Some Subtle Issues Concerning Quantum Bit Commitment

Chi-Yee Cheung
Institute of Physics, Academia Sinica

4th Workshop on Quantum Science and Technology
Tung Hai University (Sept. 11, 2009)

Plan:

(1) Introduction

(2) No-go theorem

(3) Incompleteness

(4) Summary and Conclusion

(1) Introduction

Quantum bit commitment (QBC)
is a simple but important quantum cryptographic protocol involving two parties: Alice and Bob

They are not honest, and do not trust each other – they will do whatever it takes to gain an advantage!

The security of QBC is an important issue because QBC can be used as the building block of various other two-party quantum protocols, such as quantum coin tossing, quantum oblivious transfer, and etc.

A QBC protocol has two phases:

Commitment + Unveiling

Commitment phase:

- Alice secretly commits to a bit ***b* = 0** or **1**, which is to be revealed to Bob at a later time.
- To ensure that Alice will not change her mind before unveiling, Alice and Bob execute a series of quantum and classical exchanges such that in the end, Bob has a quantum state $\rho_B^{(b)}$ (evidence) in his hand.

Unveiling phase:

1. Alice reveals the value of ***b*** *to Bob.*
2. With some additional information from Alice, Bob uses $\rho_B^{(b)}$ to check whether Alice is honest or not.

Security Issues:

A QBC protocol is secure if it is

1. **Binding:** Alice cannot change her commitment without Bob's knowledge.
2. **Concealing:** Bob cannot find out the value of ***b*** before Alice unveils it.

Concealing condition implies:

$$\rho_B^{(0)} = \rho_B^{(1)}$$ Ideal case

$$\rho_B^{(b)} \approx \rho_B^{(1)}$$ Non-ideal case

(Asymptotically equal, $n \rightarrow \infty$)

- Unconditional Security:

  If the protocol remains secure even when A and B had capabilities limited only by the laws of nature.

  (That means its security is guaranteed by the laws of nature, and is unaffected by any possible advances in technologies.)

Example (1): (Classical QBC)

1. Alice writes ***b*** on a piece of paper and locks it in a box.
2. She gives the box (but not the key) to Bob as evidence of her commitment.

Concealing: Bob cannot read the paper

Binding: Paper is in Bob's hand

However classical BC cannot be unconditionally secure, because it's security is always dependent on some unproven assumptions (conditional security):

(1)Alice cannot steal the box when Bob is not watching
(2) Bob cannot open the lock by himself
(3) Etc….

How about QBC?

Example (2):

To commit, Alice sends Bob a sequence of qubits

$$|\mathcal{S}_n^{(b)}\rangle = |\phi_1^{(b)}\rangle|\phi_2^{(b)}\rangle ... |\phi_n^{(b)}\rangle$$

Where

$$|\phi_i^{(0)}\rangle \in \{|\uparrow\rangle, |\downarrow\rangle\}$$

$$|\phi_i^{(1)}\rangle \in \{|\rightarrow\rangle, |\leftarrow\rangle\}$$

Concealing:

$$\rho_B^{(0)} = \{|\uparrow\rangle\langle\uparrow| + |\downarrow\rangle\langle\downarrow|\}/2$$
$$\rho_B^{(1)} = \{|\rightarrow\rangle\langle\rightarrow| + |\leftarrow\rangle\langle\leftarrow|\}/2$$

Binding:

If Alice commits to ***b=0*** initially, she cannot open as ***b=1***, for if she did, her chance of success on each qubit is ½, therefore the overall chance of cheating successfully is exponentially small.

So naively, it seems that such a protocol is unconditionally secure!

But wait…

(2) No-Go Theorem

Lo and Chau, Mayers (1997)

If a protocol is concealing, it cannot be binding at the same time.

Unconditionally secure QBC is impossible as a matter of principle.

Main Idea of the Proof:

Purification – Alice leaves all undisclosed classical information undetermined at the quantum level by entangling with ancillas.

• Any action taken on a quantum system can be represented by an unitary transformation on system + ancillas

• Needs quantum computers in order to cheat.

