Another simple unconditionally secure quantum bit commitment protocol — the use of bit-value dependent evidence state space*

Horace P. Yuen

Department of Electrical and Computer Engineering, Department of Physics and Astronomy, Northwestern University, Evanston, IL 60208

It is shown how the evidence state space in quantum bit commitment may be made to depend on the bit value 0 or 1 with split entangled pairs. As a consequence, one can obtain a protocol that is perfectly concealing, but is also e-binding because the bit-value dependent evidence space prevents the committing party from cheating by means of a local transformation.

In the previous paper [1], we showed how quantum teleportation may be used to perform unconditionally secure quantum bit commitment (US QBC) by preventing the committing party (Adam) from entangling the different commitment possibilities. In this paper, we will show that an even simpler US QBC protocol may be obtained by individuating the evidence state space via split entangled pairs, so that perfect concealing can be achieved, while Adam is faced with a bit-value dependent evidence space. This in turn ensures that Adam cannot cheat by means of a local transformation. The underlying idea can be explained as follows, which has already been described in Appendix B of Ref. [2]. In the usual US QBC “impossibility proof” (IP) formulation, Adam is supposedly honest when he entangles the different possible opening states \( \rho_i \) for \( b = 0 \). Actually, if he des not, i.e., if he sends \( \rho_i \in H^B \) to Babe with probability \( p_i \) but without entanglement, he will not be able to carry out the entanglement cheating with his local transformation, even though the same \( \rho_0^B = \rho_1^B \) for perfect concealing would appear to Babe. Thus, the same condition \( \rho_0^B = \rho_1^B \) may obtain for Babe under different physical situations for Adam that would allow or prevent him from cheating. This interplay of classical and quantum randomness can be utilized to yield a truly simple US QBC protocol as follows.

Let \( |k\rangle \), \( k \in \{1,2\} \), be two openly known orthogonal qubit states, \( |1\rangle|2\rangle = 0 \). Let Babe prepare two states, for bit value \( b \in \{0,1\} \):

\[
|\Psi_b\rangle = \frac{1}{\sqrt{2}} \sum_k |f_{bk}\rangle |k_b\rangle,
\]

where \( |f_{bk}\rangle \in H^{B_1} \), \( |k_b\rangle \in H^{B_2} \), \( k_b \in \{1,2\} \), \( \langle f_{b1}|f_{b2}\rangle = 0 \). She keeps \( H^{B_1}_{b1} \otimes H^{B_1}_{b1} \) and sends the ordered \( H^{B_1}_{b2} \otimes H^{B_1}_{b2} \) to Adam. Let Adam commit \( b = 0 \) by sending back \( H^{B_2}_{b2} \) to Babe while keeping \( H^{B_2}_{b1} \) himself, and vice versa for \( b = 1 \). He opens by announcing \( b \) and Babe verifies by measuring the corresponding \( |\Phi_b\rangle \) on \( H^{B_1}_{b1} \otimes H^{B_1}_{b1} \). (One may require Adam to return \( H^{B_2}_{b2} \) upon opening for another verification by Babe, but there is no need for it.) Thus, we have a situation in which the evidence state space is \( H^{B_2}_{b2} \) that depends on \( b \). The two different \( H^{B_2}_{b2} \) are individuated by entanglements to different \( H^{B_1}_{b1} \). It is clear that regardless of the concealing situation, Adam cannot cheat by switching \( H^{B_2}_{b2} \), which is already in Babe’s possession, to \( H^{B_2}_{b1} \) with probability one.

