Dilemma that Cannot Be Resolved by Biased Quantum Coin Flipping

Satoshi Ishizaka[1,2]

[1]*Nano Electronics Research Laboratories, NEC Corporation, 34 Miyukigaoka, Tsukuba 305-8501, Japan*
[2]*INQIE, the University of Tokyo, 4-6-1 Komaba, Meguro-ku, Tokyo 153-8505, Japan*

(Received 9 March 2007; revised manuscript received 3 December 2007; published 19 February 2008)

We show that a biased quantum coin flip (QCF) cannot provide the performance of a black-boxed biased coin flip, if it satisfies some fidelity conditions. Although such a QCF satisfies the security conditions of a biased coin flip, it does not realize the ideal functionality and, therefore, does not satisfy the demands for universally composable security. Moreover, through a comparison within a small restricted bias range, we show that an arbitrary QCF is distinguishable from a black-boxed coin flip unless it is unbiased on both sides of parties against insensitive cheating. We also point out the difficulty in developing cheat-sensitive quantum bit commitment in terms of the uncomposability of a QCF.

DOI: 10.1103/PhysRevLett.100.070501 PACS numbers: 03.67.Dd, 03.67.Mn

Consider Alice and Bob who have just divorced. They agree to flip a coin to decide who gets their car, but they live in different cities. How do they flip a coin by telephone? This is a well-known introduction to a coin flip [1], which is now an important cryptographic primitive on a communication network. Another important primitive is bit commitment (BC). The purpose of BC is to realize the scenario in which Alice commits to a bit (b) and later she reveals it; this is done such that Bob cannot know b until Alice reveals it, and she must reveal b as it is. A fair coin flip is realized by using secure BC.

An effort was made to construct unconditionally secure quantum BC (QBC), but unfortunately it was shown that all previously proposed QBC protocols are broken by the so-called entanglement attack [2]. After controversial discussions, it was then generally accepted that unconditionally secure QBC is impossible [3]. It was also proved that a perfectly fair quantum coin flip (QCF) is impossible [4–7].

Fortunately, quantum mechanics enables biased coin flipping [6,8–11]. In a biased QCF, if both Alice and Bob are honest, the outcome is either 0 or 1, each with probability $1/2$. A dishonest party can cheat to bias the probability to $1/2+\epsilon$, but it is ensured that the bias satisfies $|\epsilon|<1/2$; so a dishonest party cannot fully control the outcome. Moreover, when a dishonest party tries to largely bias the probability, an honest party sometimes obtains the outcome "reject," which identifies the presence of cheating. In this Letter, however, we only consider insensitive cheating such that the outcome reject never occurs. Even through insensitive cheating, a dishonest party can generally bias the probability, whose maximum (or minimum) is called the threshold for cheat sensitivity [9].

On the other hand, let us imagine ideal biased coin flipping such that a black box outputs a common random bit to both parties. A dishonest party can bias the probability of the outcome but can do nothing else because the party cannot touch the inside of the box at all. A biased QCF, at first glance, realizes the black-boxed coin flip, because it is ensured by the laws of physics that the bias range is limited to $|\epsilon|<1/2$ against all possible operations for cheating.

In this Letter, however, we show that a biased QCF generally does not provide the performance of a black-boxed biased coin flip, when it is used to resolve a quantum dilemma. Although such a QCF satisfies the security conditions of a biased coin flip, it does not realize the ideal functionality. This warns that, if a QCF is combined with another quantum cryptographic protocol, an unexpected security hole will occur.

Now, let us introduce a quantum dilemma where, in some sense, the car in the previous dilemma concerning divorce is replaced with a fully quantum object: an entangled state. Suppose that Alice is required to send half of a maximally entangled state to Bob. However, Bob doubts whether she sends the entangled state honestly. On the other hand, dishonest Bob sometimes destroys the shared entanglement and Alice worries about this. Later, Bob wishes to confirm that Alice has honestly sent the entangled state, and Alice wishes to confirm that the entanglement has been maintained safely. Therefore, both wish to get the whole state in his or her hand, because the entanglement cannot be evaluated from each half of the state (the situation is analogous to quantum bit escrow [8] as we will discuss later). Since both wishes cannot be satisfied simultaneously, let us introduce a coin flip to resolve this dilemma, and thus consider the following protocol:

Protocol 1 (sharing and maintaining entanglement).

