Alice in step 7a. In the following, we take the numbers m and n sufficiently large to enable us to ignore the statistical fluctuation.

B. Minimal CSBC protocol executed by honest parties

Here we first describe a scenario that assumes both Alice and Bob to be honest. Before running the protocol, they agree on the numbers m and n. They also decide the positive security parameter $\kappa < 1/3$, which determines the numbers κn and $(1-\kappa)n$ of test particles per sequence examined by Bob and Alice, respectively. The parameter value of κ is derived from the security analysis in Sec. IV B. For simplicity, we assume here a loss and error-free transmission of particles through quantum channels. The protocol is tolerant of the transmission loss, as mentioned in Appendix A.

1. *Commitment phase*

Step 1. Alice prepares a set of $m \times n$ carrier particles b^{ij} $(i = 1 \sim m, j = 1 \sim n)$ consisting of qubits. Address i specifies one of the m different sequences composed of n particles and

address j locates one of the n different particles belonging to the ith sequence. For each particle, she selects the sending basis $S^{ij} \in \{X,Y\}$ at random and then chooses the transmitted state $|A_S\rangle^{ij} \in \{|S+\rangle,|S-\rangle\}$ in a random way. She sends all b^{ij} particles to Bob.

Step 2. Bob chooses m different subordinate bits u^i $(i = 1 \sim m) \in \{0,1\}$ such that their parity $\oplus_{i=1}^m u^i$ represents his commitment bit $Z \in \{0,1\}$. He repeats the following substeps for the different sequences from $i = 1$ to $i = m$. (i) He assigns the coding basis C^i $(= C^{ij}) \in \{X,Y\}$ for all j $(=1 \sim n)$ particles belonging to the ith sequence such that $u^i = 0$ and 1 correspond to $C^i = X$ and Y, respectively. (ii) With the coding basis C^i, he performs the projection measurement for each particle b^{ij} and obtains the sequence of the measurement outcome $|B_C\rangle^{ij}$ $(j = 1 \sim n) \in \{|C^i+\rangle,|C^i-\rangle\}$. He defines $|B_C\rangle^{ij}$ as his coded state. (iii) He returns particles b^{ij} $(j = 1 \sim n)$ to Alice.

Step 3. For each particle, Alice performs a projection measurement with a certain readout basis $R^{ij} \in \{Y,X\}$ that must be different from the sending basis S^{ij}. She records the sequences of her measurement results $|A_R\rangle^{ij} \in \{|R+\rangle,|R-\rangle\}$, where $i = 1 \sim m$ and $j = 1 \sim n$.

Next we describe the protocol for the opening phase, in which we assume that both parties are honest.

2. Opening phase

Step 4. First, Bob opens his commitment bit Z. For all different sequences from $i = 1$ to $i = m$, he then unveils the subordinate bit $u^i \in \{0,1\}$, which is the coding basis $C^i \in \{X,Y\}$.

Step 5. For each particle b^{ij} of the ith sequence $(j = 1 \sim n)$, Alice redefines $|A_C\rangle^{ij}$ to be identical to the transmitted state $|A_S\rangle^{ij}$ if $C^i = S^{ij}$ $(\neq R^{ij})$, or to be identical to the resultant state $|A_R\rangle^{ij}$ if $C^i = R^{ij}$ $(\neq S^{ij})$.

Step 6. For each sequence, Bob samples an arbitrary set of κn $(\kappa < 1/3)$ particles at random to use them as test particles for detecting dishonest Alice, and he notifies Alice of the locations.

Step 7. For each sequence, Alice answers him with her deduced state $|A_C\rangle^{ij}$ for κn test particles.

Step 8. For each sequence, Bob examines the coincidence $|A_C\rangle^{ij} = |B_C\rangle^{ij}$ for all κn particles. Since Alice receives m different sequences composed of n particles, the total number of his test particles is $m \times (\kappa n)$. Unless he finds an anticoincidence $|A_C\rangle^{ij} \neq |B_C\rangle^{ij}$ in the spin states, he regards Alice as honest and tells her to move on to the next step. Otherwise, he aborts.

Step 9. For each sequence, Bob unveils his coded state $|B_C\rangle^{ij}$ for all $(1-\kappa)n$ remaining particles.

Step 10. For each sequence, Alice examines the coincidence $|B_C\rangle^{ij} = |A_C\rangle^{ij}$ for those $(1-\kappa)n$ particles, which she employs as test particles. She repeats the examination for every different sequence from $i = 1$ to $i = m$. If she detects no errors, she accepts his commitment bit Z. Otherwise she rejects the bit Z.

C. Bob's violation of the binding and Alice's detection

This section analyzes two typical strategies of dishonest Bob. One is mind-change strategy and the other is postponing strategy. Alice can detect dishonest Bob provided that the security parameter κ is chosen to be an appropriate value.

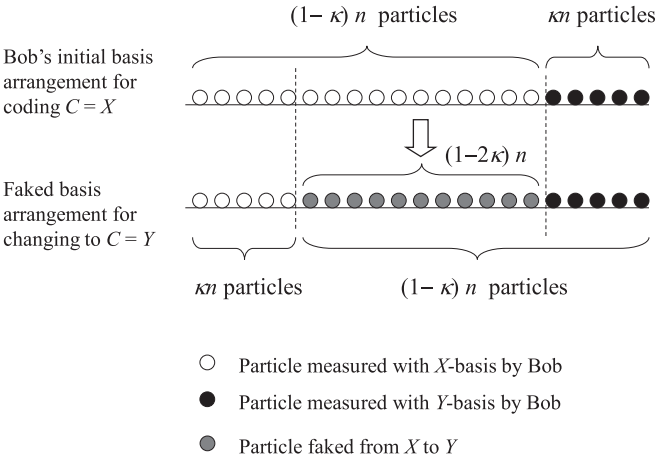


FIG. 3. Strategy of dishonest Bob, who tries to change his coding basis for one sequence.

1. Mind-change strategy

If dishonest Bob arbitrarily changes one of the m subordinate bits u^i $(i = 1 \sim m)$ in step 4 to invert the commitment bit $Z = \oplus_{i=1}^m u^i$, Alice can detect him in step 10. Suppose that he changes the hth subordinate bit u^h and fakes the coding basis C^h for the hth sequence. He can always conceal from Alice arbitrary κn particles that he does not want to be examined in step 10. This is because it is he who decides κn test particles in step 6, which can be dependent on the basis that he unveiled in step 4. Therefore, it is sufficient for him to fake the spin state $|B_C\rangle^{hj}$ for $(1-2\kappa)n$ particles rather than $(1-\kappa)n$ as illustrated in Fig. 3. Apparently, the protocol does not work when $\kappa \geqslant 1/2$. Furthermore, Sec. IV B reveals the sufficient condition $\kappa < 1/3$. The probability that he can escape her detection is estimated as $(1/2)^{(1-2\kappa)n}$, and the probability P_A that Alice can detect him is given by

$$P_{A(\text{mind change})} \sim 1 - (1/2)^{(1-2k)n} \quad \text{with} \quad k < 1/3. \qquad (1)$$

2. Postponing strategy

Another strategy of dishonest Bob is to postpone his decision of the commitment bit until the opening phase. Suppose that (i) he measures the two different half subsets of the n particles with X and Y bases, respectively, in the commitment phase, and (ii) he decides to declare an X or Y basis in the opening phase. In this case, he can escape Alice's detection for $n/2$ particles. Hence, the probability $P_{A\,(\text{postpone I})}$ is given by $\sim 1-(1/2)^{(1/2-\kappa)n}$ with $\kappa < 1/3$ and is smaller than $P_{A\ (\text{mindchange})}$. However, unlike the mind-change strategy, he is detected regardless of his later choices X and Y.

Another postponing strategy is as follows. We should note that Bob can guess Alice's registration patterns $(|A_S\rangle,|A_R\rangle)$ with $S \neq R$ summarized in Table I with finite probabilities. Suppose that (i) Bob measures particle b with the Y basis and obtains the outcome $|Y+\rangle$, and (ii) he returns particle b being in $|X+\rangle$. He can then evaluate the probabilities that she obtains the eight patterns $\{p,q,r,s,p',q',r',s'\}$

as $\{1/2,0,0,0,1/8,1/8,1/8,1/8\}$. He can expect a $3/4$ $\{=[(1/2)\times 1]+4\times[(1/8)\times(1/2)]\}$ probability of success in the postpone strategy by answering $|X+\rangle$ (or $|Y+\rangle$) in step 9 when he unveils $C^i = X$ (or $C^i = Y$) in step 4. Therefore, the probability P_A that Alice can detect this postpone strategy is given by

$$P_{A(\text{postpone II})} \sim 1-(3/4)^{(1-2k)n} \text{ with } k < 1/3. \quad (2)$$

The postpone strategy II is slightly beneficial for dishonest Bob.

Section IV B discusses security against dishonest Bob in a general framework considering entanglement-assisted attacks. It will be clarified that the κ value must be sufficiently less than $1/3$.

D. Alice's violation of the concealment and Bob's detection

This subsection is devoted to Alice's straightforward strategy when she attempts to violate the concealment of the commitment bit Z. She can certainly assert $Z = \oplus_{i=1}^{m} u^i$ if she reads out all m subordinate bits u^i or coding bases C^i $(i = 1\sim m)$ from her illegitimate access to the particles. For each particle, she concludes the coding basis C with a $1/4$ probability by the access with the readout basis R identical to the sending basis S $(R = S)$ as illustrated in Fig. 2(b). Since all n particles belonging to the same sequence are measured by Bob with an identical coding basis in step 2, Alice stops the illegitimate access once she succeeds to reveal his coding basis C. From those accesses with an illegitimate basis arrangement $R^{ij} = S^{ij} = X$, she mostly finds out $C^i = Y$ if Bob assigned $C^i = Y$. In the same way, from her accesses with another illegitimate basis arrangement $R^{ik} = S^{ik} = Y$, she knows $C^i = X$ if he assigned $C^i = X$. Hence she can determine all u^i $(i = 1\sim m)$ with a high probability, whereas it is impossible for her to completely avoid leaving evidence of her illegitimate accesses for all m sequences.

