IASSNS-HEP-96-21; quant-ph/9603004

Is Quantum Bit Commitment Really Possible?

Hoi-Kwong Lo* and H. F. Chau†

School of Natural Sciences, Institute for Advanced Study, Olden Lane, Princeton, NJ 08540

(March 4, 1996)

Abstract

We show that all proposed quantum bit commitment schemes are insecure because the sender can always cheat successfully by using an EPR-type of attack and delaying her measurement until she opens her commitment.

PACS Numbers: 03.65.Bz, 89.70.+c, 89.80.+h

*e-mail: hkl@sns.ias.edu

†e-mail: chau@sns.ias.edu

A bit commitment scheme generally involves two parties, a sender, Alice and a receiver, Bob. Suppose that Alice has a bit ($b = 0$ or 1) in mind, to which she would like to be committed towards Bob. That is to say, she wishes to provide Bob with a piece of evidence that she has a bit in mind and that she cannot change it. Meanwhile, Bob should not be able to tell from that evidence what b is. At a later time, however, it must be possible for Alice to *open* the commitment. In other words, Alice must be able to show Bob which bit she has committed to and convinced him that this is indeed the genuine bit that she had in mind when she committed.

Various quantum bit commitment schemes[1, 2, 3, 4] have been proposed in the literature and at least one of them[3] is even claimed to be provably unbreakable. However, here we demonstrate explicitly that so far all proposed quantum bit commitment schemes are inherently insecure due to an EPR-type of attack by Alice. More precisely, a dishonest Alice proceeds as follows: She prepares an entangled state of two systems and sends one of them to Bob, keeping the other herself. To open the fake commitment, she decides on the value of the bit b now and measures her system along an appropriate basis for that particular value of b.

All the proposed quantum bit commitment schemes that we are aware of share the same general procedure which can be rephrased in the language of quantum mechanics in the following manner:

(1) Alice chooses the value of a bit b to which she would like to be committed towards Bob. If $b = 0$, she prepares a state

$$|0\rangle = \sum_i \alpha_i |e_i\rangle_A \otimes |\phi_i\rangle_B, \tag{1}$$

where $\langle e_i|e_j\rangle_A = \delta_{ij}$ but the normalized states $|\phi_i\rangle_B$'s are not necessarily orthogonal to each other. Similarly, if $b = 1$, she prepares a state

$$|1\rangle = \sum_j \beta_j |e'_j\rangle_A \otimes |\phi'_j\rangle_B, \tag{2}$$

where $\langle e'_i|e'_j\rangle_A = \delta_{ij}$ but $|\phi'_j\rangle_B$'s are not necessarily orthogonal to each other.

Note that for an honest Alice, the two choices (0 or 1) for the committed bit b are supposed to be mutually exclusive and consequently $\langle e_i|e'_j\rangle_A = 0$ for all i, j. However, since the system A is in Alice's hands, a dishonest Alice has the freedom to cheat by violating this constraint.

(2) An *honest* Alice is now supposed to make a measurement on the first register and determine the value of i if $b = 0$ (j if $b = 1$).

(3) Alice sends the second register to Bob as a piece of evidence for her commitment.

(4) At a later time, Alice opens the commitment by declaring the value of b and the corresponding value of i or j.

(5) Bob may perform any measurement as he wishes on the second register to convince himself that Alice has indeed committed to the genuine bit.

We show that the above general scheme necessarily fails because Alice can always cheat successfully by delaying her choice of b until step 4. More precisely, she can prepare the same state $|0\rangle = |1\rangle$ in the first step, skip the second step altogether and finally decide on the value of b in step 4 and determine the value of i or j by performing an appropriate measurement according to her chosen value of b. Notice that the possibility of a dishonest Alice skipping the second step was not considered in Ref. [3]. This was the reason why the authors reached the erroneous conclusion that their scheme is provably unbreakable.

Let us justify our claim. First of all, in order that Bob cannot tell what b is, the second register must contain no information about which bit Alice has committed to. Therefore, it is necessary that the density matrices that describe the second register associated with the bits 0 and 1 are the same. i.e.,

$$\mathrm{Tr}_A|0\rangle\langle 0| \equiv \rho_0^B = \rho_1^B \equiv \mathrm{Tr}_A|1\rangle\langle 1|. \tag{3}$$

Thus, $|0\rangle = |1\rangle$ is at least a consistent choice in step one. Let us rewrite the state that Alice prepares in step one in the Schmidt Polar form[5]:

$$|0\rangle = |1\rangle = \sum_k \sqrt{\lambda}_k |\hat{e}_k\rangle_A \otimes |\hat{\phi}_k\rangle_B, \tag{4}$$

where $|\hat{e}_k\rangle_A$ and $|\hat{\phi}_k\rangle_B$ are orthonormal vectors for the two registers respectively and all $\sqrt{\lambda_k}$ are positive. Of course, Alice can skip step 2 without being detected by Bob. So, the only question is whether she can successfully determine the value of i or j.

