Non-static Quantum Bit Commitment

Jeong Woon Choi,[1,*] Dowon Hong,[1] Ku-Young Chang,[1] Dong Pyo Chi,[2] and Soojoon Lee[3]

[1] *Information Security Research Division, Electronics and Telecommunications Research Institute, Daejeon 305-700, Korea*
[2] *Department of Mathematical Sciences, Seoul National University, Seoul 151-747, Korea*
[3] *Department of Mathematics and Research Institute for Basic Sciences, Kyung Hee University, Seoul 130-701, Korea*

(Dated: September 15, 2009)

Quantum bit commitment has been known to be impossible by the independent proofs of Mayers, and Lo and Chau, under the assumption that the whole quantum states right before the unveiling phase are static to users. We here provide an unconditionally secure non-static quantum bit commitment protocol with a trusted third party, which is not directly involved in any communications between users and can be limited not to get any information of commitment without being detected by users. We also prove that our quantum bit commitment protocol is not secure without the help of the trusted third party. The proof is basically different from the Mayers-Lo-Chau's no-go theorem, because we do not assume the staticity of the finally shared quantum states between users.

PACS numbers: 03.67.Dd, 03.67.Hk, 03.67.Mn

I. INTRODUCTION

As one of the most basic and important cryptographic primitives, a bit commitment (BC) scheme has a lot of applications to crucial cryptographic protocols including coin flipping, interactive zero-knowledge proof, oblivious transfer, verifiable secret sharing, multiparty secure computation, and so on [1, 2, 3, 4, 5, 6]. There have also been several quantum approaches [7, 8] to guarantee the unconditional security of BC protocols, as quantum key distribution (QKD) protocols [9, 10] have done. Unfortunately, in the middle of the 1990's Mayers [11, 12], and independently Lo and Chau [13] (MLC) proved that quantum principles cannot be helpful to construct an unconditionally secure BC protocol, in contrast to a brilliant development of QKD protocols [14, 15, 16]. The impossibility of quantum bit commitment (QBC) is called the MLC's no-go theorem, which implies a severe drawback of quantum cryptography. Since then, there have been several results about QBC protocols, some of which are for the possibility through new schemes and theories [17, 18, 19], others of which are for the trade-off relations between the possibility and the impossibility [20, 21].

The most important assumption of the MLC's no-go theorem is that every QBC protocol results in a *static* quantum state, and thus both users exactly know about what it is before the unveiling time. For any initial states of Alice and Bob, $|\chi\rangle_A$ ($\chi = 0$ or 1) and $|\psi\rangle_B$, the finally shared quantum state will be given as $U_{AB}(|\chi\rangle_A \otimes |\psi\rangle_B)$, where U_{AB} represents all the algorithms involved in the protocol and is necessarily opened and known to all participants. If the QBC protocol satisfies the perfect concealment, then by the Gisin-Hughston-Jozsa-Wootters (GHJW) theorem [22] there exists a local unitary operation S_A such that $(S_A \otimes I)U_{AB}(|0\rangle_A \otimes |\psi\rangle_B) = U_{AB}(|1\rangle_A \otimes |\psi\rangle_B)$. By delaying the measurements and applying S_A to the local system, Alice is able to change her committed bit surreptitiously without being detected by Bob. This is the main stream of the MLC's no-go theorem.

However, we focus on the fact that S_A actually is given depending on the Bob's initial state $|\psi\rangle_B$. So, it would be better to denote the Alice's strategy by $S_A(\psi)$ rather than S_A. Even though it is true that there exists an exact operation $S_A(\psi)$ for each $|\psi\rangle_B$ whenever the protocol is perfectly concealing, Alice could neither figure out nor make use of $S_A(\psi)$ appropriately, if $|\psi\rangle_B$ is randomly given and kept unknown to her. A QBC protocol to realize the above situation is here called a *non-static* QBC protocol.

In this paper, by investigating the possibility and the impossibility of such non-static QBC protocols, we construct an unconditionally secure QBC protocol with the help of a trusted third party (TTP), and prove that our non-static QBC protocol is not possible without the help of a TTP. Although the existence of a TTP can be a weak point as in general cryptographic primitives, the TTP in our protocol plays only a little role to provide quantum sources to carry classical bit information. Moreover, the TTP is not actually involved in any communications between users, and cannot get any information about the commitment without being detected by users.