However, if she compromises not to determine all u^i but to guess some of them with a high probability, there is a strategy that reduces significantly the total times of the illegitimate access that is detectable by Bob in step 8. The strategy is as follows: (i) For each sequence, $i = 1,2,\ldots,m$, she fixes a readout basis $R^i \in \{X,Y\}$ temporarily for all n particles b^{ij} belonging to the same ith sequence, but she chooses the sending basis S^{ij} randomly as in step 1. (ii) For all those particles that satisfy the legitimate basis arrangement $(R^i = R^{ij}) \neq S^{ij}$, she performs the prescribed measurement in step 3. (iii) For the remaining particles specified with the illegitimate arrangement $(R^i = R^{ij}) = S^{ij}$, she continues to access the particles until she obtains the conclusive outcome $|A_R\rangle \neq |A_S\rangle$, which reveals $C^i \neq R^i$ on Bob's basis C^i. (iv) Once she knows his basis, she switches to using the legitimate arrangement $R^{ij} \neq S^{ij}$ for all the remaining particles.

Since Alice can obtain no information with regard to Bob's basis C^i from those particles that satisfy the legitimate arrangement $(R^i = R^{ij}) \neq S^{ij}$, she is concerned only with those particles that satisfy the illegitimate arrangement $(R^i = R^{ij}) = S^{ij}$ for each sequence. Here she can assume the two different cases $R^i \neq C^i$ and $R^i = C^i$. Ignoring the statistical fluctuation, $m/2$ sequences are accidentally subject to a conclusive measurement where Alice's basis is different from Bob's coding basis $(R^i \neq C^i)$. Whenever this condition is satisfied, Alice finds $C^i \neq R^i$ with a $1/2$ probability from the conclusive outcome $|A_R\rangle \neq |A_S\rangle$ by accessing one particle. If she obtains $|A_R\rangle = |A_S\rangle$ and fails in the first trial, she accesses the next particle. Once she can conclude $C^i \neq R$, she changes to the legitimate access. If she repeats this procedure up to l $(\leqslant n)$ times, she can improve the final success probability to $1-1/2^l$. Hence, she can expect to conclude $m/2$ different subordinate bits u^i if she performs illegitimate access enough times.

Next we consider all possible cases in which Alice obtains the inconclusive outcomes $|A_S\rangle = |A_R\rangle$ for the repeated l times and then stops the illegitimate access. In the above cases, although she fails to obtain conclusive results on his basis C^k, she can guess the basis C^k to be R^k with a probability $(1/2)/\{1/2+(1/2)(1/2^l)\} = (1+1/2^l)^{-1}$. Here (i) $1/2$ is in the numerator and the first term in the denominator is the probability of $R^k = C^k$, and (ii) $1/2^l$ means the probability that the inconclusive outcome $|A_R\rangle = |A_S\rangle$ continues to appear l times when $R^k \neq C^k$ holds. Therefore, even if Alice's basis is accidentally consistent with Bob's coding basis $(R^k = C^k)$, she can guess u^k with a high probability. The probability $(1+1/2^l)^{-1}$ asymptotically approaches unity with the increase of l, where the possibility of $R^k \neq C^k$ decreases exponentially with respect to l. Thus the remaining $m/2$ sequences that are subject to the inconclusive measurement $(R^i = C^i)$ are also meaningful for dishonest Alice to guess C.

In the following, we discuss the evidence of her illegitimate access. With regard to the $m/2$ sequences that are subject to the conclusive measurement $(R^i \neq C^i)$, she must access at least one particle per sequence to specify the subordinate bit u^i. This access necessarily destroys the state $|B_C\rangle$ of the particle and can be detected by Bob with a $1/2$ probability in step 7. Here we assume that she repeats the illegitimate access up to l $(\leqslant n)$ times if she needs; we can estimate the expected number of her access times for one sequence as follows:

$$\sum_{k=1}^{l} k(1/2)^{\kappa-1}(1/2) + l\,(1/2)^l = 2-(1/2)^{l-1}.$$

The second term on the left-hand side corresponds to the case in which she unfortunately fails to specify u^i. The expected number is at most 2, even though she takes a large l value. On the other hand, the remaining $m/2$ sequences that are subjected to the inconclusive measurement $(R^k = C^k)$ leave no evidence of the illegitimate access. The relevant access does not destroy the quantum state $|B_C\rangle$ of the particle, and Alice can always respond with the correct spin state $|A_C\rangle = |B_C\rangle$ in step 7.

In conclusion, the above straightforward strategy can reduce the total times of her illegitimate access that Bob can detect, whereas she can guess the commitment bit Z $(=\oplus_{i=1}^{m} u^i)$ with a high probability. Here it is possible for her to determine $m/2$ subordinate bits by the conclusive measurement, and she can guess the other $m/2$ subordinate bits by the inconclusive measurement $(R^i = C^i)$. The probability of her correct guess is evaluated by $\{(1+1/2^l)^{-1}\}^{m/2} \sim 1-(m/2)(1/2)^l$ approximately in the first order of the very small quantity $(1/2)^l$. Section IV C reexamines this strategy in a general framework taking entanglement-assisted operations into consideration.

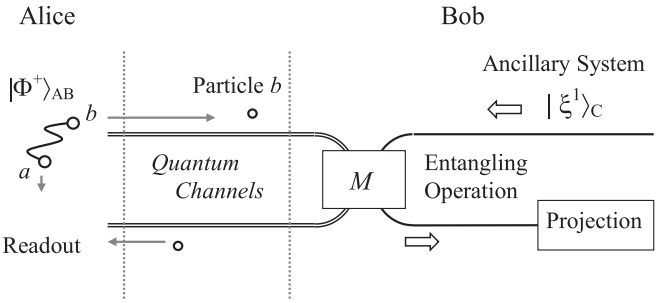


FIG. 4. General configuration of the whole system considering entanglement-assisted operations.

We then move to the view of the examiner, Bob. He can sample κn particles for his examination in each sequence, where κ is the security parameter. Since (i) the number of the sequences subject to the conclusive measurement ($R^i \neq C^i$) is $m/2$, (ii) the expected number of the illegitimate access is at most 2 for each sequence, and (iii) the probability that one arbitrary particle is sampled accidentally is κ, the total number of Alice's illegitimate accesses that are detectable by him is given by $[(m/2)\times 2]\times\kappa = \kappa m$ for a block of $m \times n$ particles. As Alice passes the examination with a $1/2$ probability in each conclusive measurement, the probability P_B of Bob's detection of dishonest Alice can be estimated by

$$P_B = 1-(1/2)^{k(m/2)\times 2}\times(1)^{k(m/2)\times l} = 1-(1/2)^{km} \quad \text{with} \quad k < 1/3. \tag{3}$$

Here the term $(1)^{\kappa(m/2)l}$ means that the $m/2$ sequences subject to the l times of the inconclusive measurement ($R^i = C^i$) do not prevent Alice from answering the correct spin states.

E. Bob's examination of the identity for the transmitted state

Finally, we mention the supplementary substep that Bob executes in step 2 of the minimal CSBC protocol. Honest Bob examines whether Alice really sent the four different states $|X\pm\rangle$ and $|Y\pm\rangle$ at random in step 1 by assessing the sequences of the resultant states $|B_C\rangle^{ij}$ ($i = 1\sim m, j = 1\sim n$). If and only if Bob can confirm the identity $I/2 = (1/2)(|+\rangle\langle+| + |-\rangle\langle-|)$ for her transmitted spin state, Bob considers Alice to be honest. By requiring this condition, we can reduce our problem to a simple form when we analyze the strategies of dishonest Alice in Secs. IV C and IV D.

IV. ENTANGLEMENT-ASSISTED FRAMEWORKS

We can expand the minimal CSBC protocol into a more general form by considering entanglement-assisted operations. This expansion greatly facilitates our ability to analyze the security aspect of the minimal CSBC protocol. As shown in Fig. 4, Alice and Bob, respectively, entangle the states $|h\rangle_a$ and $|\xi\rangle_c$ of their own ancillary particle a and system c with the state $|\lambda\rangle_b$ of flying particle b. Here, Alice prepares an initial entangled state of particles a and b such that $|\Lambda\rangle_{ab} = c_1|h^1\rangle_a|\lambda^1\rangle_b + c_2|h^2\rangle_a|\lambda^2\rangle_b$, whereas Bob executes an appropriate entangling operation M on flying particle b and his ancillary system c. Then Bob returns particle b to Alice. We assume that they utilize quantum memories to store the quantum information of the particles and the ancillary system.

A. Revisiting the opening phase for checking dishonest Bob in the minimal CSBC protocol

We can reexamine the security of the minimal CSBC protocol against dishonest Bob using the framework in which honest Alice utilizes an entangled pair of qubits a and b,

$$\begin{aligned}|\Phi+\rangle_{ab} &= \sqrt{1/2}(|X+\rangle_a|X+\rangle_b + |X-\rangle_b|X-\rangle_b)\\ &= \sqrt{1/2}(|Y+\rangle_a|Y-\rangle_b + |Y-\rangle_a|Y+\rangle_b).\end{aligned}$$

In what follows we consider Bob, who wants to escape Alice's detection completely while he delays his decision of the basis C until the opening phase. The state $|\Phi+\rangle_{ab}$ is one of the four different Bell states, which are summarized in Table II. Here she sends particle b to Bob while retaining ancillary particle a in her quantum storage and then she receives the returned particle b. Unlike the minimal protocol, she can delay choosing the measurement bases for particles a and b, respectively, until Bob unveils the coding (C) basis in the opening phase. In particular, after he unveils C, she can measure both particles a and b with the same basis that is identical to his unveiled coding basis C. Furthermore, she is later informed of the spin state $|B_C\rangle_b$ of particle b from Bob, except for κn test particles that are chosen by him as the test bit with the condition $\kappa < 1/3$. As she postpones her measurement until the opening phase, she takes no action to extract Bob's basis information in the commitment phase. In this sense, she is honest and always passes Bob's examination.

The above procedures enable her to execute the two different examinations as follows. (i) For all n pairs in a sequence, since she is informed of the coding basis C, she can

TABLE II. Four different Bell states.