Stage 1 (sharing).—Alice prepares $|\phi\rangle_{AB}=(|00\rangle+|11\rangle)/\sqrt{2}$ and sends the B qubit to Bob. This maximal entanglement is to be shared and maintained.

Stage 2 (coin flip).—Alice and Bob execute a coin flipping subprotocol. If the output of the subprotocol is 0 (1), Alice (Bob) loses the coin flip.

Stage 3 (verification).—The winner of the coin flip obtains both A and B qubits and checks whether or not the state of the AB qubits is $|\phi\rangle$ by a projective measurement. If the state is not $|\phi\rangle$, the party detects the cheating of the other party with nonzero probability.

Suppose that Alice is dishonest and sends a partially entangled state $|\Phi(a)\rangle_{AB} = \sqrt{a}|00\rangle + \sqrt{1-a}|11\rangle$ $(1/2 < a \leq 1)$ instead of $|\phi\rangle$ in stage 1. Let P_d be the probability that Bob detects this cheating. The performance of the protocol is characterized by the minimal value of P_d for a given a. Let us consider the case where a black-boxed coin flip is used in stage 2. The allowable maximal (minimal) bias of the probability of the outcome 0 is $\epsilon_{\max}$ ($\epsilon_{\min}$) and $\epsilon_{\min} < 0 < \epsilon_{\max}$. Exploiting this controllable bias range, Alice tries to decrease P_d. However, as proved later, the best strategy is to constantly bias the probability to $1/2 + \epsilon_{\min}$, and to send the A qubit as it is in stage 3, when she loses the coin flip. Namely,

$$P_d \geq P_d^{\text{box}} \equiv (1/2 + \epsilon_{\min})(1/2 - \sqrt{a(1-a)}). \qquad (1)$$

Our concern is whether or not a QCF can provide the same performance. To investigate this, let us recall a unitary model of a QCF [6,7], where all classical communication is replaced by quantum communication and all measurements are postponed until the end of the protocol. We can thus assume that Alice or Bob's operation in each round is a unitary transformation. Following the model in [6], let $|\psi_{\text{ini}}\rangle$ be an initial state of the protocol. Alice first applies U_1 to her own qubits and sends some qubits to Bob, and then Bob applies U_2 and sends some qubits to Alice. They repeat this, and the final state after all the rounds is $|\psi_{\text{fin}}\rangle = (\cdots U_3 U_2 U_1)|\psi_{\text{ini}}\rangle$. Alice and Bob then measure $|\psi_{\text{fin}}\rangle$ to obtain the outcome. When both are honest, they can obtain 0 or 1 with probability 1/2, and so $|\psi_{\text{fin}}\rangle$ is decomposed such that $|\psi_{\text{fin}}\rangle = |\psi_0\rangle + |\psi_1\rangle$, where $|\psi_c\rangle$ is a part of leading to the outcome c, $\langle\psi_0|\psi_1\rangle = 0$, and $\| \psi_c \|^2 = 1/2$. Moreover, since both must know the outcome certainty, $F(\varrho_{X,0}, \varrho_{X,1}) = 0$, where $F(\varrho, \sigma) = (\text{tr}\sqrt{\varrho^{1/2}\sigma\varrho^{1/2}})^2$ is the fidelity and $\varrho_{X,c}$ is the normalized reduced state of $|\psi_c\rangle$ for the party $X = A, B$ [6].

