PhysComp96
Extended abstract
Draft, 10 May 1996
IASSNS-HEP-96/50

Why quantum bit commitment and quantum coin tossing are impossible?*

Hoi-Kwong Lo† and H. F. Chau‡
School of Natural Sciences, Institute for Advanced Study, Princeton, NJ 08540

There had been well known claims of "provably unbreakable" quantum protocols for bit commitment and coin tossing. However, we, and independently Mayers, showed that all proposed quantum bit commitment (and coin tossing) schemes are, in principle, insecure because the sender, Alice, can always cheat successfully by using an EPR-type of attack and delaying her measurements. One might wonder if secure quantum bit commitment and coin tossing protocols exist at all. Here we prove that an EPR-type of attack by Alice will, in principle, break *any* realistic quantum bit commitment and *ideal* coin tossing scheme. Therefore, provided that Alice has a quantum computer and is capable of storing quantum signals for an arbitrary length of time, all those schemes are insecure. Since bit commitment and coin tossing are useful primitives for building up more sophisticated protocols such as zero-knowledge proofs, our results cast very serious doubt on the security of quantum cryptography in the so-called "post-cold-war" applications.

1 Introduction

Quantum cryptography was first proposed by Wiesner [20] more than two decades ago. The most well-known application of quantum cryptography is key distribution [4, 6, 10], whose security has been a subject of much recent interest [3, 9, 16, 18]. In addition to key distribution, the so-called "post-cold-war" applications of quantum cryptography have also been proposed [1, 2, 4, 5, 7, 8]. A typical problem in "post-cold-war" quantum cryptography is the two-party secure computation, in which both parties would like to know the result of a computation but neither side wishes to reveal its own data. For example, two firms will embark on a joint venture if and only if their combined capital available for the project is larger than one million dollars. They would like to know if this condition is fulfilled but neither wishes to reveal the exact amount of capital it commits to the project. In classical cryptography, this can be done either through trusted intermediaries or by invoking some unproven cryptographic assumptions such as the hardness of factoring. The big question is whether quantum cryptography can get rid of those requirements and achieve the same goal using the laws of physics alone.

Until recently, there had been much optimism in the subject. Various protocols for say bit commitment, coin tossing and oblivious transfer of quantum cryptography had been proposed [1, 2, 4, 5, 7, 8]. In particular, the BCJL [8] bit commitment scheme had been claimed to be provably unbreakable. However, in our recent paper [17], we showed that all proposed quantum bit commitment schemes are insecure because the sender, Alice, can always cheat successfully by using an EPR-type of attack and delaying her measurement until she opens her commitment. (The insecurity of the BCJL scheme was also investigated by Mayers [19] from an information-theoretic point of view.) Our result put the security of post-cold-war quantum cryptographic systems in serious doubt because bit commitment, coin tossing and oblivious transfer are crucial primitives [15] in building up more sophisticated protocols.

An important fundamental question that we left unanswered in our previous investigation was whether *any* secure quantum bit commitment scheme exists at all. Here we show that, provided that the users have the capability of storing quantum signals for an arbitrary length of time, quantum bit commitment and *ideal* quantum coin tossing are impossible: All such protocols are necessarily insecure against an EPR-type of attack by at least one of the users. Our highly disruptive results can be taken as a strong indication that, despite widespread early optimism, realistic post-cold-war applications of quantum cryptography simply do not exist. Incidentally, we have learnt that Mayers is also currently investigating the security of a general quantum bit commitment scheme.

2 Quantum bit commitment

A general bit commitment scheme 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,

*Supported by DOE grant DE-FG02-90ER40542
†Address after 1 Oct., 96: BRIMS, Hewlett-Packard Labs, Filton Road, Stoke Gifford, Bristol BS12 6QZ, UK
‡Address after 1 July, 96: Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong

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. That is, 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.

What constitutes to a cheating by Alice? If Alice commits to a particular value of b (e.g., $b = 0$) during the commitment phase and attempts to change it to another value (e.g., $b = 1$) during the opening phase, Alice is cheating. A bit commitment scheme is secure against Alice only if such a fake commitment will be discovered by Bob. In this section, we show that, contrary to popular belief, all quantum bit commitment schemes are, in principle, insecure against a cheating Alice.