	Z basis	X basis	Y basis	Composite spin angular momentum
$\|\Phi+\rangle_{ab}$	$\frac{\|Z+\rangle_a\|Z+\rangle_b+\|Z-\rangle_a\|Z-\rangle_b}{\sqrt{2}}$	$\frac{\|X+\rangle_a\|X+\rangle_b+\|X-\rangle_a\|X-\rangle_b}{\sqrt{2}}$	$\frac{\|Y+\rangle_a\|Y-\rangle_b+\|Y-\rangle_a\|Y+\rangle_b}{\sqrt{2}}$	$(s=1, s_Y=0)$
$\|\Psi+\rangle_{ab}$	$\frac{\|Z+\rangle_a\|Z-\rangle_b+\|Z-\rangle_a\|Z+\rangle_b}{\sqrt{2}}$	$\frac{\|X+\rangle_a\|X+\rangle_b-\|X-\rangle_a\|X-\rangle_b}{\sqrt{2}}$	$\frac{\|Y+\rangle_a\|Y+\rangle_b-\|Y-\rangle_a\|Y-\rangle_b}{i\sqrt{2}}$	$(s=1, s_z=0)$
$\|\Psi-\rangle_{ab}$	$\frac{\|Z+\rangle_a\|Z-\rangle_b-\|Z-\rangle_a\|Z+\rangle_b}{\sqrt{2}}$	$\frac{-\|X+\rangle_a\|X-\rangle_b+\|X-\rangle_a\|X+\rangle_b}{\sqrt{2}}$	$\frac{-\|Y+\rangle_a\|Y-\rangle_b+\|Y-\rangle_a\|Y+\rangle_b}{i\sqrt{2}}$	$(s=0, s_i=0; i=x,y,z)$
$\|\Phi-\rangle_{ab}$	$\frac{\|Z+\rangle_a\|Z+\rangle_b-\|Z-\rangle_a\|Z-\rangle_b}{\sqrt{2}}$	$\frac{\|X+\rangle_a\|X-\rangle_b+\|X-\rangle_a\|X+\rangle_b}{\sqrt{2}}$	$\frac{\|Y+\rangle_a\|Y+\rangle_b+\|Y-\rangle_a\|Y-\rangle_b}{\sqrt{2}}$	$(s=1, s_x=0)$

compare her outcomes $|A_C\rangle_a$ and $|A_C\rangle_b$, which she obtains from the measurement on particles a and b, respectively. She examines the parallel spin correlation when $C=X$ is informed, or the antiparallel spin correlation for the $C=Y$ cases (see $|\Phi+\rangle_{ab}$ in Table II). (ii) For $(1-\kappa)n$ untested particles in the sequence of particles b, since she is informed of $|B_C\rangle_b$ in addition to the basis C, she can compare $|A_C\rangle_b$ with $|B_C\rangle_b$. She examines whether they match.

Therefore, dishonest Bob must pass both examinations at the same time with regard to the above $(1-\kappa)n$ particles. If dishonest Bob wants to pass the first examination completely, he may return particle b without disturbing the entangled state $|\Phi+\rangle_{ab}$. However, if he does this, he cannot pass the second examination. This is because he is ignorant of the spin state $|A_C\rangle_b$ that she obtains. On the other hand, if he wants to pass the second examination completely, he may prepare a dummy pair of particles a' and b' in the entangled state $|\Phi+\rangle_{a'b'}$ and send only particle b' to Alice while keeping particle b in his hand. As he can always make sure of her measurement outcome $|A_C\rangle_{b'}$ from his outcome $|B_C\rangle_{a'}$ for particle a' with the measurement basis C, he can achieve his purpose regardless of his delayed choice $C=X$ or Y. However, if he does this, he cannot pass the first examination. This is because he cannot ensure the spin correlation between $|A_C\rangle_a$ and $|A_C\rangle_{b'}$. This observation suggests that the security against dishonest Bob is attributed to the principles of quantum mechanics as regards the complementary nature between the spin angular momentum of a composite system represented by the entangled state $|\Phi+\rangle_{ab}$ and the spin angular momentum of each particle a or b.

Hence, dishonest Bob may not be able to pass the first and second examinations simultaneously in this expanded procedure in which Alice utilizes the entangled state $|\Phi+\rangle_{ab}$ and the quantum state storage. The first and second examinations in the expanded procedure correspond to the $C=S$ and R cases in the minimal CSBC protocol, respectively. In the $C=S$ case, the role of $|A_C\rangle_b$ in the first examination can be regarded as being replaced with that of $|B_C\rangle_b$, which is compared with her transmitted state. In the $C=R$ case, $|B_C\rangle_b$ is compared with her read-out state. Although the two cases are exclusive in the minimal CSBC protocol, dishonest Bob is ignorant of her sending (S) and readout (R) bases. Therefore, the opening phase for checking dishonest Bob in the minimal CSBC protocol is reasonable from the viewpoint given above.

B. Security against dishonest Bob using an entangled state

By utilizing an entanglement-assisted attack, dishonest Bob can reduce the probability of being detected. To clarify this point, we refine his operation for particle b of the entangled pair $|\Phi+\rangle_{ab}$ in a general form. First, he prepares his ancillary system $|\xi\rangle_c$, which is defined in a three-dimensional Hilbert space spanned with the basis $\{|\xi^1\rangle,|\xi^2\rangle,|\xi^3\rangle\}$, and $|\xi^1\rangle$ is the initial state. Then he performs a unitary entangling operation $M(c_1,c_2,c_3)$ on particle b in step 2, as shown in Fig. 4. He then returns particle b to Alice. The operation $M(c_1,c_2,c_3)$ is defined by

$$M(c_1,c_2,c_3) = c_1 I_b(|\xi^1\rangle\langle\xi^1|)_c + c_2 X_b(|\xi^2\rangle\langle\xi^1|)_c + c_3(-iY_b)(|\xi^3\rangle\langle\xi^1|)_c, \quad (4)$$

where (X_b,Y_b) and I_b are the Pauli operators and the identity operator acting on particle b, respectively.

For example, honest Bob who selected $C=X$ in step 2 employs $M_X \equiv M(\sqrt{1/2},\sqrt{1/2},0)$. The state of the system evolves into

$$|\psi_X\rangle_{abc} = M_X|\phi+\rangle_{ab}|\xi^1\rangle_c = \sqrt{1/2}(|X+\rangle_a|X+\rangle_b \times |\phi^1\rangle_c + |X-\rangle_a|X-\rangle_b \times |\phi^2\rangle_c) \quad (5a)$$

with

$$|\phi^1\rangle_c = \sqrt{1/2}(|\xi^1\rangle_c + |\xi^2\rangle_c) \quad \text{and}$$
$$|\phi^2\rangle_c = \sqrt{1/2}(|\xi^1\rangle_c - |\xi^2\rangle_c). \quad (5b)$$

He then performs a projection measurement for his ancillary system with the basis $\{|\phi^1\rangle,|\phi^2\rangle,|\xi^3\rangle\}$ in step 4 so that he can unveil the correct state $|\varphi_C\rangle_b \in \{|X+\rangle_b,|X-\rangle_b\}$. For $C=Y$, he employs $M_Y \equiv M(\sqrt{1/2},0,\sqrt{1/2})$ as

$$|\psi_Y\rangle_{abc} = M_Y|\phi+\rangle_{ab}|\xi^1\rangle_c = \sqrt{1/2}(|Y+\rangle_a|Y-\rangle_b|\psi^1\rangle_c + |Y-\rangle_a|Y+\rangle_b|\psi^2\rangle_c) \quad (6a)$$

with

$$|\psi^1\rangle_c = \sqrt{1/2}(|\xi^1\rangle_c + i|\xi^3\rangle_c) \quad \text{and}$$
$$|\psi^2\rangle_c = \sqrt{1/2}(|\xi^1\rangle_c - i|\xi^3\rangle_c), \quad (6b)$$

and he adopts another basis $\{|\psi^1\rangle,|\psi^2\rangle,|\xi^2\rangle\}$ for the ancillary system. Hence, his choice of either coding basis X or Y is generalized into the choice of entangling operation M_X or M_Y. He cannot transform between $|\psi_X\rangle_{abc}$ and $|\psi_Y\rangle_{abc}$ by performing any local deterministic operation on his ancillary system. We can prove this point by comparing the diagonal forms for the two reduced density matrices $\mathrm{Tr}_{ab}(|\psi_X\rangle\langle\psi_X|)_{abc} = (1/2)(|\xi^1\rangle\langle\xi^1|+|\xi^2\rangle\langle\xi^2|)_c$ and $\mathrm{Tr}_{ab}(|\psi_Y\rangle\langle\psi_Y|)_{abc} = (1/2)(|\xi^1\rangle\langle\xi^1|+|\xi^3\rangle\langle\xi^3|)_c$, where Tr_{ab} indicates the partial trace out of the quantum states of a pair of particles a and b. This point ensures that dishonest Bob cannot pass the first and second examinations simultaneously as discussed in Sec. IV A. Appendix B examines a more extended entangling operation.

Next we consider dishonest Bob, who tries to perform a sophisticated postpone strategy; he can utilize $M_{\mathrm{postpone}} \equiv M(\sqrt{1/3},\sqrt{1/3},\sqrt{1/3})$, which is derived in Appendix B. The evolved state of the system can be represented by

$$M_{\mathrm{postpone}}|\phi+\rangle_{ab}|\xi^1\rangle_c = \sqrt{2/3}|\Psi_X\rangle_{abc} + \sqrt{1/3}|\Psi-\rangle_{ab}|\xi^3\rangle_c = \sqrt{2/3}|\Psi_Y\rangle_{abc} + \sqrt{1/3}|\Psi+\rangle_{ab}|\xi^2\rangle_c, \quad (7)$$

where $|\Psi\pm\rangle_{ab}$ represents the certain Bell states summarized in Table II. When he tells either coding basis, he can adopt either basis $\{|\phi^1\rangle,|\phi^2\rangle,|\xi^3\rangle\}$ or $\{|\psi^1\rangle,|\psi^2\rangle,|\xi^2\rangle\}$ for his ancillary system depending on his delayed choice of $C=X$ or Y. If he chooses the former basis and then obtains the result $|\phi^1\rangle$ or $|\phi^2\rangle$, he is aware of his success and he can pass Alice's examination by unveiling the basis $C=X$ and the state $|X+\rangle_b$ or $|X-\rangle_b$. On the other hand, if he obtains $|\xi^3\rangle$, which occurs with a $1/3$ probability, the state of the pair falls into the illegitimate entangled state $|\Psi-\rangle_{ab}$ and he fails to answer the correct spin state of particle b with a $1/2$ probability. Then he is detected

with a $1/2$ probability per particle in step 10 of the minimal protocol. A similar scenario holds for $C = Y$.