II. NON-STATIC QBC PROTOCOLS

Hereafter we consider a more generalized version of QBC protocols which varies the resulting states according to the initial state $|\psi\rangle_B$ generated by Bob (or a TTP), and thus the strategy $S_A(\psi) \otimes I$ by a dishonest Alice might be also changed according to $|\psi\rangle_B$. One possible way to accomplish the above property is that Bob (or a TTP), instead of Alice, prepares and sends an initial quantum state $|\psi\rangle_B$ to Alice, where $|\psi\rangle_B$ should be kept unknown to Alice. Then Alice applies an associate uni-

*Electronic address: jw˙choi@etri.re.kr

tary operator to $|\psi\rangle_B$ to commit a bit χ.

For example, suppose that when $\chi = 0$, Alice chooses one of M and N randomly, and similarly when $\chi = 1$, one of J and K randomly, where M, N, J, and K are defined as

$$\begin{aligned} M &= I, \quad N = -i\sigma_y \\ J &= \frac{1-i}{2\sqrt{2}}\left[I + i\left(\sigma_x - \sigma_y + \sigma_z\right)\right] \\ K &= \frac{1+i}{2\sqrt{2}}\left[I + i\left(\sigma_x + \sigma_y - \sigma_z\right)\right], \end{aligned} \tag{1}$$

where σ_x, σ_y, and σ_z are the Pauli matrices. To guarantee the randomness, Alice prepares an auxiliary state $|+\rangle_A = \frac{|0\rangle_A + |1\rangle_A}{\sqrt{2}}$, and then she applies a unitary operator either $|0\rangle_A\langle 0| \otimes M + |1\rangle_A\langle 1| \otimes N$ (if $\chi = 0$) or $|0\rangle_A\langle 0| \otimes J + |1\rangle_A\langle 1| \otimes K$ (if $\chi = 1$) to $|+\rangle_A \otimes |\psi\rangle_B$ so that she finally obtains the following states

$$\begin{aligned} |\Phi_0(\psi)\rangle_{AB} &= \frac{|0\rangle_A \otimes M|\psi\rangle_B + |1\rangle_A \otimes N|\psi\rangle_B}{\sqrt{2}} \quad \text{and} \\ |\Phi_1(\psi)\rangle_{AB} &= \frac{|0\rangle_A \otimes J|\psi\rangle_B + |1\rangle_A \otimes K|\psi\rangle_B}{\sqrt{2}}. \end{aligned} \tag{2}$$

By performing the standard measurement on her local system $\mathcal{H}_A$, Alice provides Bob with an uniformly distributed ensemble, either $\xi_0(\psi) = \{M|\psi\rangle_B, N|\psi\rangle_B\}$ or $\xi_1(\psi) = \{J|\psi\rangle_B, K|\psi\rangle_B\}$ as shown in TABLE I.

TABLE I: The change of the initial states $|\psi\rangle_B = m|0\rangle_B + n|1\rangle_B$ ($|m|^2 + |n|^2 = 1$): It shows how the initial states $|\psi\rangle_B$ are transformed by unitary operators M, N, J, and K randomly chosen according to χ. ($|\pm\rangle_B$ denotes $\frac{|0\rangle_B \pm |1\rangle_B}{\sqrt{2}}$.)

χ	Operators	$\|0\rangle_B$	$\|1\rangle_B$	$\|\psi\rangle_B = m\|0\rangle_B + n\|1\rangle_B$
0	M	$\|0\rangle_B$	$\|1\rangle_B$	$m\|0\rangle_B + n\|1\rangle_B$
	N	$\|1\rangle_B$	$-\|0\rangle_B$	$m\|1\rangle_B - n\|0\rangle_B$
1	J	$\|+\rangle_B$	$i\|-\rangle_B$	$m\|+\rangle_B + in\|-\rangle_B$
	K	$\|-\rangle_B$	$i\|+\rangle_B$	$m\|-\rangle_B + in\|+\rangle_B$

Without an additional information about the ensembles, Bob will regard them as a density operator, either $\rho_0(\psi) = (M|\psi\rangle_B\langle\psi|M^\dagger + N|\psi\rangle_B\langle\psi|N^\dagger)/2$ or $\rho_1(\psi) = (J|\psi\rangle_B\langle\psi|J^\dagger + K|\psi\rangle_B\langle\psi|K^\dagger)/2$, respectively.