2.1 Model of two-party quantum protocols

Quantum bit commitment and coin tossing are examples of two-party quantum protocols. A two-party quantum protocol involves a pair of quantum machines in the hands of two users, A (Alice) and B (Bob) respectively, which interact with each other through a quantum channel, C. More formally, we consider the direct product H of the three Hilbert spaces H_A, H_B and H_C where H_A (H_B) is the Hilbert space of Alice's (Bob's) machine and H_C is the Hilbert space of the channel. We assume that initially each machine is in some specified pure quantum state. A and B then engage in a number of rounds of quantum communication with each other through the channel C. More concretely, A and B alternately performs a unitary transformation on $H_D \otimes H_C$ where $D \in \{A, B\}$.

The above model is a simplification of a model proposed by Yao [21]. Although Yao apparently did not emphasize the generality of his model, it appears to us that any realistic two-party computation can be described by Yao's model. For instance, since Alice and Bob are separated by a long distance, it is impractical to demand simultaneous two-way communications between them. The idea of alternate rounds of one-way communications in Yao's model is, therefore, reasonable. However, there are two significant distinctions between Yao's model and ours. First, Yao's model deals with mixed initial states whereas we assume that the initial state of each machine is pure. Second, in Yao's model, the user D does two things in each round of the communication: D carries out a measurement on the current mixed state of the portion of the space, $H_D \otimes H_C$, in his/her control and then performs a unitary transformation on $H_D \otimes H_C$. In our model, the measurement step has been eliminated.

Nevertheless, we would like to argue that there is no loss in generality and that our model still gives the most general procedure of a two-party quantum protocol. Let us consider the first distinction. In assuming that the initial state of each machine is pure, we are just giving the users complete control over the initial states of the machines. Any situation with mixed initial state can be included in our consideration simply by attaching a quantum dice to a machine and considering the pure state as describing the combined state of the two.

What about the second distinction? We make the simple but crucial observation that one can avoid dealing with the collapse of a wavefunction associated with a measurement altogether. The point is, that, in principle, D has the option of adding an ancilla to his/her quantum machine and using a *reversible* unitary operation to replace a measurement. D can then read off the state of his/her ancilla only at the *very end* of the protocol. Put it another way: Alice and Bob are assumed to be in possession of quantum computers and quantum storage devices. Note that our model is general enough to incorporate any classical computation and communications. It cannot be overemphasized that this unitary description leads to no loss in generality and indeed *any* two-party quantum protocol can be described by our model. (See [12] and, in particular, the Appendix B of the revised version of [16] for related discussions.) Such a unitary description will greatly simplify our discussion.

2.2 Procedure of quantum bit commitment

Granting the possession of quantum computers and quantum storage devices by Alice, the most general procedure for an ideal quantum bit commitment scheme can be rephrased in the following manner.

(a) Preparation of states: Alice chooses the value of a bit b to which she would like to be committed towards Bob. If $b = 0$ (respectively $b = 1$), she prepares a state $|0\rangle$ (respectively $|1\rangle$) for H_A. The two states $|0\rangle$ and $|1\rangle$ are orthogonal to each other. Bob prepares a state $|B_0\rangle \otimes |C_0\rangle$ for the product Hilbert space $H_B \otimes H_C$.

(b) The actual commitment: Step (b) involves a specified number of rounds of quantum communication alternately between Alice and Bob. As noted above, each round of quantum communication can be modeled as a unitary transformation on $H_D \otimes H_C$ ($D \in \{A, B\}$), which in turn induces a unitary transformation on the space $H = H_A \otimes H_B \otimes H_C$.

Notice that for an *ideal* bit commitment, it must be the case that, at the end of step (b), Bob still has absolutely no information about the value of the committed bit b. (We will relax this assumption when we come to the non-ideal case in the next subsection.) Now that the com-

mitment has been made, both sides may wait an arbitrary length of time until the last step:

(c) Opening of the commitment: A specified number of rounds of quantum communication alternately between Alice and Bob are again involved. As in step (b), we model each round of quantum communication as a unitary transformation on $H_D \otimes H_C$ ($D \in \{A, B\}$), which in turn induces a unitary transformation on the space $H = H_A \otimes H_B \otimes H_C$.