Since (i) $(2/3)n$ particles per sequence can pass Alice's examination on average in step 10 and (ii) Bob can conceal κn arbitrary particles in a set of his test particles, the probability that he can escape her detection is represented by $(1/2)^{\max[n/3-\kappa n,0]}$. This is the reason that the security parameter κ must be set sufficiently less than $1/3$ when they achieve the consensus on κ. Thus, if Alice executes the minimal protocol, the probability P_A that she can defeat the sophisticated postpone strategy is estimated by

$$P_{A(\text{postpone III})} = 1 - (1/2)^{(1/3-k)n} \quad \text{with} \quad k < 1/3. \tag{8}$$

C. Security against dishonest Alice using an entangled state

The purpose of dishonest Alice is to find a combination of the initial transmitted state of particle b and the measurement basis for returned particle b such that she can obtain much information relevant to Bob's basis choice without leaving evidence of the illegitimate access. In the entanglement-assisted framework, she uses the maximally entangled state $|\Phi+\rangle_{ab}$ and postpones measuring staying particle a until receiving particle b. Note in this framework that the use of $|\Phi+\rangle_{ab}$ ensures the identity $I/2 = \mathrm{Tr}_a(|\Phi+\rangle\langle\Phi+|)_{ab}$ for the particle b; she can always pass the supplemental examination by Bob as regards the identity of the transmitted state (see Sec. III E). More generally, we can start from the condition in which she prepares initially a product state $|\chi\rangle = \otimes_{j=1}^{n}|\Phi+\rangle_{ab}{}^{(j)}$ for a sequence of n different pairs of staying and flying particles.

Once Alice prepares the initial product state $|\chi\rangle$, she can postpone choosing a measurement basis for the set of n staying particles until she receives the set of n flying particles. Her prior choice of the initial transmitted state is replaced by the posterior choice of the measurement basis in the entanglement-assisted framework. In fact, if Alice obtains the measurement outcome $|\psi_k\rangle_A$ as a result of her collective projection measurement with the basis $\{|\psi_i\rangle_A;\ i = 1 \sim 2^n\}$ on n staying particles, this is equivalent to her sending the entangled state $|\varphi_k\rangle_B$ of n flying particles provided that $|\chi\rangle = \sum_{i=1}^{2^n} c_i|\psi_i\rangle_A|\varphi_i\rangle_B$ $(i = 1 \sim 2^n)$ holds, where $|\psi_i\rangle_A$ (or $|\varphi_i\rangle_B$) denotes a set of 2^n different orthogonal normalized entangled states of n staying (or flying) particles, and $\sum_{i=1}^{2^n}|c_i|^2 = 1$ holds. Therefore, a variety of Alice's strategies is attributed to her different choices of the measurement basis for a sequence of n different pairs of staying and returned particles, which is initially prepared in $|\chi\rangle$.

With regard to each pair of particles a and b, two different density matrices relevant to the different basis choices of honest Bob are given by

$$\rho_X = \mathrm{Tr}_c(|\Psi_X\rangle\langle\Psi_X|)_{abc} \quad \text{and} \quad \rho_Y = \mathrm{Tr}_c(|\Psi_Y\rangle\langle\Psi_Y|)_{abc}.$$

ρ_X and ρ_Y are derived, respectively, from Eqs. (5) and (6), where Tr_c denotes the partial trace over the states of Bob's ancillary system. When Bob chooses either coding basis $C = X$ or Y for particle b in step 2, Alice receives the density matrix ρ_X or ρ_Y in step 3. Therefore, her purpose is to find the measurement basis for a particle pair that makes it possible for her to perform an unambiguous state discrimination between ρ_X and ρ_Y. Since ρ_X and ρ_Y are expressed in diagonal forms simultaneously as

$$\rho_X = \frac{1}{2}\begin{bmatrix}1&0&0&0\\0&0&0&0\\0&0&1&0\\0&0&0&0\end{bmatrix} \quad \text{and} \quad \rho_Y = \frac{1}{2}\begin{bmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&1\end{bmatrix}$$

with the Bell basis $\{|\Phi+\rangle_{ab},|\Phi-\rangle_{ab},|\Psi+\rangle_{ab},|\Psi-\rangle_{ab}\}$, the Bell state serves as the unambiguous state discrimination. (i) Her measurement outcomes $|\Psi+\rangle$ and $|\Psi-\rangle$ reveal $C = X$ and Y, respectively, without errors. (ii) The outcome $|\Phi+\rangle$ affords her no information. (iii) The outcome $|\Phi-\rangle$ is never obtained.

This observation holds directly for a sequence of returned n particles b^{ij} $(j = 1 \sim n)$ that are coded with an identical basis of either $C^i = X$ or Y. As the initial state of n pairs is prepared in $|\chi\rangle = \otimes_{j=1}^{n}|\Phi+\rangle_{ab}{}^{(j)}$, the density matrices of the sequences of n pairs are given by the direct products over n individual pairs as

$$\rho_X^i = \bigotimes_{j=1}^{n}\rho_X^{ij} \quad \text{and} \quad \rho_Y^i = \bigotimes_{j=1}^{n}\rho_Y^{ij},$$

where the above density matrices are defined in a 4^n-dimensional Hilbert space. We can express ρ_X^i and ρ_Y^i in diagonal forms simultaneously provided that we employ the Bell basis for each pair. Therefore, Alice can distinguish ρ_X^i and ρ_Y^i by choosing the Bell basis for different individual pairs. If she repeats the measurement until she obtains a conclusive outcome, she can determine the coding basis C^i or subordinate bit u^i. Its success probability is given by $1-(1/2)^n$. Hence, she can determine the commitment bit $Z = \oplus_{i=1}^{m} u^i$ with the probability $(1-1/2^n)^m$.

On the other hand, the Bell state measurement necessarily leaves behind evidence of her illegitimate access, as explained below. The Bell state measurement is equivalent to determining the spin angular momentum for a composite system of spins a and b [19]. Table II summarizes this point. However, the projection to the possible three Bell states $\{|\Phi+\rangle_{ab},|\Psi+\rangle_{ab},|\Psi-\rangle_{ab}\}$ for a pair of spins a and b necessarily destroys the spin state $|B_C\rangle_b$ of particle b. This means that Alice cannot escape Bob's examination as long as she executes the Bell state measurement. Thus security against dishonest Alice is attributed to the complementary relationship between the spin angular momentum of the composite system and that of an individual particle [19].

More generally, as the information relevant to Bob's basis choice is coded in the composite spin angular momentum of each pair, collective measurements over several pairs necessarily disturb this information. Moreover, collective measurements over pairs destroy the spin state $|B_C\rangle_b$ of each particle b and may bring incorrect answers when she is subjected to Bob's examination. Therefore, it seems less beneficial for dishonest Alice to employ a collective attack for the set of different pairs.

Finally, it is worth mentioning the relationship between the Bell state measurement above and the straightforward strategy supposed in the minimal CSBC protocol (see Sec. III D). Assume that she replaces the Bell basis with the product state basis $\{|X+\rangle_a|X+\rangle_b$, $|X+\rangle_a|X-\rangle_b$, $|X-\rangle_a|X+\rangle_b$, $|X-\rangle_a|X-\rangle_b\}$. Alice can consider

the projection onto a certain product state $|X+\rangle_a|X-\rangle_b$ or $|X-\rangle_a|X+\rangle_b$ to be equivalent to the projection into the Bell state $|\Psi-\rangle_{ab} = \sqrt{1/2}(-|X+\rangle_a|X-\rangle_b+|X-\rangle_a|X+\rangle_b)$ and she can conclude $C = Y$. This is because ρ_X and ρ_Y do not contain the Bell state $|\Phi-\rangle$, which is defined as $\sqrt{1/2}(|X+\rangle_a|X-\rangle_b+|X-\rangle_a|X+\rangle_b)$. On the other hand, the projection onto the state $|X+\rangle_a|X+\rangle_b$ or $|X-\rangle_a|X-\rangle_b$ provides no conclusive result while it preserves the spin state $|X+\rangle_b$ or $|X-\rangle_b$. Whenever Alice obtains the result $|X+\rangle_a|X+\rangle_b$ or $|X-\rangle_a|X-\rangle_b$ on successive l occasions for the kth sequence, however, she can reduce the probability of $C^k = Y$ to $1/2^l$ and guess $C^k = X$ with a probability $(1+1/2^l)^{-1}$ without leaving behind evidence. Thus she can reduce the evidence of the illegitimate access by about 50% without sacrificing gained information.

Finally, we mention the appropriate (m,n,κ) values for a given security criteria ε. We define ε as Bob's failure probability $1-P_B = (1/2)^{\kappa m}$ in detecting the straightforward strategy of dishonest Alice [see Eq. (3)]. We set the same criteria ε for Alice's failure probability $1-P_{A\,(\text{postpone III})} = (1/2)^{(1/3-\kappa)n}$ in detecting the third postpone strategy of dishonest Bob [see Eq. (8)]. Hence, m and n are given by $m = (\log_{1/2}\varepsilon)/\kappa$ and $n = (\log_{1/2}\varepsilon)/(1/3-\kappa)$, respectively. $\kappa = 1/6$ minimizes the total round-trip times $m \times n$. The criterion $\varepsilon = 10^{-9}$ requires $(m,n) = (180\ 180)$ and 32 400 times of the round trip for the cheat-sensitive commitment of a classical one-bit.

D. Complementary relationships between the spin-state assertion and the coding basis determination

As discussed in Sec. IV C, dishonest Alice is inevitably detected by Bob in the opening phase whenever she tries to determine or guess his coding basis C in the commitment phase. This subsection shows an example in which she can obtain no information relevant to his coding basis C in the commitment phase as long as she tries to escape his examination. If she attempts to pass the examination perfectly in the opening phase, what kinds of illegitimate measurements are allowed for Alice in the commitment phase?

To find the above type of illegitimate measurements, we introduce a measurement Γ performed with a four-dimensional projection basis $\{|P\rangle,|Q\rangle,|R\rangle,|S\rangle\}$ for a pair of staying and returned particles in the commitment phase. Alice must design the measurement Γ such that she can assert the correct spin state $|C\pm\rangle$ of particle b whenever she is notified of Bob's coding basis C. As she must prepare the maximally entangled state $|\Phi+\rangle_{ab}$ to satisfy the identity condition $I/2 = \text{Tr}_a(|\Phi+\rangle\langle\Phi+|)_{ab}$ for particle b (see Section III E), the correlation between the quantum state $|\Pi\rangle_{ab}$ of the particle pair and the state $|\xi\rangle_c$ of Bob's ancillary system is always represented by $|\psi_X\rangle_{abc}$ [see Eq. (5)] or $|\psi_Y\rangle_{abc}$ [see Eq. (6)] depending on his basis choice $C = X$ or Y.