To prove that this can indeed be done, let us re-express $|0\rangle$ in the Schmidt polar form by inserting the identity operator $\sum_k |\hat{\phi}_k\rangle_B\langle\hat{\phi}_k|_B$ in Eq. (1):

$$\begin{aligned} |0\rangle &= \sum_i \alpha_i |e_i\rangle_A \otimes |\phi_i\rangle_B \\ &= \sum_k \sum_i \alpha_i |e_i\rangle_A \otimes |\hat{\phi}_k\rangle_B \langle\hat{\phi}_k|\phi_i\rangle_B \\ &= \sum_k \left(\sum_i \alpha_i \langle\hat{\phi}_k|\phi_i\rangle_B |e_i\rangle_A \right) \otimes |\hat{\phi}_k\rangle_B . \end{aligned} \tag{5}$$

A comparison with Eq. (4) implies that

$$\sqrt{\lambda_k}|\hat{e}_k\rangle_A = \sum_i \alpha_i \langle\hat{\phi}_k|\phi_i\rangle_B |e_i\rangle_A \tag{6}$$

where no summation in k is implied. By a similar argument, we obtain

$$\sqrt{\lambda_k}|\hat{e}_k\rangle_A = \sum_j \beta_j \langle\hat{\phi}_k|\phi'_j\rangle_B |e'_j\rangle_A \tag{7}$$

where no summation in k is implied. Notice that Eqs. (6) and (7) are merely telling us how the vectors $|\hat{e}_k\rangle_A$'s are mapped into the Hilbert spaces spanned by $\{|e_i\rangle_A\}$ and $\{|e'_j\rangle_A\}$ respectively.

The case when the three Hilbert spaces have the same dimension is particularly easy to understand. In this case, Eqs. (6) and (7) specify the unitary transformation between the three Hilbert space. For a cheating Alice, step four becomes

(4') A *dishonest* Alice decides on the value of the bit b now. If she chooses b to be zero, she measures her first register along the basis $\{|e_i\rangle_A\}$ and tells Bob the value of i obtained in her measurement. Similarly, if she chooses b to be one, she measures her first register along the basis $\{|e'_j\rangle_A\}$ and tells Bob the value of j.

Therefore, she can always cheat successfully. Notice that she is able to cheat primarily because she can *delay* her measurement until step four.

The case when the three Hilbert spaces have different dimensions is similar. One just extends the dimensions of the two smaller Hilbert spaces if necessary and the problem immediately reduces to one with equal dimensions. [In that case, Eqs. (6) and (7) specify how the Hilbert space spanned by $\{|\hat{e}_k\rangle_A\}$ should be *embedded* into two larger Hilbert spaces spanned by vectors $\{|e_i\rangle_A\}$ and $\{|e'_j\rangle_A\}$ respectively.]

In summary, we have shown that a general class of quantum bit commitment schemes is insecure because Alice can always cheat by an EPR-type of attack. More precisely, Alice cheats by entangling the state of the system that Bob receives with another system in her hands and performing a delayed measurement on her own system when she is required to open the commitment. Moreover, her measurement basis will depend on the value of the bit she chooses. Since all the proposed quantum bit commitment schemes belong to the class that we have just analyzed, our results automatically imply that they are all insecure. If any secure quantum bit commitment scheme exists at all, it must therefore follow a different procedure than the one laid down in the beginning of this paper. The construction of truly secure quantum bit commitment protocols will be an important subject in future investigations. Moreover, the security of other quantum cryptographic protocols say for oblivious transfer[6, 7, 8] and coin tossing remains to be examined. One might wonder if all of quantum cryptography may stumble under closer scrutinies. Fortunately, the security of quantum key distribution has recently been established[9] and quantum cryptography should be useful for at least this purpose.

This work is supported by DOE grant DE-FG02-90ER40542.

REFERENCES

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, p. 175-179. IEEE, 1984.

[2] G. Brassard and C. Crépeau. Quantum bit commitment and coin tossing protocols. In *Advances in Cryptology: Proceedings of Crypto '90*, Lecture Notes in Computer Science, Vol. 537, p. 49-61. Springer-Verlag, 1991.

[3] G. Brassard, C. Crépeau, R. Jozsa and D. Langlois, A quantum bit commitment scheme provably unbreakable by both parties, in *Proceedings of the 34th annual IEEE Symposium on the Foundation of Computer Science*, Nov. 1993, p.362-371.

[4] M. Ardehali, A perfectly secure quantum bit commitment protocol, Los Alamos preprint archive quant-ph/9505019.

[5] See, for example, the Appendix of L. P. Hughston, R. Jozsa and W. K. Wootters, A complete classification of quantum ensembles having a given density matrix, Phys. Lett. **A183**, p. 14-18, (1993).

[6] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, Practical quantum oblivious transfer, in *Advances in Cryptology: Proceedings of Crypto '91*, Lecture Notes in Computer Science, Vol. 576, p. 351-366. Springer-Verlag, 1992.

[7] D. Mayers, On the security of quantum oblivious transfer and key distribution protocols, in *Advances in Cryptology: Proceedings of Crypto '95*, Lecture Notes in Computer Sciences, Vol. 963, p. 124-135. Springer-Verlag, 1995.

[8] M. Ardehali, A simple quantum oblivious transfer protocols, Los Alamos preprint archive quant-ph/9512026.

[9] H.-K. Lo and H. F. Chau, Quantum cryptography in noisy channels, Los Alamos preprint archive quant-ph/9511025.