In a secure bit commitment scheme, Bob will learn the value of b and be convinced that Alice has already committed to that value of b at the end of step (b) and cannot change it anymore in step (c).

However, we show that the above general scheme necessarily fails because Alice can always cheat successfully by using *reversible* unitary operations in step (b) and subsequently rotating a state that corresponds to $b = 0$ to one that corresponds to $b = 1$ and vice versa in the beginning of step (c). Note that Alice's ability of cheating lies on her capability of storing coherent quantum signals for a long period of time (until the beginning of step (c)).

Let us justify our claim. Consider more closely the situation at the end of step (b). Let $|0\rangle_{\rm com}$ and $|1\rangle_{\rm com}$ denote the state of $H = H_A \otimes H_B \otimes H_C$ at that time corresponding to the two possible values of b respectively. In order that Alice and Bob can follow the procedures, they must know the exact forms of all the unitary transformations involved.[1] Therefore, Alice must be capable of computing the two states $|0\rangle_{\rm com}$ and $|1\rangle_{\rm com}$. Since the channel will sit idle for a long while, its state has to be trivial. We may, therefore, assume that the channel C is in a prescribed pure state $|u\rangle_C$ at the end of step (b). Moreover, the fact that Bob has absolutely no information about the value of b implies that the density matrix in his hand is independent of the value of b. That is to say that ${\rm Tr}_A\left(|0\rangle_{\rm com}\langle 0|_{\rm com}\right) = {\rm Tr}_A\left(|1\rangle_{\rm com}\langle 1|_{\rm com}\right)$. But then $|0\rangle_{\rm com}$ and $|1\rangle_{\rm com}$ of H must have the same Schmidt polar form (See for example, the Appendix of [13].):

$$|0\rangle_{\rm com} = \left(\sum_k \sqrt{\lambda_k}|\hat{e}_k\rangle_A \otimes |\hat{\phi}_k\rangle_B\right) \otimes |u\rangle_C, \qquad (1)$$

and

$$|1\rangle_{\rm com} = \left(\sum_k \sqrt{\lambda_k}|\hat{e}_k\rangle'_A \otimes |\hat{\phi}_k\rangle_B\right) \otimes |u\rangle_C, \qquad (2)$$

where $|\hat{e}_k\rangle_A$ and $|\hat{e}_k\rangle'_A$ are two orthonormal bases of H_A and $|\hat{\phi}_k\rangle_B$ is an orthonormal basis of H_B.

[1] As stated earlier, any probabilistic scheme can be rephrased as a deterministic one by considering the state of the combined system of the quantum dice and the original system.

The key observation is that these two states are related by a unitary transformation acting on H_A alone! Consequently, Alice can make a fake commitment and change the value of b in the beginning of step (c). For example, she may proceed as follows: First, Alice always takes $b = 0$ in step (a) and goes through step (b). It is only in the beginning of step (c) that Alice decides on the actual value of b that she wishes to open. If she decides $b = 0$ now, she can go through step (c) honestly. If she wishes to change the value of b from 0 to 1, she simply applies a unitary transformation to rotate her state from $|0\rangle_{\rm com}$ to $|1\rangle_{\rm com}$ before going through step (c). Since the unitary transformation acts on H_A alone, Bob clearly has no way of knowing Alice's dishonesty.[2] In conclusion, provided that Alice possesses quantum computers and quantum storage devices, our results show that all quantum bit commitment schemes are insecure because Alice can cheat successfully by using an EPR-type of attack.