A perfectly concealing protocol can be obtained in the following way. Let Adam apply the following transformation on \( H^{B_2}_{b2} \) before committing it: \( |\Psi_b\rangle \in H^{B_1}_{b1} \otimes H^{B_1}_{b2} \equiv H^{B_1}_{b} \) becomes \( |\Phi_b\rangle \in H^{B_2}_{b} \otimes H^A \),

\[
|\Phi_b\rangle = \frac{1}{\sqrt{2}} \sum_{k,i} |f_{bk}\rangle V_i |k_b\rangle |e_i\rangle,
\]

where \( i \in \{1,2,3,4\} \), \( |e_i\rangle \) complete orthonormal in \( H^A \), and \( V_i \) are four unitary qubit operators given by \( I, \sigma_x, -i\sigma_y, \sigma_z \) in terms of the Pauli spin operators when \( |1\rangle \) and \( |2\rangle \) lie on the qubit \( z \)-axis. Eq. (2) can be obtained by the unitary transformation \( \sum_i |e_i\rangle \langle e_i| \otimes V_i \) on \( H^A \otimes H^{B_2}_{b2} \) with initial state \( |\psi_A\rangle \in H^A \) that has \( \langle e_i|\psi_A\rangle =\frac{1}{\sqrt{2}} \). By tracing over \( H^A \), it is easy to verify from (2) that under either \( b, \rho_0^B = \rho_1^B = \frac{1}{2} (I_2 \otimes I_1) \), where \( I_2 \) is the identity on \( H^{B_2}_{b2} \otimes H^{B_1}_{b2} \) and \( I_1 \) is the identity qubit operator on the space \( H^{B_1}_{b1} \) that Adam sends to Babe as evidence, but to Babe it is just an identity on a qubit which can be either \( H^{B_1}_{b1} \) or \( H^{B_1}_{b2} \). Adam opens by announcing \( b \) and sending \( H^A \) to Babe, who verifies by measuring the projection onto \( |\Phi_b\rangle \) on \( H^{B_2}_{b} \otimes H^A \). (She can actually also measure \( \{ |f_{bk}\rangle \} \) and \( \{ |e_i\rangle \} \) first.)

This protocol QBC4p lies outside the IP formulation because \( |\Phi_b\rangle \in H^{B_2}_{b} \otimes H^A \) with \( H^{B_2}_{b} \) \( b \)-dependent. It is perfectly concealing because Babe does not know which \( H^{B_2}_{b} \) is committed to her, and Adam cannot cheat perfectly because the Schmidt decomposition from the IP does not apply with \( b \)-dependent \( H^{B_2}_{b} \). Intuitively, it is evident that the entanglement of \( H^{B_2}_{b2} \) to \( H^{B_1}_{b1} \) cannot be changed to \( H^{B_1}_{b2} \) by means of operations on \( H^{B_2}_{b2} \). Indeed, assuming as usual that Adam opens perfectly on \( b = 0 \), i.e., with probability one, which means Babe has \( H^{B_1}_{b1} \otimes H^{B_2}_{b2} \) in her possession as evidence, Adam can only cheat by sending in \( H^A \) with a local transformation \( U^A \) and announcing \( b = 1 \) instead. It is clear that since the state Babe verifies on would not be \( |\Phi_1\rangle \) in such a

*NOTE: This paper is the second of three papers that together provide a detailed description of various gaps in the QBC “impossibility proof,” as well as security proofs for five different protocols, QBC1, QBC2, QBC2.1, QBC4, and QBC5. They also explain and correct some of the claims on my previous QBC protocols.

†Electronic address: yuen@ece.northwestern.edu
case, Adam cannot cheat perfectly. In fact, the state that Babe verifies on becomes

$$\frac{1}{8} \text{tr}_{H_{12}} \left( \sum_k |f_{1k}\rangle |k_1\rangle \right) \left( \sum_{k'} \langle f_{1k'}| \langle k'_1| \right) \otimes \text{tr}_{H_{12}} \left( U^A|\Phi_0\rangle \langle \Phi_0| U^{A\dagger} \right)$$  

which yields the maximum probability of successful cheating, $p_A = \frac{1}{2}$, with $U^A = I$ when Babe measures $|\Phi_1\rangle \langle \Phi_1|$. (Adam cannot do better by sending in another $H^A$ instead of $H^A$.) As in the case of IP formulation, the exact $\{|f_{1k}\rangle\}$ and $\{|e_i\rangle\}$ do not matter as long as they form an orthogonal set. Note that we have already contradicted the IP claim that Adam can cheat perfectly even with perfect $b = 0$ opening when the protocol is perfectly concealing.