Let $\epsilon_{\max}$ be the possible maximal bias for the outcome 0 of this QCF, which is achieved if Alice applies U_i' instead of U_i. The final state is then $|\psi_{\text{fin}}'\rangle = (\cdots U_3' U_2 U_1')|\psi_{\text{ini}}\rangle = |\psi_0'\rangle + |\psi_1'\rangle$, where $\langle\psi_0'|\psi_1'\rangle = 0$ and $\| \psi_0' \|^2 = 1/2 + \epsilon_{\max}$. Moreover, $\varrho_{B,c}'$, which is the reduced state of $|\psi_c'\rangle$, must not be conclusively distinguished from $\varrho_{B,c}$ by Bob so that the cheating is insensitive [hence $\text{supp}(\varrho_{B,c}') \subset \text{supp}(\varrho_{B,c})$ where $\text{supp}(\varrho)$ denotes the support space of ϱ]. Since Alice must know the outcome certainty, $F(\varrho_{A,0}', \varrho_{A,1}') = 0$; otherwise the cheating is sensitive due to the disagreement of their outcomes. Likewise, let $\epsilon_{\min}$ be the minimal bias that is achieved by U_i''. The corresponding final state, the reduced state, and so on, are also indicated by the double prime. These satisfy the same conditions as in the $\epsilon_{\max}$ case, except $\| \psi_0'' \|^2 = 1/2 + \epsilon_{\min}$.

Now, let us consider Alice's cheating strategy for protocol 1. In the QCF subprotocol executed in stage 2, she applies the controlled unitary transformations

$$O_i = |0\rangle\langle 0|_A \otimes U_i'' + |1\rangle\langle 1|_A \otimes U_i' \qquad (2)$$

to $|\Phi(a)\rangle_{AB} \otimes |\psi_{\text{ini}}\rangle$. The whole state after all the rounds of the QCF subprotocol is

$$\sqrt{a}|00\rangle_{AB} \otimes (|\psi_0''\rangle + |\psi_1''\rangle) + \sqrt{1-a}|11\rangle_{AB} \otimes (|\psi_0'\rangle + |\psi_1'\rangle) = \sqrt{a}|00\rangle_{AB} \otimes |\psi_0''\rangle + \sqrt{1-a}|11\rangle_{AB} \otimes |\psi_0'\rangle$$
$$+ \sqrt{a}|00\rangle_{AB} \otimes |\psi_1''\rangle + \sqrt{1-a}|11\rangle_{AB} \otimes |\psi_1'\rangle. \qquad (3)$$

The first two and the last two terms in Eq. (3) lead to the outcomes 0 and 1, respectively. Since Bob's reduced state of the system employed for the QCF is $a\varrho_{B,c}'' + (1-a)\varrho_{B,c}'$ for the outcome c, and $\text{supp}(\varrho_{B,c}'')$, $\text{supp}(\varrho_{B,c}') \subset \text{supp}(\varrho_{B,c})$, he knows the outcome certainty by a regular measurement. Alice's reduced state is $a|0\rangle\langle 0|_A \otimes \varrho_{A,c}'' + (1-a)|1\rangle\langle 1|_A \otimes \varrho_{A,c}'$, and she can obtain the outcome certainty using the projector $|0\rangle\langle 0|_A \otimes \Pi_c'' + |1\rangle\langle 1|_A \otimes \Pi_c'$, where Π_c' (Π_c'') distinguishes $\varrho_{A,0}'$ and $\varrho_{A,1}'$ ($\varrho_{A,0}''$ and $\varrho_{A,1}''$). Suppose that the outcome of the QCF is 0; the state of the AB qubits will be checked by Bob in stage 3. Before Alice sends the A qubit to Bob, she applies $|0\rangle\langle 0|_A \otimes I + |1\rangle\langle 1|_A \otimes V$, where V maximizes the overlap between $|\psi_0''\rangle$ and $|\psi_0'\rangle$ such that $|\langle\psi_0''|V|\psi_0'\rangle|^2 = \| \psi_0'' \|^2 \| \psi_0' \|^2 F(\varrho_{B,0}', \varrho_{B,0}'')$ [12]. Through this procedure, the whole state becomes $|\Psi_0\rangle = \sqrt{a}|00\rangle_{AB} \otimes |\psi_0''\rangle + \sqrt{1-a}|11\rangle_{AB} \otimes V|\psi_0'\rangle$, and P_d in this strategy is

$$\begin{aligned} P_d^Q &= \text{tr}[|\Psi_0\rangle\langle\Psi_0|(I - |\phi\rangle\langle\phi|)_{AB}] \\ &= \tfrac{1}{2}[a(\tfrac{1}{2} + \epsilon_{\min}) + (1-a)(\tfrac{1}{2} + \epsilon_{\max})] \\ &\quad - [a(1-a)(\tfrac{1}{2} + \epsilon_{\min})(\tfrac{1}{2} + \epsilon_{\max})F]^{1/2}, \qquad (4) \end{aligned}$$