Instead of $|X\pm,X\pm\rangle_{ab}$ or $|Y\pm,Y\mp\rangle_{ab}$, she can find an alternative expression for $|\Pi\rangle_{ab}$ in $|\psi_X\rangle_{abc}$ or $|\psi_Y\rangle_{abc}$ by considering the preservation of the inner products such as $(\langle X-,X-|X+,X+\rangle)_{ab} = 0$, $(\langle Y-,Y+|Y+,Y-\rangle)_{ab} = 0$, $(\langle Y\pm,Y\mp|X+,X+\rangle)_{ab} = 1/2$, and $(\langle Y\pm,\mp|X-,X-\rangle)_{ab} = 1/2$.

TABLE III. Alice's assertion for Bob's spin state $|\pm\rangle$ depending on his basis notification.

	Bob's notification of basis C	
Alice Measurement outcomes	Bob notified of X basis	Bob notified of Y basis
$\|P\rangle$	+	+
$\|Q\rangle$	−	−
$\|R\rangle$	+	−
$\|S\rangle$	−	+

For example, she can rewrite $|X\pm,X\pm\rangle_{ab}$ and $|Y\pm,Y\mp\rangle_{ab}$ with the basis $\{|P\rangle,|Q\rangle,|R\rangle,|S\rangle\}$ as follows:

$$
\begin{aligned}
|X+\rangle_a|X+\rangle_b &= \sqrt{1/2}(|P\rangle_{ab} + |R\rangle_{ab}),\\
|X-\rangle_a|X-\rangle_b &= \sqrt{1/2}(|Q\rangle_{ab} + |S\rangle_{ab}),\\
|Y+\rangle_a|Y-\rangle_b &= \sqrt{1/2}(|Q\rangle_{ab} + |R\rangle_{ab}),\\
|Y-\rangle_a|Y+\rangle_b &= \sqrt{1/2}(|P\rangle_{ab} + |S\rangle_{ab}).
\end{aligned}
$$

Furthermore, she can determine the basis state $\{|P\rangle,|Q\rangle,|R\rangle,|S\rangle\}$ by solving the above equations with $|Y\pm\rangle = \{(1\pm i)|X+\rangle + (1\mp i)|X-\rangle\}/2$. Thus she can find the alternative expressions for $|\psi_X\rangle_{abc}$ and $|\psi_Y\rangle_{abc}$ such that

$$
\begin{aligned}
|\Psi_X\rangle_{abc} = \sqrt{1/2}\{&\sqrt{1/2}(|P\rangle_{ab} + |R\rangle_{ab})|\phi^1\rangle_c\\
&+ \sqrt{1/2}(|Q\rangle_{ab} + |S\rangle_{ab})|\phi^2\rangle_c\},
\end{aligned}
\tag{9}
$$

$$
\begin{aligned}
|\Psi_Y\rangle_{abc} = \sqrt{1/2}\{&\sqrt{1/2}(|Q\rangle_{ab} + |R\rangle_{ab})|\psi^1\rangle_c\\
&+ \sqrt{1/2}(|P\rangle_{ab} + |S\rangle_{ab})|\psi^2\rangle_c\}.
\end{aligned}
\tag{10}
$$

As shown in Eqs. (9) and (10), if she employs the above basis $\{|P\rangle,|Q\rangle,|R\rangle,|S\rangle\}$ for the measurement Γ in the commitment phase, she can answer the correct spin state $|C\pm\rangle$ to Bob in the opening phase. She can always assert the spin state of particle b from her measurement outcome in accordance with Table III. This framework is very similar to the assertion scheme proposed by Vaidman, Aharonov, and Albert [20].

With regard to the extraction of Bob's basis information, however, the measurement Γ provides Alice with no information. We can clarify this point from the expressions for $\rho_X = \text{Tr}_c(|\psi_X\rangle\langle\psi_X|)_{abc}$ and $\rho_Y = \text{Tr}_c(|\psi_Y\rangle\langle\psi_Y|)_{abc}$ with the basis $\{|P\rangle,|Q\rangle,|R\rangle,|S\rangle\}$,

$$
\rho_X = \frac{1}{4}\begin{bmatrix} 1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \rho_Y = \frac{1}{4}\begin{bmatrix} 1 & 0 & 0 & 1\\ 0 & 1 & 1 & 0\\ 0 & 1 & 1 & 0\\ 1 & 0 & 0 & 1 \end{bmatrix}.
$$

Each diagonal element is identical for ρ_X and ρ_Y. Hence, she can obtain no information with regard to his basis choice $C = X$ or Y. Thus, in this example, it is impossible for Alice to pass the examination by Bob and to obtain Bob's basis information simultaneously. Appendix C discusses this point for more general cases, where the initial state of the particle pair is extended to a nonmaximally entangled state.

As shown in Appendix D, the following basis $\{|p\rangle,|q\rangle,|r\rangle,|s\rangle\}$ or $\{|p'\rangle,|q'\rangle,|r'\rangle,|s'\rangle\}$ is an explicit example

for the basis state $\{|P\rangle,|Q\rangle,|R\rangle,|S\rangle\}$ with the additional phase factors $e^{i\phi}$:

$$\{|p\rangle,|q\rangle,|r\rangle,|s\rangle\} = \{|Y-\rangle_a|X+\rangle_b,|Y+\rangle_a|X-\rangle_b,|Y+\rangle_a|X+\rangle_b,|Y-\rangle_a|X-\rangle_b\}$$

or

$$\{|p'\rangle,|q'\rangle,|r'\rangle,|s'\rangle\} = \{|X+\rangle_a|Y+\rangle_b,|X-\rangle_a|Y-\rangle_b,|X+\rangle_a|Y-\rangle_b,|X-\rangle_a|Y+\rangle_b\}.$$

This is exactly the legitimate arrangements ($S \neq R$) in the sending (S) and readout (R) bases, which are prescribed for Alice in the minimal protocol. Thus the security of the minimal protocol is given by the nature of the measurement Γ.

Here it is worth mentioning that the above assertion scheme for the spin state with the two conjugate bases $\{|p\rangle,|q\rangle,|r\rangle,|s\rangle\}$ and $\{|p'\rangle,|q'\rangle,|r'\rangle,|s'\rangle\}$ has a similar structure to that of a quantum communication channel analogous to one out of two oblivious transfers that we have proposed [21]. Appendix D also outlines this point.

Furthermore, by considering an appropriate projection measurement $\tilde{\Gamma}$ that is modified from the measurement Γ, we can study the quantitative relationship between the information that Alice can obtain and the probability of being detected by Bob. She can choose the projection measurement $\tilde{\Gamma}$ such that she can obtain a small amount of information on Bob's coding basis C while leaving little evidence of her illegitimate access. She may be able to guess the coding basis C by increasing the number of measurements per sequence. This strategy, however, offers no advantage. Appendix E examines this point.

V. SUMMARY

First, in this paper we proposed a quantum protocol for bit escrow with a round trip of a qubit. Alice, the receiver of the bit, sends one of two spin states $|S\pm\rangle$ by choosing basis S in a random way from two conjugate bases X and Y. Bob, the sender of the bit, performs a projection measurement with coding basis $C \in \{X,Y\}$ and returns a resultant state $|C\pm\rangle$. She performs a projection measurement with another basis R ($\neq S$) and obtains an outcome $|R\pm\rangle$. Thus she can assert the spin state $|C+\rangle$ or $|C-\rangle$ depending on the coding basis C that is announced later from Bob. Afterward, she can discover Bob, who unveils a wrong basis with a faked spin state. On the other hand, if Alice infers the coding basis C, but destroys $|C\pm\rangle$, by setting basis R identical to S, Bob can detect this by requesting that she guess the spin state $|C\pm\rangle$.

Then we constructed a quantum communication protocol for the cheat-sensitive commitment of a classical bit (CSBC) by utilizing the above bit escrow protocol as a building block. Our proposed scheme avoids the loophole relevant to the decomposability of a quantum bit escrow and quantum weak coin flipping [18] that is addressed for the conventional CSBC protocol. To ensure impartial examinations for the two parties and probabilistic security improvements with respect to m and n, the classical bit is encoded in a block of $m \times n$ particles of a qubit. Bob can probabilistically detect dishonest Alice when she violates concealment in the commitment phase. Alice can probabilistically detect dishonest Bob provided that (i) he tries to change the commitment bit from its initial value in the opening phase, or (ii) he postpones deciding the bit value until the opening phase.

Our CSBC protocol is composed of the quantum communication part and the classical information part. The former is relevant to each round trip of a qubit particle. The latter involves (i) coding a classical bit in a block of $m \times n$ qubits and (ii) using all particles as test bits for impartial examinations between the two parties. With regard to the bottom-up approach from the quantum communication part, our heuristic study suggests that the security is attributed to the complementary nature of the spin angular momentum of a composite spin system and that of the individual spin. On the other hand, it is still unclear how we can prove unconditional security. This question is open for future studies. We hope that our proposal stimulates more discussion on the topic of a quantum protocol for cheat-sensitive bit commitment.

ACKNOWLEDGMENTS

We thank S. Yamashita and M. Nakanishi for valuable discussions and Y. Tokura for his encouragement during this research. This research is supported by the Japan Society for the Promotion of Science (JSPS) through its "Funding Program for World-Leading Innovative R&D on Science and Technology (FIRST Program)."

APPENDIX A

For simplicity, in this paper we assume a lossless and error-free transmission of particles through quantum channels. If the quantum channel has a finite dissipation, however, the minimal protocol is insecure against dishonest Alice. This is because she can always fake the failure of the transmission and discard a certain particle when the quantum state of the particle is destroyed by her illegitimate access. To eliminate this fault in a simple way, Bob can scramble the transmission order of the particles when he returns a set of $m \times n$ particles to Alice in step 2. After confirming her reception of the particles, he reveals the correct addresses (i,j) only for those particles transmitted successfully. With regard to the transmission error, the minimal protocol requires an error rate ε that is sufficiently less than $2/n$. If not $\varepsilon \ll 2/n$, Bob has difficulty discriminating the evidence of Alice's illegitimate access from the transmission errors. Modification to improve the error tolerance is planned for future work.