Let us consider the cases that $|\psi\rangle_B = |0\rangle_B$ and $|\psi\rangle_B = |+\rangle_B$. It is very easy to show that $\rho_0(\psi = 0) = \rho_1(\psi = 0) = \rho_0(\psi = +) = \rho_1(\psi = +) = I/2$. However, we can ask a question such as "Is there any proper strategy S_A to change not only $|\Phi_0(\psi = 0)\rangle_{AB}$ to $|\Phi_1(\psi = 0)\rangle_{AB}$ but also $|\Phi_0(\psi = +)\rangle_{AB}$ to $|\Phi_1(\psi = +)\rangle_{AB}$?" The answer is NO. In fact, up to the left multiplication of diagonal matrices, $S_A(\psi = 0)$ should be $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, while $S_A(\psi = +)$ should be $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ i & -1 \end{pmatrix}$. This means that a certain fixed attack by Alice cannot be available for all $|\psi\rangle_B$, and therefore Alice should be able to choose a strategy appropriate to an unknown $|\psi\rangle_B$.

However, this example has a problem that the QBC protocol is not perfectly concealing. If Bob prepares the initial state as $|\psi\rangle_B = \frac{|0\rangle_B + i|1\rangle_B}{\sqrt{2}}$, then he can know Alice's commitment in advance, because ρ_0 and ρ_1 are obviously different. To solve this problem, we employ a TTP, and then investigate the securities of QBC protocols with and without the help of the TTP in the next two subsections.

A. Non-static QBC Protocol with a TTP

Alice and TTP previously share $\mathcal{N}$ maximally entangled states $|\Psi^-\rangle_{TA} = (|01\rangle_{TA} - |10\rangle_{TA})/\sqrt{2}$ satisfying $|\Psi^-\rangle_{TA} = (U \otimes U)|\Psi^-\rangle_{TA}$ up to the global phase for all unitary operators U.

(i) [Pre-Commitment] TTP performs random orthogonal measurements $M_i = \{|\phi_i\rangle_T\langle\phi_i|_T, |\phi_i^\perp\rangle_T\langle\phi_i^\perp|_T\}$ ($1 \le i \le \mathcal{N}$) on his side of $|\Psi^-\rangle_{TA}$'s. Then Alice and TTP always have the opposite state, that is, if TTP's result is $|\phi_i\rangle_T$ ($|\phi_i^\perp\rangle_T$), then Alice must have $|\psi_i\rangle_A = |\phi_i^\perp\rangle_A$ ($|\phi_i\rangle_A$). However, Alice does not know what $|\psi_i\rangle_A$'s are actually, because TTP keeps M_i unknown to her.

(ii) [Commitment] To commit a bit χ, Alice encodes χ into $|\psi_i\rangle_A$ by applying an operator P_i randomly chosen from M, N, J, and K as follows. If Alice wants to commit 0, then she sends Bob $M|\psi_i\rangle_A$ or $N|\psi_i\rangle_A$ at random, and if she wants to commit 1, then she sends $J|\psi_i\rangle_A$ and $K|\psi_i\rangle_A$ randomly.

(iii) [Holding Phase] It proceeds without doing anything for a certain period which users agreed with at the beginning stage of the protocol.

(iv) [Unveiling Phase] At a specific later time, Alice publicly announces all P_i's and then TTP all M_i's and measurement outcomes. Then Bob verifies the commitment by checking whether the measurement outcomes are always opposite or not, when he performs M_i's on $P_i^\dagger P_i|\psi_i\rangle_A$. If Alice is honest, then the measurement outcomes should be opposite for all i.

In step (ii), as noticed previously, by using the ancillary state $|+\rangle_{A'}$ and the non-local unitary operations such as $|0\rangle_A\langle 0| \otimes M + |1\rangle_A\langle 1| \otimes N$ and $|0\rangle_A\langle 0| \otimes J + |1\rangle_A\langle 1| \otimes K$ according to χ, Alice obtains $|\Phi_0\rangle_{A'A} = \left(|0\rangle_{A'} \otimes M|\psi\rangle_A + |1\rangle_{A'} \otimes N|\psi\rangle_A\right)/\sqrt{2}$ and $|\Phi_1\rangle_{A'A} = \left(|0\rangle_{A'} \otimes J|\psi\rangle_A + |1\rangle_{A'} \otimes K|\psi\rangle_A\right)/\sqrt{2}$. However, due to the randomness of $|\psi\rangle_A$, $|\Phi_\chi\rangle_{A'A}$ will be changed every time. These states can come to not only product states but also maximally entangled state. So, Alice could not control the relation between $|\Phi_0\rangle_{A'A}$ and $|\Phi_1\rangle_{A'A}$ as she wants, without the knowledge of $|\psi\rangle_A$'s (actually M_i's).