When the $b = 0$ perfect opening condition is relaxed, it is clear that Adam still cannot cheat perfectly, but it is possible that the overall successful opening probability (honest plus cheating) may be better than $1/2 \times 1 + 1/2 \times 1/2 = \frac{3}{4}$. By continuity it can be seen that Adam’s optimum cheating probability $P^A$ is arbitrarily close to $p_A = \frac{1}{2}$ if the $b = 0$ opening probability is arbitrarily close to 1, the case of interest.

Before proceeding, a few clarifying comments on this protocol are in order. First, Adam cannot cheat by permutation entanglement of the states in $H^B_{12}$ and $H^B_{12}$, which would lead to a nonzero failure probability of opening for either $b$ and belongs to the situation just discussed above. Secondly, Adam cannot cheat by using different $V_i$ in 2, for exactly the same reasons as the discussions surrounding 3. Thus, he should follow the protocol, and thus prevents Babe from cheating. Third, Adam cannot cheat by measuring on either $H^B_{12}$ before commitment. Such an action merely disentangles $H^B_{12}$ from $H^B_{12}$ and prevents Babe from verifying.

Protocol QBC4 is obtained when QBC4p is extended to a sequence of $\{|\Psi_0\rangle \langle \Psi_1|\}$, $\ell \in \{1, \ldots, n\}$, each of the form 4, with $|f_{b\ell}\rangle \in H^B_{12}$, $|k_\ell\rangle \in H^B_{12}$, etc. Babe should send Adam $\{H^B_{12} \otimes H^B_{12}\}$ and Adam should commit to Babe $\{H^B_{12}\}$ for the same $b$ for all $\ell$, and opens by announcing $b$ and submitting $\{H^A_\ell\}$, with Babe verifying $\{\Phi_\ell\}$ on $H^B_\ell \otimes H^A_\ell$ for each $\ell$. Since there is no new entanglement possibility for Adam, the protocol is perfectly concealing with $P^A = p_\beta^A$ going to zero exponentially in $n$. Thus, QBC4 is perfectly concealing and $\epsilon$-binding for any $\epsilon > 0$ by letting $n$ be large.

So far we have assumed Babe is honest in sending Adam $\{H^B_{12} \otimes H^B_{12}\}$ with states $\{|\Psi_0\rangle \langle \Psi_1|\}$. However, she could cheat by sending in different states, e.g., unentangled states which are orthogonal for $b = 0$ and 1. This kind of cheating is not accounted for in the IP formulation, which assumes the parties are honest during commitment, but can be handled in at least two different ways as discussed in Ref. 3. The second way in a game-theoretic formulation is quantitatively described there, and can be used for QBC4 since Babe still cannot cheat by entanglement over $\ell$ under Adam’s actions $V_i$. In Appendix A of this paper, the first way using an ensemble is analyzed. We summarize our perfectly concealing and $\epsilon$-binding protocol, assuming that either one of these methods has been employed to guarantee legal states have been sent from Babe.

**PROTOCOL QBC4**

(i) Babe sends Adam $n$ ordered pairs $\{H^B_{12} \otimes H^B_{12}\}$ of qubits, $\ell \in \{1, \ldots, n\}$, which are entangled to $\{H^B_{12} \otimes H^B_{12}\}$ in her possession in states $\{|\Psi_0\rangle \langle \Psi_1|\}$ of the form 4.

(ii) To commit $b$, Adam applies, for each $\ell$, $\sum_i |e_i\rangle \langle e_i| \otimes V_i$ on $H^B_\ell \otimes H^B_\ell$, resulting in a state $|\Phi_\ell\rangle$ of the form 2, and sends $\{H^B_{12}\}$ to Babe as evidence.

(iii) Adam opens by announcing $b$ and submitting $\{H^A_\ell\}$. Babe verifies by projective measurements of $\{|\Phi_\ell\rangle\}$ for all $\ell$.