where $F \equiv F(\varrho_{B,0}', \varrho_{B,0}'')$. Comparing Eqs. (1) and (4), it is found that $P_d^Q < P_d^{\text{box}}$ if $1 > a > (r-1)^2/[4(\sqrt{rF} - 1)^2 + (r-1)^2]$ and

$$F > 1/r \equiv (1 + 2\epsilon_{\min})/(1 + 2\epsilon_{\max}). \qquad (5)$$

This result shows that, if a QCF has the property of Eq. (5), there exists a finite range of a in which $P_d^Q < P_d^{\text{box}}$. Therefore, it is concluded that such a QCF cannot provide the performance of a black-boxed coin flip.

The point of the above cheating strategy is that it is possible to superpose two biasing operations U_i' and U_i''. This enables Alice to correlate the state of the AB qubits with the outcome of the QCF such that the state is more entangled than $|\Phi(a)\rangle_{AB}$ whenever Alice loses the QCF (and thus P_d decreases). For this purpose, Alice utilizes the difference of $\| \psi_0'' \|$ and $\| \psi_0' \|$ (i.e., the difference of $\epsilon_{\max}$ and $\epsilon_{\min}$). However, this procedure has created undesired entanglement between the AB qubits and the system employed for the QCF, and so Alice needs to disentangle them; otherwise the entanglement of the AB qubits will be washed out by the undesired entanglement. This is done by increasing the overlap between $|\psi_0'\rangle$ and $|\psi_0''\rangle$. Note that the disentangling process is incomplete (unless $F = 1$), and, as a result, the state of the AB qubits is a mixed state.

To further investigate the difference between a QCF and a black-boxed coin flip, let us introduce the following biasing operation: Suppose that Alice has a local ancilla qubit and she prepares the initial state $|\psi_{\rm ini}\rangle \otimes (\sqrt{1-x}|0\rangle_a + \sqrt{x}|1\rangle_a)$ for the QCF, where the subscript a denotes the ancilla qubit. Then, if she applies $\tilde{U}_i = U_i \otimes |0\rangle\langle 0|_a + U_i'' \otimes |1\rangle\langle 1|_a$ to the initial state, the QCF is biased by $x\epsilon_{\rm min}$. Moreover, when the outcome is 0, Bob's reduced state is $\tilde{\varrho}_{B,0} = \varrho_{B,0} + x(\varrho''_{B,0} - \varrho_{B,0})$. Now, let us imagine a special circumstance where Alice's ability is restricted such that she can only use $\tilde{U}_i$ for biasing the QCF (the point is that she cannot directly employ U_i''). As a result, the bias of the QCF is restricted within $[x\epsilon_{\rm min}, 0]$, and, therefore, it may be natural to compare it with the black-boxed coin flip with the same bias range. Then, if Alice adopts the cheating strategy like Eq. (2), where U_i and $\tilde{U}_i$ are superposed as $O_i = |0\rangle\langle 0|_A \otimes \tilde{U}_i + |1\rangle\langle 1|_A \otimes U_i$ to decrease P_d, we have Eq. (5) in which $\epsilon_{\rm max}$ and $\epsilon_{\rm min}$ are replaced by 0 and $x\epsilon_{\rm min}$, respectively; so $P_d^Q < P_d^{\rm box}$ if $F(\varrho_{B,0}, \tilde{\varrho}_{B,0}) > 1 + 2x\epsilon_{\rm min}$. However, this fidelity condition is always satisfied for $x \to 0$ because $F(\varrho_{B,0}, \tilde{\varrho}_{B,0}) = 1 - \mathcal{O}(x^2)$. The same discussion holds if the bias is restricted within $[0, x\epsilon_{\rm max}]$. In this way, an arbitrary QCF is distinguishable from a black-boxed coin flip (as $P_d^Q < P_d^{\rm box}$) unless the QCF is unbiased against insensitive cheating.