Of course, we need to calculate the success probability of the delayed measurement attack proposed in the MLC's no-go theorem, which can be measured with the fidelity $F(|\psi\rangle, |\phi\rangle) = |\langle\psi|\phi\rangle|^2$. Suppose that, to change

the committed bit from 0 to 1, Alice applies a local unitary operation $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. The success probability is

$$\mathbb{F} = \frac{1}{2}\{F(aM|\psi\rangle_A + bN|\psi\rangle_A, J|\phi\rangle_A) + F(cM|\psi\rangle_A + dN|\psi\rangle_A, K|\phi\rangle_A)\}, \quad (3)$$

and therefore, in the Bloch representation, $|\psi\rangle_A = \cos(\theta/2)|0\rangle_A + e^{i\phi}\sin(\theta/2)|1\rangle_A$ $(0 \le \theta \le \pi, 0 \le \phi \le 2\pi)$, the expected success probability is

$$\begin{aligned} & \frac{1}{4\pi}\int_0^{2\pi}\int_0^{\pi} \mathbb{F}\sin\theta \; d\theta d\phi \\ = & \frac{|a|^2+|b|^2+|c|^2+|d|^2}{4} + \frac{Re(a\overline{b}-c\overline{d})}{6} \\ = & \frac{1}{2} + \frac{2Re(a\overline{b})}{6} \le \frac{1}{2} + \frac{|a\overline{b}|}{3} \le \frac{2}{3}, \end{aligned} \quad (4)$$

where $\overline{z}$ is the complex conjugate of a given complex number z. Since the protocol is repeated $\mathcal{N}$ times, Alice's attack is detected with the probability greater than $1-(2/3)^{\mathcal{N}}$ which goes to 1 as $\mathcal{N} \to \infty$. That is, this QBC protocol satisfies the asymptotic bindingness, where the level of security follows as noticed in [20].

We should also consider the concealment. One of the assumptions of our protocol is that Alice and TTP previously share the singlet states. This means that Bob has no way to interrupt the quantum channel between them to get some information. That is to say, Bob should gain information about the commitment from only quantum states given by Alice. Another assumption is that TTP should choose M_i's at true random. So, the finally encoded states will appear to Bob as $I/2$, which guarantees the perfect concealment.

To transmit only digital information through classical channels, TTP can choose the bases of M_i's in a discretized subset of the Bloch space. For instance, TTP can select finite points uniformly dividing the sub-circle spanned by $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$. Since our protocol satisfies the perfect concealment for all initial states $|\psi\rangle_A$ such that $m\overline{n} \in \mathbb{R}$, so do all points in the sub-circle. Of course, the success probability will be changed a little bit but less than 1, and therefore this protocol still satisfies the bindingness. Such a restriction on the domain of initial states gives us one more advantage, which prohibits TTP from generating the initial states such that $m\overline{n} \notin \mathbb{R}$ and knowing Alice's commitment in advance. TTP should always announce Bob the right information about his measurements, because if TTP announces dishonestly, then the measurements in the wrong bases will make a disturbance on the correlation between Alice and Bob, and thus the dishonest behavior will be detected by users.

In result, the quantum entanglement shared between Alice and TTP guarantees not only the non-staticity, but therefore also the unconditional security of our protocol, which cannot be realized by the classical cryptographic theories.

B. Non-static QBC Protocol without a TTP

We here deal with a self-enforcing QBC protocol (without a TTP), which is slightly modified from our previous QBC protocol like that Bob, instead of TTP, generates initial quantum states $|\psi\rangle_B$ and Alice applies unitary operators to $|\psi\rangle_B$ to commit χ.

The following lemma is a necessary and sufficient condition for our self-enforcing QBC protocol to be perfectly concealing against Bob using any kind of quantum entangled state $|\Psi\rangle_{BB'}$ on the extended system $\mathcal{H}_B \otimes \mathcal{H}_{B'}$.