This protocol belongs to what we call Type 4 protocols, in which split entangled pairs are used to individuate state spaces $H^B_{12}$ for Adam, while his bit choice of $H^B_{12}$ or $H^B_{12}$ is indistinguishable to Babe. In this way, both perfect concealing and $\epsilon$-binding can be obtained in a situation not covered by the impossibility proof. However, if only $\epsilon$-concealing is to be obtained, the same idea of bit-value dependent state space can be used without Babe’s entangled pairs to achieve $\epsilon$-binding also. In one such case, Babe only sends one unentangled qubit to be returned for $b = 0$ and another for $b = 1$, from which Adam picks with his bit choice and commits it among many decoy states 3 to achieve $\epsilon$-concealing. It should be clear that Adam cannot achieve with success probability arbitrarily close to one in this situation, and thus the protocol can be extended to an $\epsilon$-binding one. This and another implementation of this idea of $b$-dependent $H^B_{12}$ are treated under Type 2 protocols in Ref. 3. To reiterate the main idea underlying these protocols: the evidence state space can be different to one party (Adam) depending on the bit value, but indistinguishable to the other party (Babe) through classical randomness.

**APPENDIX A: HONESTY GUARANTEE FROM AN ENSEMBLE**

One general approach to guarantee with probability arbitrarily close to 1 that a party $B$ is sending a “legal” state from $|\psi_k\rangle$ allowed by the protocol, or at least sending the entangled superposition

$$|\Psi\rangle = \sum_k \lambda_k |\psi_k\rangle_B |f_k\rangle_C$$  

for orthonormal $|f_k\rangle_C \in H^C$, is the following. She sends in $N$ states, each randomly drawn independently from
the given allowed set \( \{ \psi_k \} \) and named, say, by its temporal position. The other party \( A \) randomly picks \( N - n \) of such states and asks \( B \) to reveal them. After verifying that they are correct, the probability that all \( n \) remaining states are at least of the form \( (A1) \) can be made arbitrarily close to 1 by proper choice of \( n, N \) as follows.

Suppose \( B \) mixes in states \( \psi' \) that allows her to cheat with probability \( P^B \leq \frac{1}{2} \geq \epsilon \) for a given \( \epsilon \). Then the cheating detection probability \( \delta = 1 - |\langle \psi' | \psi_k \rangle|^2 > 0 \) minimized over the choice of \( k \) and \( \psi' \) is a fixed number dependent only on \( \epsilon \) and the protocol, independent of \( n \) and \( N \). Suppose \( B \) mixes in \( m \) such \( \psi' \) out of the \( N \) states she sends to \( A \). We grant that \( B \)'s cheating is successful if there is just one copy of \( \psi' \) in the \( n \)-group untested by \( A \) and the measurements by him reveals no different states from \( \{ \psi_k \} \). In order that there is a non-vanishing probability found in the random \( n \)-group that \( A \) sets aside, \( m/N \) must be non-vanishing with \( m/N \to p \) in the limit \( N \to \infty \). Let \( \alpha = n/N \) so that asymptotically for large \( N, \alpha \) is the fraction of states among the \( N \) set aside. In order for \( B \) to be able to cheat, one has \( m\alpha \geq 1 \) for large \( N \) because \( m\alpha \) is the average number of \( \psi' \) in the \( n \)-group. The probability that the cheating detection fails in the \( N - n \) group is then

\[
(1 - \delta)^m(1 - \alpha) \leq (1 - \delta)^{\frac{m\alpha}{m}} \to 0, \quad (A2)
\]

which can be made arbitrarily small by having \( \alpha \) arbitrarily small that obtains with \( N \to \infty \) for fixed \( n \). This argument can be completely quantified via the hypergeometric distribution and the Chernov bound without passing to the limit \( N \to \infty \), although the limiting argument suffices for the present purpose.

In QBC4, there is no entanglement possibility for Babe, and the above analysis works with \( k = 1 \). The modification is that Adam would need Babe to send him \( \{ \mathcal{H}_{01}^B \otimes \mathcal{H}_{11}^B \} \) together with the exact \( \{ |f_{bk} \rangle \} \) for checking that the states are indeed \( |\Psi_0 \rangle |\Psi_1 \rangle \) of the form \( (1) \).

**ACKNOWLEDGMENTS**

This work was supported by the Defence Advanced Research Project Agency and The Army Research Office.