To see these results graphically, the following two bounds are plotted in Fig. 1:

$$\text{(I) } F(\epsilon) > 1/(1+2\epsilon) \quad \text{for } \epsilon_{\rm min} = 0 \quad \text{and} \quad \epsilon = x\epsilon_{\rm max} \geq 0,$$
$$\text{(II) } F(\epsilon) > 1 + 2\epsilon \quad \text{for } \epsilon_{\rm max} = 0 \quad \text{and} \quad \epsilon = x\epsilon_{\rm min} \leq 0.$$

If the fidelity F of the QCF, whose bias is forcedly restricted within (I) $[0, \epsilon]$ and (II) $[\epsilon, 0]$, is located outside the gray region, the QCF is distinguishable from the black-boxed coin flip with the same bias range.

All of the above discussions hold when Bob is dishonest, if we assume that Bob's dishonest action in stage 1 is to perform the following positive operator valued measurement (POVM) of the B qubit:

$$\begin{aligned} M_0 &= \sqrt{a}|0\rangle\langle 0| + \sqrt{1-a}|1\rangle\langle 1|, \\ M_1 &= \sqrt{1-a}|0\rangle\langle 0| + \sqrt{a}|1\rangle\langle 1|, \end{aligned} \tag{6}$$

where $M_0^\dagger M_0 + M_1^\dagger M_1 = \mathbb{1}_B$. Depending on the outcome of the POVM, the postmeasured state becomes $|\Phi(a)\rangle_{AB}$ or $|\Phi(1-a)\rangle_{AB}$, each with probability 1/2. He then tries to decrease P_d. For $|\Phi(a)\rangle$, the same cheating strategy as used with dishonest Alice is applicable. This is the case for $|\Phi(1-a)\rangle$, if the role of $|0\rangle_B$ and $|1\rangle_B$ is exchanged in the controlled operations of the cheating strategy. Then, we have the same bound for $F \equiv F(\varrho'_{A,1}, \varrho''_{A,1})$, but $\epsilon_{\rm max}$ and $\epsilon_{\rm min}$ must be read as those for the outcome 1 of the QCF. This implies that a QCF must be unbiased on both Alice and Bob's sides simultaneously, so that it is indistinguishable from a black-boxed coin flip.

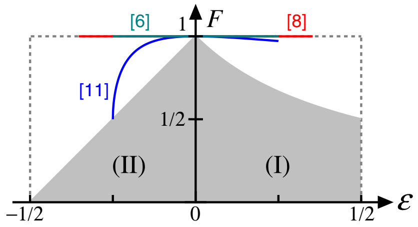

FIG. 1 (color online). Bound for fidelity (F) as a function of bias (ϵ). If a QCF is located outside the gray region, it is distinguishable from a black-boxed coin flip. The fidelity for the QCF protocols proposed in [6,8,11] is also plotted, where we assumed dishonest Bob.

So, let us now prove Eq. (1). The general action of dishonest Alice when deciding on the bias of a black-boxed coin flip is described by a POVM $\{L_\epsilon\}$ of the A qubit ($\int d\epsilon L_\epsilon^\dagger L_\epsilon = \mathbb{1}_A$). The probability of the outcome 0 is then biased to $\frac{1}{2} + \epsilon$, and the state of the AB qubits will be checked by Bob with this probability. The singlet fraction $\mathcal{F}(\sigma) = \langle\phi|\sigma|\phi\rangle$ is bounded as $\mathcal{F}(\sigma) \leq [{\rm tr}\sigma + N_B(\sigma)]/2$, where $N_B(\sigma)$ is negativity [13] (the subscript denotes the partial transposition with respect to the B qubit). Since N_B is an entanglement monotone [14], the average cannot be increased by the local operation of the POVM. Hence,

$$\begin{aligned} P_d &= \int_{\epsilon_{\rm min}}^{\epsilon_{\rm max}} d\epsilon \left(\frac{1}{2} + \epsilon\right) {\rm tr}[L_\epsilon |\Phi(a)\rangle\langle\Phi(a)| L_\epsilon^\dagger (I - |\phi\rangle\langle\phi|)] \\ &\geq \frac{1}{2}\left(\frac{1}{2} + \epsilon_{\rm min}\right)\left[1 - \int d\epsilon N_B(L_\epsilon|\Phi(a)\rangle\langle\Phi(a)|L_\epsilon^\dagger)\right] \\ &\geq \frac{1}{2}\left(\frac{1}{2} + \epsilon_{\rm min}\right)[1 - N_B(|\Phi(a)\rangle)], \end{aligned} \tag{7}$$

and we have Eq. (1), because $N_B(|\Phi(a)\rangle) = 2\sqrt{a(1-a)}$.