Lemma 1. *A non-static QBC protocol is perfectly concealing for all qubits $|\psi\rangle_B$ and all entangled state $|\Psi\rangle_{BB'}$ if and only if M, N, J, and K should satisfy the following equations*

$$\begin{aligned} M|0\rangle_B\langle 0|M^\dagger + N|0\rangle_B\langle 0|N^\dagger &= J|0\rangle_B\langle 0|J^\dagger + K|0\rangle_B\langle 0|K^\dagger, \\ M|1\rangle_B\langle 1|M^\dagger + N|1\rangle_B\langle 1|N^\dagger &= J|1\rangle_B\langle 1|J^\dagger + K|1\rangle_B\langle 1|K^\dagger, \\ & \textit{and} \\ M|0\rangle_B\langle 1|M^\dagger + N|0\rangle_B\langle 1|N^\dagger &= J|0\rangle_B\langle 1|J^\dagger + K|0\rangle_B\langle 1|K^\dagger. \end{aligned} \quad (5)$$

Proof. By a direct calculation, we first prove that the above condition is a necessary and sufficient condition for $\rho_0(\psi) = \rho_1(\psi)$ for all qubits $|\psi\rangle_B = m|0\rangle_B + n|1\rangle_B$. It is very clear that if M, N, J, and K satisfy Eq. (5), then $\rho_0(\psi) = \rho_1(\psi)$. Conversely, we should show that all M, N, J, and K such that $\rho_0(\psi) = \rho_1(\psi)$ satisfy Eq. (5). The first two equations of Eq. (5) can be easily derived from the cases that $m \neq 0, n = 0$ and $m = 0, n \neq 0$. Therefore, M, N, J, and K should eventually satisfy $\mathrm{Re}\left(m\overline{n}(M|0\rangle_B\langle 1|M^\dagger + N|0\rangle_B\langle 1|N^\dagger)\right) = \mathrm{Re}\left(m\overline{n}(J|0\rangle_B\langle 1|J^\dagger + K|0\rangle_B\langle 1|K^\dagger)\right)$, for all m and n. Considering the cases that $m = n = 1$ and $m = 1, n = i$, we can obtain the third equation of Eq. (5). It is trivial to extend the necessary and sufficient condition to all bipartite entangled states $|\Psi\rangle_{BB'}$ on $\mathcal{H}_B \otimes \mathcal{H}_{B'}$, where $\dim \mathcal{H}_B = 2$ and $\dim \mathcal{H}_{B'}$ is arbitrary, because $|\Psi\rangle_{BB'}$ has the Schmidt decomposition [23] and we can regard $|0\rangle_B$ and $|1\rangle_B$ as eigenvectors of the density operator $\mathrm{tr}_{B'}(|\Psi\rangle_{BB'}\langle\Psi|)$. □

In addition, we also figure out what kind of unitary operators M, N, J, and K are able to satisfy the perfect concealment, that is, the necessary and sufficient condition given in Lemma 1. Unfortunately, Theorem 2 tells us that there is a strategy for Alice to cheat the commitment freely, regardless of whether she knows the initial quantum states or not.

Theorem 2. *If a non-static QBC protocol is perfectly concealing, then there exists a local unitary operator $S_A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $J = aM + bN$ and $K = cM + dN$.*

Proof. Considering the orthogonality and the GHJW theorem for the perfect concealment, we can let M, N, J,

TABLE II: The parametrization for the unitary operators M, N, J, and K satisfying that $\rho_0(\psi) = \rho_1(\psi)$ for all $|\psi\rangle_B$:

$$|x|^2 + |y|^2 = 1 \ (y \neq 0),\ |\alpha| = 1,\ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} s & t \\ u & v \end{pmatrix} : \text{unitary}$$