APPENDIX B

We derive the entangling operation $M_{\text{postpone}} \equiv M(\sqrt{1/3},\sqrt{1/3},\sqrt{1/3})$ that minimizes the failure probability of dishonest Bob, who tries to postpone his decision until the opening phase. After the entangling operation $M(c_1,c_2,c_3)$ [see Eq. (4)] on the initial state $|\Phi+\rangle_{ab}|\xi^1\rangle_c$, the state of the whole system is represented as follows:

$$M(c_1,c_2,c_3)|\phi+\rangle_{ab}|\xi^1\rangle_c = c_1|\phi+\rangle_{ab}|\xi^1\rangle_c + c_2|\Psi+\rangle_{ab}|\xi^2\rangle_c + c_3|\Psi-\rangle_{ab}|\xi^3\rangle_c$$
$$= |X+\rangle_a|X+\rangle_b\left(\frac{c_1|\xi^1\rangle_c + c_2|\xi^2\rangle_c}{\sqrt{2}}\right) + |X-\rangle_a|X-\rangle_b\left(\frac{c_1|\xi^1\rangle_c - c_2|\xi^2\rangle_c}{\sqrt{2}}\right) + c_3|\Psi-\rangle_{ab}|\xi^3\rangle_c$$
$$= |Y+\rangle_a|Y-\rangle_b\left(\frac{c_1|\xi^1\rangle_c + ic_3|\xi^3\rangle_c}{\sqrt{2}}\right) + |Y-\rangle_a|Y+\rangle_b\left(\frac{c_1|\xi^1\rangle_c - ic_3|\xi^3\rangle_c}{\sqrt{2}}\right) + c_2|\Psi+\rangle_{ab}|\xi^2\rangle_c. \quad \text{(B1)}$$

The following four conditions are requested for a set of (c_1,c_2,c_3): (i) normalization condition $|c_1|^2+|c_2|^2+|c_3|^2 = 1$, (ii) orthogonal relationship between $c_1|\xi^1\rangle + c_2|\xi^2\rangle$ and $c_1|\xi^1\rangle - c_2|\xi^2\rangle$, (iii) orthogonal relationship between $c_1|\xi^1\rangle + ic_3|\xi^3\rangle$ and $c_1|\xi^1\rangle - ic_3|\xi^3\rangle$, and (iv) equal failure probabilities for the two different delayed choices of X and Y. From the above conditions, we can determine $(c_1,c_2,c_3) = (\sqrt{1/3},\sqrt{1/3},\sqrt{1/3})$. The quantity $|c_3|^2 = |c_2|^2 = 1/3$ indicates the possible minimum failure probability for Bob's delayed choice of Y or X.

A more general entangling operation is as follows. Bob prepares an additional ancillary system $|\chi\rangle_d$ and sets the initial state $|\chi^i\rangle_d = d_1|\chi^1\rangle_d + d_2|\chi^2\rangle_d$ with the two different orthogonal states $|\chi^1\rangle_d$ and $|\chi^2\rangle_d$. When he employs an extended entangling operation $M_x\otimes(|\chi^1\rangle\langle\chi^1|)_d + M_Y\otimes(|\chi^2\rangle\langle\chi^2|)_d$ on $|\Phi+\rangle_{ab}|\xi^1\rangle_c|\chi^1\rangle_d$, he obtains the state $|\zeta\rangle_{abcd} = d_1|\chi^1\rangle_d|\psi_X\rangle_{abc} + d_2|\chi^2\rangle_d|\psi_Y\rangle_{abc}$. The accidental projection to $|\chi^1\rangle_d$ or $|\chi^2\rangle_d$ results in $|\psi_X\rangle_{abc}$ or $|\psi_Y\rangle_{abc}$. However, Bob cannot control the results of the projection in a deterministic way and therefore he cannot utilize this operation to postpone his decision.

Although he can alter the quantum state from $|\zeta\rangle_{abcd}$ by performing a local deterministic operation on his ancillary systems, all transformable quantum states must be characterized by certain eigenvalues peculiar to the reduced density matrix $\sigma = \mathrm{Tr}_{ab}(|\zeta\rangle\langle\zeta|)_{abcd}$. Here Tr_{ab} denotes the partial trace over the states of a particle pair in Alice's hand. Actually, σ is expressed as

$$\sigma = [|d_1|^2(|\chi^1\rangle\langle\chi^1|)_d(|\xi^1\rangle\langle\xi^1| + |\xi^2\rangle\langle\xi^2|)_c + |d_2|^2 \times (|\chi^2\rangle\langle\chi^2|)_d(|\xi^1\rangle\langle\xi^1| + |\xi^3\rangle\langle\xi^3|)_c + \{d_1d_2^*(|\chi^1\rangle\langle\chi^2|)_d + d_1^*D_2(|\chi^2\rangle\langle\chi^1|)_d\}(|\xi^1\rangle\langle\xi^1|)_c]/2$$

and has the specific eigenvalues $\{1, |d_1|^2, 0, 0, 0, 0, |d_2|^2, 0\}$. Therefore, once Bob fixes the amplitudes $(d_1,d_2) = (1,0)$ in the commitment phase, he cannot alter them into $(d_1,d_2) = (0,1)$ in the opening phase in a deterministic way.

APPENDIX C

Suppose that Alice replaces $|\Phi+\rangle_{ab}$ with a general nonmaximally entangled state $|\eta\rangle_{ab}$ of the particle pair with the normalization $|\alpha|^2+|\beta|^2 = 1$,

$$|\eta\rangle_{ab} = a\,|\mu\rangle_a\,|X+\rangle_b + \beta\,|\nu\rangle_a\,|X-\rangle_b\,,$$

where $|\mu\rangle_a$ and $|\nu\rangle_a$ indicate arbitrary normalized states of particle a and $\langle\mu|\nu\rangle = 0$ is not necessarily satisfied. Regardless of $|\eta\rangle_{ab}$, she can always introduce the measurement Γ by choosing an appropriate basis $\{|P\rangle,|Q\rangle,|R\rangle,|S\rangle\}$, whereas Γ provides no information on Bob's choice of basis. We show this point in the following.

Instead of Eqs. (5) and (6), we define quantum states $|\tilde{\Psi}_X\rangle$ and $|\tilde{\Psi}_Y\rangle$as

$$|\tilde{\Psi}_X\rangle = M_X\,|\eta\rangle_{ab}\,|\xi^1\rangle_c = \alpha\,|\mu\rangle_a\,|X+\rangle_b\,|\phi^1\rangle_c + \beta\,|\nu\rangle_a\,|X-\rangle_b \times |\phi^2\rangle_c$$

and

$$|\tilde{\Psi}_Y\rangle = M_Y\,|\eta\rangle_{ab}\,|\xi^1\rangle_c = \sqrt{1/2}(\alpha\,e^{i\pi/4}\,|\mu\rangle_a + \beta\,e^{-i\pi/4}\,|\nu\rangle_a)\,|Y-\rangle_b\,|\psi^1\rangle_c + \sqrt{1/2}(\alpha\,e^{-i\pi/4}\,|\mu\rangle_a + \beta\,e^{i\pi/4}\,|\nu\rangle_a)\,|Y+\rangle_A\,|\psi^2\rangle_c,$$

respectively. First, Γ must satisfy the following two expressions:

$$|\mu\rangle_a\,|X+\rangle_b = a\,|P\rangle_{ab} + b\,|R\rangle_{ab} \quad \text{with} \quad |a|^2+|b|^2 = 1$$

and

$$|\nu\rangle_a\,|X-\rangle_b = c\,|Q\rangle_{ab} + d\,|S\rangle_{ab} \quad \text{with} \quad |c|^2+|d|^2 = 1$$

such that the basis $\{|P\rangle,|Q\rangle,|R\rangle,|S\rangle\}$ can bring the following expression:

$$|\tilde{\Psi}_X\rangle = (\alpha a|P\rangle_{ab} + \alpha b\,|R\rangle_{ab})|\phi^1\rangle_c + (\beta c\,|Q\rangle_{ab} + \beta d\,|S\rangle_{ab})|\phi^2\rangle_c. \quad \text{(C1)}$$

Then the orthogonal relationship with $|\mu\rangle_a|X+\rangle_b$ determines the form of $|\mu\rangle_a|X-\rangle_b$ as

$$|\mu\rangle_a|X-\rangle_b = s(b^*|P\rangle_{ab} - a^*|R\rangle_{ab}) + t|Q\rangle_{ab} + u|S\rangle_{ab} \quad \text{with} \quad |s|^2+|t|^2+|u|^2 = 1.$$

The form of $|\nu\rangle_a|X+\rangle_b$ can be determined in the same way as

$$|\nu\rangle_a\,|X+\rangle_b = v(d^*\,|Q\rangle_{ab} - c^*\,|S\rangle_{ab}) + w\,|P\rangle_{ab} + x\,|R\rangle_{ab} \quad \text{with} \quad |v|^2+|w|^2+|x|^2 = 1.$$

Using the relationships $|\mu\rangle_a\,|Y\pm\rangle_b = \sqrt{1/2}(e^{\pm i\pi/4}\,|\mu\rangle_a\,|X+\rangle_b + e^{\mp i\pi/4}\,|\mu\rangle_a\,|X-\rangle_b)$ and

$|\nu\rangle_a\,|Y\pm\rangle_b = \sqrt{1/2}(e^{\pm i\pi/4}\,|\nu\rangle_a\,|X+\rangle_b + e^{\mp i\pi/4}\,|\nu\rangle_a\,|X-\rangle_b)$,

we can rewrite $|\tilde{\Psi}_Y\rangle$ with the basis $\{|P\rangle,|Q\rangle,|R\rangle,|S\rangle\}$ as follows:

$$i|\tilde{\Psi}_Y\rangle = (1/2)\{(i\alpha a - A)|P\rangle_{ab} + (i\beta c + C)|Q\rangle_{ab} + (i\alpha b + B)|R\rangle_{ab} + (i\beta d - D)|S\rangle_{ab}\}|\psi^1\rangle_c + (1/2)\{(i\alpha a + A)|P\rangle_{ab} + (i\beta c - C)|Q\rangle_{ab} + (i\alpha b - B)|R\rangle_{ab} + (i\beta d + D)|S\rangle_{ab}\}|\psi^2\rangle_c,$$

where $A = \alpha s b^* - \beta w$, $B = \alpha s a^* + \beta x$, $C = \beta v d^* - \alpha t$, and $D = \beta v c^* + \alpha u$.

If we take the set of conditions

$$i\alpha a = A, \tag{C2a}$$
$$i\beta d = D, \tag{C2b}$$
$$i\alpha b = B, \tag{C2c}$$
$$i\beta c = C, \tag{C2d}$$

we can obtain a desired expression for $|\tilde{\Psi}_Y\rangle$,

$$|\tilde{\Psi}_Y\rangle = \{\beta c|Q\rangle_{ab} + ab|R\rangle_{ab}\}|\psi^1\rangle_c + \{\alpha a|P\rangle_{ab} + \beta d|S\rangle_{ab}\}|\psi^2\rangle_c. \tag{C3}$$

A pair consisting of Eqs. (C1) and (C3) means the successful achievement of measurement Γ with the basis $\{|P\rangle,|Q\rangle,|R\rangle,|S\rangle\}$, where Alice can always assert the spin state of particle b correctly once she has been notified of his coding basis in the opening phase.