Purification ⇒

At the end of commitment phase:

- Instead of a mixed state $\rho_B^{(b)}$ in H_B
- There exists a pure state $|\Psi_{AB}^{(b)}\rangle$ in $H_A \otimes H_B$
- H_A is used to store Alice's undisclosed info.

As long as

$$\mathrm{Tr}_A \ |\Psi_{AB}^{(b)}\rangle\langle\Psi_{AB}^{(b)}| = \rho_B^{(b)}$$

Bob cannot tell whether Alice has purified or not!

Alice has a perfect cheating strategy (EPR attack)

$$\rho_B^{(0)} = \rho_B^{(1)}$$

By a theorem of Hughston, Jozsa, and Wooters [Phys. Lett. A 183 (1993) 14.]

Schmidt decomposition:

$$|\Psi_{AB}^{(0)}\rangle = \sum_i \sqrt{\lambda^i}\, |e_A^i\rangle \otimes |\psi_B^i\rangle$$

$$|\Psi_{AB}^{(1)}\rangle = \sum_i \sqrt{\lambda^i}\, |f_A^i\rangle \otimes |\psi_B^i\rangle$$

Therefore $|\Psi_{AB}^{(1)}\rangle = U_A|\Psi_{AB}^{(0)}\rangle$

Notice: U_A acts on H_A only

Hence Alice can execute it without Bob's knowledge

That means Alice can change from

b=0 to ***b=1*** without being detected!

⇨ **Cheating!**

(Concealing protocol are not binding!)

How does it work in example (2)?

Instead of honestly producing

$$|\phi_i^{(0)}\rangle \in \{|\uparrow\rangle, |\downarrow\rangle\}$$

$$|\phi_i^{(1)}\rangle \in \{|\rightarrow\rangle, |\leftarrow\rangle\}$$

Alice generates (purification)

$$|\psi_i^{(0)}\rangle = \{|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle\}/\sqrt{2}$$

$$|\psi_i^{(1)}\rangle = \{|\uparrow\leftarrow\rangle + |\downarrow\rightarrow\rangle\}/\sqrt{2}$$

That is, instead of fixing undisclosed information at the beginning, Alice leaves it undetermined at the quantum level (delayed measurements!).

Then she can cheat perfectly:

$$|\psi_i^{(1)}\rangle = U_A|\psi_i^{(0)}\rangle$$

So according to the above arguments,
which seem quite general,
unconditionally secure QBC is impossible!

→ *ruled out as a matter of principle.*

Question: Does the “no-go theorem” cover all possible cases?

Note that QBC has a definite objective, but the corresponding ***procedure*** is not precisely defined.

*There are **infinitely** many ways to do QBC.*

So how could one be sure the no-go result is universally valid?

See, e.g., H. P. Yuen: quant-ph/0808.2040

(3) Incompleteness

(a) How about Secret Parameters?

In the impossibility proof, in order that Alice knows U_A, it is assumed that Alice knows every details of the protocol, so that no secret parameters exist.

What if Bob is allowed to generate secret parameters unknown to Alice?

The point is:

If the pure state $|\Psi^{(b)}_{AB}(\omega)\rangle$ depends on some parameter ω unknown to Alice?

Then

$$|\Psi^{(1)}_{AB}(\omega)\rangle = U_A(\omega)|\Psi^{(0)}_{AB}(\omega)\rangle$$

1. In general, $U_A(\omega)$ depends ω
2. But ω is not known to Alice, therefore she cannot calculate $U_A(\omega)$
3. If so, then unconditionally secure QBC might be possible (?)

The point is, the no-go theorem only proves the existence of $U_A(\omega)$, but there is no guarantee that it is known to Alice!

However, we find that for a **concealing** QBC protocol, the cheating unitary transformation U_A is independent of any secret parameter (probability distribution), ω, chosen by Bob.

(Purification: From a purified point of view, probability distributions are the only possible unknowns left.)