Operators	$\|0\rangle_B$	$\|1\rangle_B$
M	$\|0\rangle_B$	$\|1\rangle_B$
N	$x\|0\rangle_B + y\|1\rangle_B$	$\alpha(\overline{y}\|0\rangle_B - \overline{x}\|1\rangle_B)$
J	$(a+bx)\|0\rangle_B + by\|1\rangle_B$	$t\alpha\overline{y}\|0\rangle_B + (s - t\alpha\overline{x})\|1\rangle_B$
K	$(c+dx)\|0\rangle_B + dy\|1\rangle_B$	$v\alpha\overline{y}\|0\rangle_B + (u - v\alpha\overline{x})\|1\rangle_B$

and K be unitary matrices as shown in TABLE II, without loss of generality. In this case, it is obvious that M, N, J, and K satisfy the first two equations of Eq. (5). By the third equation of Eq. (5), all parameters in TABLE II should follow that

$$\begin{aligned} \overline{\alpha}xy &= (a+bx)\overline{t\alpha}y + (c+dx)\overline{v\alpha}y, \\ -y\overline{\alpha}x &= by(\overline{s} - \overline{t\alpha}x) + dy(\overline{u} - \overline{v\alpha}x), \\ 1 - \overline{\alpha}x^2 &= (a+bx)(\overline{s} - \overline{t\alpha}x) + (c+dx)(\overline{u} - \overline{v\alpha}x), \\ \overline{\alpha}y^2 &= by^2\overline{t\alpha} + dy^2\overline{v\alpha}. \end{aligned} \quad (6)$$

We first consider the case that $\rho_0(\psi = 0)$ is invertible (of rank 2), that is, $y \neq 0$. Eq. (6) can be rewritten as

$$\begin{aligned} 1 &= a\overline{s} + c\overline{u}, \\ 0 &= b\overline{s} + d\overline{u}, \\ 0 &= a\overline{t} + c\overline{v}, \text{ and} \\ 1 &= b\overline{t} + d\overline{v}. \end{aligned} \quad (7)$$

This means that $\begin{pmatrix} \overline{s} & \overline{t} \\ \overline{u} & \overline{v} \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, that is, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$. Therefore, there exists a unitary operator $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $J = aM + bN$ and $K = cM + dN$.

Let us consider the case that the rank of $\rho_0(\psi = 0)$ is 1, that is $y = 0$, where we can reparameterize M, N, J, and K as shown in TABLE III. For the perfect concealment, the parameters should satisfy

$$j\overline{k} + l\overline{m} = \alpha\overline{\beta} + \gamma\overline{\delta}. \quad (8)$$

If $j\overline{k} + l\overline{m} \neq 0$, then $j\overline{k} = \alpha\overline{\beta}$, $l\overline{m} = \gamma\overline{\delta}$ or $j\overline{k} = \gamma\overline{\delta}$, $l\overline{m} = \alpha\overline{\beta}$, because of the unity of parameters. This property means that the matrices have the relations such as $M \propto J$, $N \propto K$ or $M \propto K$, $N \propto J$, where $A \propto B$ denotes $A = cB$ for a constant c. Therefore, the commitments according to χ's are actually same and thus make no sense. If $j\overline{k} + l\overline{m} = 0$, under the assumption that $j\overline{k} \neq l\overline{m}$ (Otherwise, for all quantum states $|\psi\rangle_B$, $\text{rank}(\rho_0(\psi)) = \text{rank}(\rho_1(\psi)) = 1$, and thus $M \propto N \propto J \propto K$, which is meaningless.), we can find a unitary operator $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $J = aM + bN$ and $K = cM + dN$, where a, b, c, and d are given as

$$\begin{aligned} a &= \frac{l\beta - m\alpha}{lk - mj}, b = \frac{k\alpha - j\beta}{lk - mj}, c = \frac{l\delta - m\gamma}{lk - mj}, \text{ and} \\ d &= \frac{k\gamma - j\delta}{lk - mj}. \end{aligned}$$

This completes the proof. □

TABLE III: The reparametrization of TABLE II for the unitary operators M, N, J, and K satisfying that $\text{rank}(\rho_0(\psi = 0)) = 1$:

$$|j| = |k| = |l| = |m| = 1,\ |\alpha| = |\beta| = |\gamma| = |\delta| = 1$$

Operators	$\|0\rangle_B$	$\|1\rangle_B$
M	$j\|0\rangle_B$	$k\|1\rangle_B$
N	$l\|0\rangle_B$	$m\|1\rangle_B$
J	$\alpha\|0\rangle_B$	$\beta\|1\rangle_B$
K	$\gamma\|0\rangle_B$	$\delta\|1\rangle_B$

By using $S_A \otimes I$, Alice can freely exchange unitary operators M and N with J and K so that she can cheat her committed bit with certainty without being detected by Bob. Therefore, we can find out that, even though dishonest Bob makes use of arbitrary dimensional ancillary system, if Alice and Bob communicate through the only two-dimensional channel, then any non-static QBC protocols we propose are not secure, and in fact, the perfect concealment makes the non-static QBC protocol static without the help of a TTP.