However, the measurement Γ provides no information on Bob's coding basis in the commitment phase. We can examine this point from the expressions for $\tilde{\rho}_X = \mathrm{Tr}_c(|\tilde{\Psi}_X\rangle\langle\tilde{\Psi}_X|)$ and $\tilde{\rho}_Y = \mathrm{Tr}_c(|\tilde{\Psi}_Y\rangle\langle\tilde{\Psi}_Y|)$ with the basis $\{|P\rangle,|Q\rangle,|R\rangle,|S\rangle\}$,

$$\tilde{\rho}_X = \frac{1}{2}\begin{bmatrix} |\alpha|^2|a|^2 & 0 & |\alpha|^2 ab^* & 0 \\ 0 & |\beta|^2|c|^2 & 0 & |\beta|^2 cd^* \\ |\alpha|^2 ba^* & 0 & |\alpha|^2|b|^2 & 0 \\ 0 & |\beta|^2 dc^* & 0 & |\beta|^2|d|^2 \end{bmatrix}$$

and

$$\tilde{\rho}_Y = \frac{1}{2}\begin{bmatrix} |\alpha|^2|a|^2 & 0 & 0 & \alpha\beta^* ad^* \\ 0 & |\beta|^2|c|^2 & \alpha^*\beta cb^* & 0 \\ 0 & \alpha\beta^* bc^* & |\alpha|^2|b|^2 & 0 \\ \alpha^*\beta da^* & 0 & 0 & |\beta|^2|d|^2 \end{bmatrix}.$$

For each diagonal element, $\tilde{\rho}_X$ and $\tilde{\rho}_Y$ have an identical value. Therefore, Alice obtains no information on Bob's coding basis. This is an intuitive proof of the impossibility of performing Γ and determining Bob's basis simultaneously.

We explain below how Alice determines (a,b), (c,d), (s,t,u), and (v,w,x) in an appropriate way when she prepares $|\eta\rangle_{ab}$. From the conditions (C2a)–(C2d), we obtain (i) a pair consisting of $a^*w + b^*x = i(\alpha/\beta)(|b|^2 - |a|^2)$ and $ct^* + du^* = i(\beta^*/\alpha^*)(|c|^2 - |d|^2)$ by computing (C2c) $\times\, b^* -$ (C2a) $\times\, a^*$ and (C2b) $\times\, d^* -$ (C2d) $\times\, c^*$, (ii) a pair consisting of $ax - bw = -(\alpha/\beta)(s - i2ab)$ and $ax + bw = s(\alpha/\beta)(|b|^2 - |a|^2)$ by calculating (C2c) $\times\, a \pm$ (C2a) $\times\, b$, and (iii) a pair consisting of $cu - dt = -(\beta/\alpha)(v - i2cd)$ and $cu + dt = v(\beta/\alpha)(|d|^2 - |c|^2)$ by calculating (C2b) $\times\, c \pm$ (C2d) $\times\, d$. We utilize the above relationships just below.

In addition to the normalization conditions, we can derive directly the following two constraints:

$$(\langle\mu|_a\langle X\pm|_b)(|\nu\rangle_a|X\pm\rangle_b) = \langle\mu \mid \nu\rangle = a^*w + b^*x = ct^* + du^*, \tag{C4a}$$
$$(\langle\mu|_a\langle X-|_b)(|\nu\rangle_a|X+\rangle_b) = -(ax - bw)s^* - (cu - dt)^*v = 0. \tag{C4b}$$

Then Eqs. (C4a) and (C4b) can be reformulated by

$$-i\alpha^*\beta\langle\mu \mid \nu\rangle = |\alpha|^2(|b|^2 - |a|^2) = |b|^2(|c|^2 - |d|^2)$$

and

$$|\alpha|^2(|S|^2 - i2s^*ab) + |\beta|^2(|v|^2 + i2vc^*d^*) = 0,$$

respectively. For example, the condition $\langle\mu|\nu\rangle = 0$ brings $|b|^2 = |a|^2 = 1/2$ and $|c|^2 = |d|^2 = 1/2$. When both $(\alpha,\beta) = (\sqrt{1/2},\sqrt{1/2})$ and $\langle\mu|\nu\rangle = 0$ are satisfied, Eqs. (9) and (10) hold.

APPENDIX D

For the $\{|p\rangle,|q\rangle,|r\rangle,|s\rangle\}$ basis or the $\{|p'\rangle,|q'\rangle,|r'\rangle,|s'\rangle\}$ basis, we can derive the following relationships with use of $|Y\pm\rangle = \{(1 \pm i)|X+\rangle + (1 \mp i)|X-\rangle\}/2$ or $|X\pm\rangle = \{(1 \mp i)|Y+\rangle + (1 \pm i)|Y-\rangle\}/2$:

$$\begin{aligned}
\sqrt{1/2}(e^{i\pi/4}|p\rangle + e^{-i\pi/4}|r\rangle) &= \sqrt{1/2}(e^{-i\pi/4}|p'\rangle + e^{i\pi/4}|r'\rangle) \\
&= |X+\rangle a|X+\rangle b, \\
\sqrt{1/2}(e^{i\pi/4}|q\rangle + e^{-i\pi/4}|s\rangle) &= \sqrt{1/2}(e^{-i\pi/4}|q'\rangle + e^{i\pi/4}|s'\rangle) \\
&= |X-\rangle a|X-\rangle b, \\
\sqrt{1/2}(e^{i\pi/4}|q\rangle + e^{-i\pi/4}|r\rangle) &= \sqrt{1/2}(e^{-i\pi/4}|q'\rangle + e^{i\pi/4}|r'\rangle) \\
&= |Y+\rangle a|Y-\rangle b, \\
\sqrt{1/2}(e^{i\pi/4}|p\rangle + e^{-i\pi/4}|s\rangle) &= \sqrt{1/2}(e^{-i\pi/4}|p'\rangle + e^{i\pi/4}|s'\rangle) \\
&= |Y-\rangle a|Y+\rangle b.
\end{aligned}$$

In the above expressions, we can confirm that each basis satisfies Γ with the definition of $\{|P\rangle,|Q\rangle,|R\rangle,|S\rangle\} \equiv \{e^{i\pi/4}|p\rangle, e^{i\pi/4}|q\rangle, e^{-i\pi/4}|r\rangle, e^{-i\pi/4}|s\rangle\}$ or $\{|P\rangle,|Q\rangle,|R\rangle,|S\rangle\} \equiv \{e^{-i\pi/4}|p'\rangle, e^{-i\pi/4}|q'\rangle, e^{i\pi/4}|r'\rangle, e^{i\pi/4}|s'\rangle\}$. Moreover, we can derive another set of the expressions as follows:

$$\begin{aligned}
\sqrt{1/2}(e^{-i\pi/4}|p\rangle + e^{i\pi/4}|r\rangle) &= \sqrt{1/2}(e^{i\pi/4}|q'\rangle + e^{-i\pi/4}|s'\rangle) \\
&= |X-\rangle a|X+\rangle b, \\
\sqrt{1/2}(e^{-i\pi/4}|q\rangle + e^{i\pi/4}|s\rangle) &= \sqrt{1/2}(e^{i\pi/4}|p'\rangle + e^{-i\pi/4}|r'\rangle) \\
&= |X+\rangle a|X-\rangle b, \\
\sqrt{1/2}(e^{-i\pi/4}|q\rangle + e^{i\pi/4}|r\rangle) &= \sqrt{1/2}(e^{i\pi/4}|p'\rangle + e^{-i\pi/4}|s'\rangle) \\
&= |Y+\rangle a|Y+\rangle b, \\
\sqrt{1/2}(e^{-i\pi/4}|p\rangle + e^{i\pi/4}|s\rangle) &= \sqrt{1/2}(e^{i\pi/4}|q'\rangle + e^{-i\pi/4}|r'\rangle) \\
&= |Y-\rangle a|Y-\rangle b
\end{aligned}$$

By use of the pair of $\{|p\rangle,|q\rangle,|r\rangle,|s\rangle\}$ and $\{|p'\rangle,|q'\rangle,|r'\rangle,|s'\rangle\}$ bases, we can realize a communication channel analogous to one out of two oblivious transfers from Bob to Alice, which has been proposed in [21]. Here we suppose that Bob sends a product state $|\varphi\rangle_a|\psi\rangle_b$ of particles a and b to Alice. He can code the two-bit of information $(u,v) \in \{(0,0), (0,1), (1,0), (1,1)\}$ on the pair by employing one of the two conjugate bases $\{|X\pm,X\pm\rangle_{ab}\}$ and $\{|Y\pm,Y\pm\rangle_{ab}\}$, where they decide the following rules:

(i) For $(u,v) = (0,0)$, he sends $|X+\rangle a|X+\rangle b$ or $|Y-\rangle a|Y+\rangle b$.

(ii) For $(u,v) = (0,1)$, he sends $|X-\rangle a|X+\rangle b$ or $|Y-\rangle a|Y-\rangle b$.
(iii) For $(u,v) = (1,0)$, he sends $|X+\rangle a|X-\rangle b$ or $|Y+\rangle a|Y+\rangle b$.
(iv) For $(u,v) = (1,1)$, he sends $|X-\rangle a|X-\rangle b$ or $|Y+\rangle a|Y-\rangle b$.

As Bob chooses either one of the two conjugate bases in a random way, Alice can never determine u and v without errors at the same time. However, if she chooses the $\{|p\rangle,|q\rangle,|r\rangle,|s\rangle\}$ basis to measure the pair, she can conclude $u = 0$ and 1 whenever she obtains the outcomes $|p\rangle$ and $|q\rangle$, respectively. If she obtains the outcome $|r\rangle$ or $|s\rangle$, she notifies him of the failure. In the same way, if she chooses the $\{|p'\rangle,|q'\rangle,|r'\rangle,|s'\rangle\}$ basis to measure the pair, she can conclude $v = 0$ and 1 whenever she obtains the outcomes $|p'\rangle$ and $|q'\rangle$, respectively. We can design the protocol such that Bob cannot infer her choice without being detected by her [21].