So far, we have focused on the comparison through P_d. Now, we concentrate on a case where $P_d = 0$; the probability of detecting cheating is strictly zero, and so the state of the AB qubits must be precisely $|\phi\rangle$ when it is checked in stage 3. The performance of protocol 1 is then characterized by the maximal allowed value of a for a dishonest party. Suppose again that Alice is dishonest. For a black-boxed coin flip, it is found from Eq. (1) that $a = 1/2$ must hold; so she cannot cheat at all under $P_d = 0$, as expected. For a QCF, however, it is found from Eq. (4) that $P_d^Q = 0$ even for $a = 1/2 + (\epsilon_{\rm max} - \epsilon_{\rm min})/[2(1 + \epsilon_{\rm max} + \epsilon_{\rm min})] > 1/2$ if $F = 1$. This occurs for an arbitrary pair of biasing operations as far as $F = 1$ for the pair. So, by replacing $\epsilon_{\rm max}$ and $\epsilon_{\rm min}$ with ϵ' and ϵ'', it is found that Alice can successfully cheat if the QCF satisfies

$$\Delta a \equiv \max_{\epsilon', \epsilon'', F=1} (\epsilon' - \epsilon'')/[2(1 + \epsilon' + \epsilon'')] > 0, \tag{8}$$

where the maximization is taken over all the pairs of the two biasing operations subject to $F(\varrho'_{B,0}, \varrho''_{B,0}) = 1$. Such a QCF also cannot provide the performance of a black-boxed coin flip, and even allows the cheating that is completely prohibited by a black-boxed coin flip. Note that the same discussion holds again for dishonest Bob.

As a simple example, let us analyze the following protocol [15] (this is not a true QCF because the probability of the outcome is not $1/2$ even if both are honest).

Protocol 2 (QCF-like).—Alice prepares $|\phi\rangle_{CD}$ and sends the D qubit to Bob. He optionally checks $|\phi\rangle_{CD}$ (getting the C qubit). If he uses the option, this protocol automatically outputs 1. Otherwise, he measures the D qubit in the $\{|0\rangle, |1\rangle\}$ basis and sends the result to Alice, and she confirms the validity by measuring the C qubit. This protocol then outputs the measurement result.

In this protocol, it is confirmed that $F(\varrho'_{A,1}, \varrho''_{A,1}) = 1$ for Bob's two biasing operations of (i) he always uses the option ($\epsilon' = 1/2$), and (ii) he measures the D qubit, and if the result is 1, he uses the option ($\epsilon'' = 0$). Hence, we have $\Delta a \geq 1/6$ and $a \geq 2/3$ from Eq. (8). On the other hand, it can be shown that $a \leq 2/3$ for Bob's general action [16]. Therefore, it is found that the cheating strategy considered in this Letter has optimally maximized a under $P_d = 0$. This is the case for the 3-round protocol in [8] ($a = \cos\frac{\pi}{8}$) and for the optimal 3-round protocol in [6] ($a = 3/4$), for which we assumed dishonest Bob.

As mentioned before, the situation considered in this Letter is analogous to quantum bit escrow [8], which is a weak variant of QBC such that either Alice or Bob can detect cheating with nonzero probability.

Protocol 3 (quantum bit escrow).

Stage 1 (commitment).—To commit to $b = 0$ (1), Alice prepares either $|0\rangle_B$ or $|-\rangle_B$ ($|1\rangle_B$ or $|+\rangle_B$), each with probability $1/2$, which is written as $|\xi_{bx}\rangle$ where x denotes the encoding basis. She then sends the B qubit to Bob.

Stage 2 (opening).—Alice reveals b.