III. CONCLUSION

We have dealt with a new QBC scheme which can be not static so that the final quantum states are determined randomly and kept unknown to all participants until the unveiling phase. However, we would like to emphasize that our QBC scheme does not oppose the MLC's no-go theorem, but ensures its security only by enforcing Alice to change the attack strategy according to the unknown initial quantum information.

We have shown that it is possible to construct an unconditionally secure QBC protocol with the help of a TTP, where the role of the TTP can be limited not to get any information of the committed bit in advance and actually users can perceive any dishonest behaviors of the TTP. Unfortunately, we have also proved that the non-static QBC protocol is not secure without the help of the TTP. In a self-enforcing non-static QBC protocol, the necessary and sufficient condition for the perfect concealment eventually makes the QBC protocol static. It

would be important to check if we can extend the impossibility of the self-enforcing QBC protocols to the cases with no limits on the dimension of quantum channels and the number of the quantum states in ensembles.

Acknowledgments

This work was supported by the IT R&D program of MKE/IITA (Grant No. 2005-Y-001-05, "Developments of next generation security technology" and Grant No. 2008-F-035-02, "Development of Key Technologies for Commercial Quantum Cryptography Communication System"). D.P.C. was supported by a Korea Science and Engineering Foundation (KOSEF) grant funded by the Korean Government (MOST). S.L. was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (Grant No. 2009-0076578).

[1] M. Blum, in *Proceedings of the 24th IEEE Computer Society International Conference*, (IEEE, New York, 1982), pp. 133–137.
[2] G. Brassard, D. Chaum, and C. Crépeau, Journal of Computer and System Sciences, **37**, 156 (1988).
[3] S. Goldwasser, S. Micali, and C. Rackoff, SIAM Journal on Computing, **18**, 186 (1989).
[4] O. Goldreich, S. Micali, and A. Wigderson, Journal of ACM, **38**, 691 (1991).
[5] C. H. Bennett, G. Brassard, C. Crépeau, and M. -H. Skubiszewska, in *Advances in Cryptology: Proceedings of Crypto '91*, Lecture Notes in Computer Science Vol. 576 (Springer-Verlag, 1992), p. 351–366.
[6] J. Kilian, in *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, Chicago, 1988, p. 20–31.
[7] G. Brassard and C. Crépeau, in *Advances in Cryptology: Proceedings of Crypto'90*, Lecture Notes in Computer Science Vol. 537 (Springer-Verlag, Berlin, 1991), p. 49–61.
[8] G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois, in *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science*, 1993 (IEEE, Los Alamitos, 1993), p. 362–371.
[9] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, 1984 (IEEE, New York, 1984), p. 175–179.
[10] H. -K. Lo and H. F. Chau, Science **283**, 2050–2056 (1999).
[11] D. Mayers, LANL Report No. quant-ph/9603015.
[12] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).
[13] H. K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).
[14] P. A. Hiskett et al., New J. Phys. **8**, 193–197 (2006).
[15] R. Ursin et al., Nature Physics **3**, 481–486 (2007).
[16] G. Smith, J. M. Renes, and J. A. Smolin, Phys. Rev. Lett. **100**, 170502 (2008).
[17] A. Kent, Phys. Rev. Lett. **83**, 1447 (1999).
[18] L. Hardy and A. Kent, Phys. Rev. Lett. **92**, 157901 (2004).
[19] G. P. He, Phys. Rev. A. **74**, 022332 (2006).
[20] R. W. Spekkens and T. Rudolph, Phys. Rev. A **65**, 012310 (2001).
[21] G. M. D'Ariano, D. Kretschmann, D. Schlingemann, and R. F. Werner, Phys. Rev. A. **76**, 032328 (2007).
[22] N. Gisin, Helv. Phys. Acta **62**, 363 (1989); L. P. Hughston, R. Jozsa, and W. K. Wootters Phys. Lett. A **183**, 14 (1993).
[23] E. Schmidt, Math. Ann. **63**, 433 (1907).