APPENDIX E

We can observe an intuitive relationship between the information Alice can obtain from a sequence of n pairs and Bob's detection probability. She can always choose her projection basis $\{|\tilde{P}\rangle,|\tilde{Q}\rangle,|\tilde{R}\rangle,|\tilde{S}\rangle\}$ in such way that $|\psi_X\rangle_{abc}$ [see Eq. (5)] and $|\psi_Y\rangle_{abc}$ [see Eq. (6)] are represented by

$$\begin{aligned}|\Psi_X\rangle_{\rm abc} &= \sqrt{1/2}(|X+\rangle_a|X+\rangle_b|\phi^1\rangle_c + |X-\rangle_a|X-\rangle_b|\phi^2\rangle_c)\\ &= (1/2)[(\sqrt{1-\sin 2\theta}|\tilde{P}\rangle + \sqrt{1+\sin 2\theta}|\tilde{R}\rangle|\phi^1\rangle_c)\\ &\quad + (\sqrt{1-\sin 2\theta}|\tilde{Q}\rangle + \sqrt{1+\sin 2\theta}|\tilde{S}\rangle)|\phi^2\rangle_c] \quad \text{(E1)}\end{aligned}$$

and

$$\begin{aligned}|\Psi_Y\rangle_{\rm abc} &= \sqrt{1/2}(|Y+\rangle_a|Y-\rangle_b|\psi^1\rangle_c + |Y-\rangle_a|Y+\rangle_b|\psi^2\rangle_c)\\ &= (1/2)[\{\cos\theta(|\tilde{Q}\rangle + |\tilde{R}\rangle) - \sin\theta(|\tilde{P}\rangle - |\tilde{S}\rangle)\}|\psi^1\rangle_c\\ &\quad + \{\cos\theta(|\tilde{P}\rangle + |\tilde{S}) - \sin\theta \times (|\tilde{Q}\rangle - |\tilde{R}\rangle)\}|\psi^1\rangle_c].\\ &\quad \text{(E2)}\end{aligned}$$

If the parameter angle θ decreases to zero, the basis $\{|\tilde{P}\rangle,|\tilde{Q}\rangle,|\tilde{R}\rangle,|\tilde{S}\rangle\}$ approaches the $\{|P\rangle,|Q\rangle,|R\rangle,|S\rangle\}$ basis, which gives the measurement Γ discussed in Sec. IV D. Angle θ determines the information that Alice can obtain and the probability that she is detected. In practice, when $\theta = 0$, she can obtain no information relevant to Bob's choice but she leaves behind no evidence.

First we evaluate the probability that Alice's guess on Bob's basis is correct. The diagonal elements of the density matrices are different for $\rho_X = {\rm Tr}_c(|\psi_X\rangle\langle\psi_X|)_{abc}$ and $\rho_Y = {\rm Tr}_c(|\psi_Y\rangle\langle\psi_Y|)_{abc}$ with the $\{|\tilde{P}\rangle,|\tilde{Q}\rangle,|\tilde{R}\rangle,|\tilde{S}\rangle\}$ basis,

$$\rho_X; [\rho_X]_{PP} = [\rho_X]_{QQ} = \frac{1}{4} - \frac{\sin 2\theta}{4},$$

$$[\rho_X]_{RR} = [\rho_X]_{SS} = \frac{1}{4} + \frac{\sin 2\theta}{4},$$

$$\rho_Y; [\rho_Y]_{PP} = [\rho_Y]_{QQ} = [\rho_Y]_{RR} = [\rho_Y]_{SS} = \frac{1}{4}.$$

With ρ_Y, two different pairs of outcomes $\{|\tilde{P}\rangle,|\tilde{Q}\rangle\}$ and $\{|\tilde{R}\rangle,|\tilde{S}\rangle\}$ appear with an equal probability of 1/2. On the other hand, if ρ_X is received, the pairs $\{|\tilde{P}\rangle,|\tilde{Q}\rangle\}$ and $\{|\tilde{R}\rangle,|\tilde{S}\rangle\}$ appear with different probabilities $(1-\sin 2\theta)/2$ and $(1+\sin 2\theta)/2$, respectively.

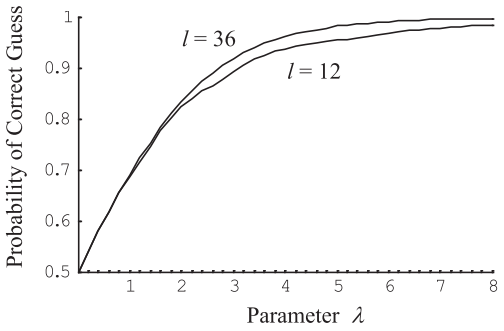


FIG. 5. Probability of Alice's correct guess with respect to parameter λ.

Therefore, she can guess the coding basis X or Y from the measurement outcomes for a set of n pairs identically prepared in ρ_X or ρ_Y. If Alice performs the measurement for l ($\leqslant n$) pairs, she can expect to observe the outcomes $\{|\tilde{P}\rangle,|\tilde{Q}\rangle\}$ with the different frequencies for ρ_X and ρ_Y. This difference is evaluated by $\Delta \equiv (\sin 2\theta\ /2)l$. To distinguish between the two different probability distributions with high probability, the difference Δ has to be sufficiently larger than the statistical variance $\delta \sim (\sqrt{l}\cos 2\theta\ )/2$ of the binary distribution relevant to ρ_X. Thus we can introduce a parameter $\lambda \equiv \Delta/\delta = \sqrt{l}\tan 2\theta$ as a quantity specifying the information she can obtain. Figure 5 shows the probability of her correct guess with respect to λ for $l = 12$ and 36.

We then estimate the probability $P_{\text{Alice-escape}}$ that she can escape the detection. Equation (E1) implies that she can always pass the examination when she is notified of the X basis by Bob. In contrast, Eq. (E2) means that she is detected with a finite probability of $\sin^2\theta$ when she is notified of the Y basis. The total amount of illegitimate access that is detectable by Bob is approximately given by $\kappa \times (m/2) \times l$ for a set of $m \times n$ particles, where (i) l is the number of pairs measured with the $\{|\tilde{P}\rangle,|\tilde{Q}\rangle,|\tilde{R}\rangle,|\tilde{S}\rangle\}$ basis per sequence, (ii) $m/2$ denotes the number of the sequence coded with the Y basis by Bob, and (iii) security parameter κ is the probability that one arbitrary particle is sampled by him for the test. Hence, the probability $P_{\text{Alice-escape}}$ can be estimated at

$$P_{\text{Alice-escape}} = (\cos^2\theta)^{k(m/2)l} = \left(\frac{1 + 1/\sqrt{1+\lambda^2/l}}{2}\right)^{\kappa(m/2)l} \quad \text{(E3a)}$$

$$\sim [\exp(-\lambda^2/8)]^{km} \quad \text{for} \quad \lambda/\sqrt{l} = \tan 2\theta \ll 1. \quad \text{(E3b)}$$

The probability P_B that Bob can detect Alice is given by $1 - P_{\text{Alice-escape}}$.

Although a large λ value improves the probability of her correct guess to close to unity, it becomes more difficult for her to escape detection. When $\sin 2\theta = 1$, the basis $\{|\tilde{P}\rangle,|\tilde{Q}\rangle,|\tilde{R}\rangle,|\tilde{S}\rangle\}$ becomes $\{i|X-\rangle_a|X+\rangle_b, i|X+\rangle_a|X-\rangle_b, |X+\rangle_a|X+\rangle_b, |X-\rangle_a|X-\rangle_b\}$. This basis choice is exactly the straightforward strategy that we discussed in Sec. III D, where the probability of detection per particle is $\cos^2\theta = 1/2$ and the

parameter λ becomes infinitely large. By substituting $l = 2$ as the average value of the required access times, we can obtain Eq. (3) for the probability P_B. If Alice chooses a small angle θ and a large time l for the measurements to achieve a large λ value, the probability $P_{\text{Alice-escape}}$ is estimated by Eq. (E3b). By comparing the term $[\exp(-\lambda^2/8)]^\kappa m$ in Eq. (E3b) with the term $(1/2)^{\kappa m}$ on the right-hand side of Eq. (3), we can observe that her strategy here is not advantageous. In fact, $\exp(-\lambda^2/8)$ is quite a bit smaller than $1/2$ for the λ value, that causes a high probability in guessing.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.

[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000), Chap. 12.6.

[3] J. Kilian, in *Proceedings of the 20th ACM Symposium on the Theory of Computing* (ACM, New York, 1988), p. 20; G. Brassard, C. Crepeau, R. Jozsa, and D. Langlois, in *Proceedings of the 34th Annual IEEE Symposium on the Foundation of Computer Science* (IEEE Computer Society, Los Alamitos, CA, 1993), p. 362.

[4] H. K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997); H. K. Lo, Phys. Rev. A **56**, 1154 (1997).

[5] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).

[6] A. Kent, Phys. Rev. A **61**, 042301 (2000).

[7] G. M. D'Ariano, D. Kretschmann, D. Schlingemann, and R. F. Werner, Phys. Rev. A **76**, 032328 (2007).

[8] H. K. Lo and H. F. Chau, Physica D **120**, 177 (1998).

[9] A. Ambainis, J. Comput. Syst. Sci. **68**, 398 (2004).

[10] D. Mayers, L. Salvail, and Y. Chiba-Kohno, e-print arXiv:quant-ph/9904078 (1999).

[11] D. Aharonov, A. Ta-Shma, U. V. Vazirani, and A. C. Yao, in *Proceedings of the 32nd ACM Symposium on the Theory of Computing* (ACM, New York, 2000), p. 705, e-print arXiv:quant-ph/0004017; the task of a quantum bit escrow is defined in this paper. We employ their definition.

[12] R. W. Spekkens and T. Rudolph, Phys. Rev. Lett. **89**, 227901 (2002).

[13] L. Goldenberg, L. Vaidman, and S. Wiesner, Phys. Rev. Lett. **82**, 3356 (1999).

[14] A. Kent, Phys. Rev. Lett. **90**, 237901 (2003).

[15] G. P. He and Z. D. Wang, Phys. Rev. A **73**, 012331 (2006).

[16] L. Hardy and A. Kent, Phys. Rev. Lett. **92**, 157901 (2004).

[17] C. Mochon, Phys. Rev. A **70**, 032312 (2004).

[18] S. Ishizaka, Phys. Rev. Lett. **100**, 070501 (2008).

[19] J. J. Sakurai, *Modern Quantum Mechanics* (Addison-Wesley, New York, 1994), revised edition, Chap. III.

[20] L. Vaidman, Y. Aharonov, and D. Z. Albert, Phys. Rev. Lett. **58**, 1385 (1987).

[21] K. Shimizu and N. Imoto, Phys. Rev. A **66**, 052316 (2002); **67**, 034301 (2003).