Proof:

If Bob is allowed to choose ω from $\{\omega_i\}$ in secret, then we must in general assume that he purifies his choices with a certain probability distribution

$$\pi = \{p_i\}$$

That is, instead of picking a particular ω_i , and producing

$$|\Psi_{AB}^{(b)}(\omega_i)\rangle$$

Bob entangles all his possible choices

$$|\Psi'^{(b)}_{AB}(\pi)\rangle = \sum_i \sqrt{p_i}\,|\Psi^{(b)}_{AB}(\omega_i)\rangle\ |\chi_i\rangle$$

Where $\{\chi_i\}$ are orthonormal ancilla states.

Now the protocol is concealing. Therefore no matter what $\{p_i\}$ Bob uses, the resulting reduced density matrix must be independent of ***b***

$$\rho'^{(0)}_B = \rho'^{(1)}_B$$

Then there exists an U'_A such that

$$|\Psi'^{(1)}_{AB}(\pi)\rangle = U'_A \ |\Psi'^{(0)}_{AB}(\pi)\rangle$$

Since $|\chi_i\rangle$ are orthogonal states in H_B

Whereas U'_A acts on H_A only.

Then it is easy to show that

$$|\Psi^{(1)}_{AB}(\omega_i)\rangle = U'_A \ |\Psi^{(0)}_{AB}(\omega_i)\rangle, \quad \forall \omega_i$$

Hence

$$U_A(\omega) = U'_A$$

Is independent of ω !

That means Alice can cheat perfectly whether Bob uses secret parameters or not.

The up shot is, for a concealing QBC protocol, i.e.,

$$\rho_B^{(0)} = \rho_B^{(1)}$$

U_A is independent of any of Bob's secret probabilities, and Alice can calculate it without knowing what Bob actually uses.

→ *However, this result is not included in the original no-go theorem.*

(B) Is the cheating strategy proved in no-go theorem universal?

Let us look at the following simple protocol:

Commitment:

(1) Bob generates ***n*** singlet Bell states, and send half of each Bell state to Bob.

(2) To commit to ***b=1***, Alice measures one of the qubits in her hand and announce the outcome.

(3) To commit to ***b=0***, she does nothing, and announce randomly a fake outcome.

Unveiling:

(1) Alice reveals ***b=0*** or ***b=1***

(2) She then returns all the qubits to Bob,
and if ***b=1***, identifies the measured qubit.

(3) If ***b=0***, Bob checks that all the Bell states are intact. If ***b=1***, he checks that Alice had indeed measured the qubit she identified, and the rest Bell states are intact.

This QBC protocol is concealing, because it can be proven that measuring one out of ***n*** qubits will not produce detectable effect on Bob's side (if ***n*** is large enough).

This protocol is not binding, but the cheating strategy is not necessarily via a unitary operation in Alice's Hilbert space as claimed.
→ If Alice initially commits to ***b=0***, she has actually not made any measurement. Therefore, if she now wants to switch to ***b=1,***

before unveiling, she must measure one of her qubits, until the outcome is the same as the fake one she had made up during the commitment phase.

(The detail is more complicated, but this is in principle what she has to do.)

So you see, although Alice can still cheat, the cheating strategy is **not** an unitary transformation as claimed by the no-go theorem. It is instead a series of measurements.

(c) QBC using unstable particles

For example, Bob generates a Bell state

$$|\varphi\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle|\mathbf{1}\rangle - |1\rangle|\mathbf{0}\rangle\Big)$$

(where one of the particle is unstable, say, neutron), and sends the unstable particle to Alice, which she uses to commit.
I think this approach has good potential, I have not worked out all the details. If it really works out, I will report to you next time.

Summary:

We have shown that the no-go theorem actually does not cover all cases.

(1) First of all, it did not consider the possibility of Bob using secret probability distributions.

(2) Secondly, the cheating strategy is not necessarily a unitary operation executed by Alice.

Conclusion:

We have not been able to show unconditionally secure QBC is possible, however it is clear that the no-go theorem does not cover all possible situations. *Hence the case is far from settled!*

I hope next time, I will be able to come up with a concrete QBC protocol, and show that unconditionally secure QBC is indeed possible!

Thank you for your attention!

- Lo and Chau: “In order that Alice and Bob can follow the procedures, they must know the exact forms of all unitary transformations involved“
- Mayers: “It is a principle that we must assume that every participant knows every detail of the protocol, including the distribution of probability of a random variable generated by another participant"