Stage 3 (verification).—Either Alice or Bob obtains the B qubit and checks whether or not it is $|\xi_{bx}\rangle$ to detect cheating (Alice reveals x if Bob checks the state).

The question of whether or not it is possible to use a biased QCF for the purpose of deciding which party will check the B qubit in stage 3 was raised in [8]. If this is so, the resultant protocol is cheat-sensitive QBC (CSQBC) [8,15], which enables both to detect cheating, albeit with smaller nonzero probability.

However, since the resultant CSQBC has the same structure as in protocol 1, it struggles with the difference between a QCF and a black-boxed coin flip. For example, if $\Delta a > 0$, dishonest Bob can steal partial information about b before the opening stage by a POVM as in Eq. (6) [16]. Alice cannot detect his cheating because he can precisely recover $|\xi_{bx}\rangle$ from a state collapsed by the POVM whenever he loses the QCF, as he recovers $|\phi\rangle$ from $|\Phi(a)\rangle$ or $|\Phi(1-a)\rangle$. Likewise, if $\Delta a > 0$, dishonest Alice can change the probability of revealing $b = 0$ in the opening stage. Therefore, a QCF that is combined with bit escrow should not satisfy Eq. (8) on both sides of parties. Unfortunately, this is not the case in the example of CSQBC suggested in [8], and even in [15]. We described the cheating method for those in [16]. Note that, as far as we know, an explicit protocol for secure CSQBC has not been found yet [16], contrary to the widespread belief that CSQBC is possible.

To summarize, we showed that a QCF cannot provide the performance of a black-boxed coin flip, if it satisfies the fidelity conditions of Eqs. (5) or (8). Such a QCF obviously does not fulfill the conditions for universally composable (UC) security, the demands for ensuring the security of a cryptographic primitive regardless of how it is used in applications [17]. This result is quite a contrast to quantum key distribution (QKD), where a QKD protocol is automatically UC secure if it satisfies the general security conditions [18]. Moreover, through a comparison within a small restricted bias range, we showed that an arbitrary QCF is distinguishable from a black-boxed coin flip unless it is unbiased on both sides of parties against insensitive cheating, i.e., unless it is a cheat-sensitive unbiased QCF. Finally, we discussed the relation to CSQBC constructed from bit escrow and a QCF, and pointed out the difficulty in developing secure CSQBC in terms of the uncomposability condition of Eq. (8). We hope these results shed some light on the important open problem of whether or not quantum mechanics enables cheat-sensitive bit commitment and cheat-sensitive unbiased coin flipping.

[1] M. Blum, in *Proceedings of the IEEE Spring Computer Conference* (IEEE, New York, 1982), p. 133.

[2] H.-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997); D. Mayers, *ibid.* **78**, 3414 (1997).

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

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

[5] D. Mayers, L. Salvail, and Y. Chiba-Kohno, arXiv:quant-ph/9904078.

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

[7] A. Ambainis *et al.*, in *Proceedings of the 19th IEEE Conference on Computational Complexity* (IEEE Computer Society, Washington, DC, 2004), p. 250.

[8] D. Aharonov, A. Ta-Shma, U. V. Vazirani, and A. C. Yao, in *Proceedings of the 32nd ACM Symposium on Theory of Computing* (ACM, New York, 2000), p. 705.

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

[10] C. Mochon, in *Proceedings of the 45th IEEE Symposium on Foundation of Computer Science* (IEEE Computer Society, Washington, DC, 2004), p. 2.

[11] R. Colbeck, Phys. Lett. A **362**, 390 (2007).

[12] R. Jozsa, J. Mod. Opt. **41**, 2315 (1994).

[13] G. Vidal and R. F. Werner, Phys. Rev. A **65**, 032314 (2002).

[14] M. B. Plenio, Phys. Rev. Lett. **95**, 090503 (2005).

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

[16] S. Ishizaka, arXiv:quant-ph/0703099v3.

[17] M. Ben-Or and D. Mayers, arXiv:quant-ph/0409062.

[18] M. Ben-Or *et al.*, *Theory of Cryptography* (Springer, Berlin, Heidelberg, 2005), pp. 386–406.