2.3 Non-ideal bit commitment

In our above discussion, we have assumed that the bit commitment scheme is ideal in the sense that Bob has absolutely no information about the value of b at the end of step (b). This is the physical reason behind the mathematical statement that $\rho_0^{\rm com} = {\rm Tr}_A\left(|0\rangle_{\rm com}\langle 0|_{\rm com}\right) = {\rm Tr}_A\left(|1\rangle_{\rm com}\langle 1|_{\rm com}\right) = \rho_1^{\rm com}$. (i.e., the two density matrices corresponding to the two cases $b = 0$ and $b = 1$ are identical.) However, in realistic applications, one might allow Bob to have a very tiny amount of information about b at that time. It is intuitively obvious that this is not going to change our conclusion. On the one hand, if Bob has a large probability of distinguishing between the two states corresponding to $b = 0$ and $b = 1$ at the end of step (b), the scheme is inherently unsafe against Bob. On the other hand, if Bob has a small probability of distinguishing between the two states, then clearly, the density matrices $\rho_0^{\rm com} = {\rm Tr}_A\left(|0\rangle_{\rm com}\langle 0|_{\rm com}\right)$ and $\rho_1^{\rm com} = {\rm Tr}_A\left(|1\rangle_{\rm com}\langle 1|_{\rm com}\right)$ must be close to each other in some sense. We have seen in the last subsection that when the two density matrices are identical, Alice can always cheat successfully. It is, therefore, at least highly suggestive that, when the two density matrices are only slightly different, Alice will have a probability close to 1 of cheating successfully. A detailed calculation, which will be sketched briefly in the next subsection, shows that this is indeed the case. Therefore, even

[2] What is the problem with quantum bit commitment? Here is an analogy. Suppose that there are two novels whose first halves are the same, but the second halves are different. I give you only the first half of one of the two novels and I tell you that I have committed to a particular novel and that I cannot change it anymore. Will you trust me? Of course not. Since the first halves of the two novels are the same, no real commitment has been made. I am free to give you the second half of either novel and claim that I have committed to either one all along. There is no way for you to tell whether I am lying.

non-ideal bit commitment schemes are necessarily highly insecure.

2.4 Fidelity

In this subsection, we sketch the mathematical proof of the insecurity of non-ideal quantum bit commitment scheme. (See also Mayers [19].) Readers who are uninterested in mathematical details may skip this subsection on first reading. The price that they have to pay is to take Eqs. (6) and (8) for granted.

First of all, the *fidelity* [11, 14] between two density matrices ρ_0 and ρ_1 of a system B is defined as

$$F(\rho_0, \rho_1) = \mathrm{Tr}\sqrt{\rho_1^{1/2}\rho_0\rho_1^{1/2}}. \tag{3}$$

$0 \leq F \leq 1$. $F = 1$ if and only if $\rho_0 = \rho_1$. Returning to the case of non-ideal bit commitment that we have been considering, the fact that Bob has a small probability for distinguishing between two states ρ_0^{com} and ρ_1^{com} implies that the fidelity $F(\rho_0^{\mathrm{com}}, \rho_1^{\mathrm{com}})$ is very close to 1. i.e.,

$$F(\rho_0^{\mathrm{com}}, \rho_1^{\mathrm{com}}) = 1 - \delta, \tag{4}$$

where δ is small.

An alternative and equivalent definition of fidelity involves the concept of *purification*. Imagine another system E attached to our given system B. There are many pure states $|\psi_0\rangle$ and $|\psi_1\rangle$ on the composite system such that

$$\mathrm{Tr}_E\left(|\psi_0\rangle\langle\psi_0|\right) = \rho_0 \qquad \text{and} \qquad \mathrm{Tr}_E\left(|\psi_1\rangle\langle\psi_1|\right) = \rho_1. \tag{5}$$

The pure states $|\psi_0\rangle$ and $|\psi_1\rangle$ are called the purifications of the density matrices ρ_0 and ρ_1. The fidelity can be defined as

$$F(\rho_0, \rho_1) = \max|\langle\psi_0|\psi_1\rangle| \tag{6}$$

where the maximization is over all possible purifications. Let us go back to a non-ideal quantum bit commitment scheme. We take E to be the combined system of Alice's machine A and the channel C. It follows from Eqs. (4) and (6) that there exist purifications $|\psi_0\rangle_{ABC}$ and $|\psi_1\rangle_{ABC}$ of ρ_0^{com} and ρ_1^{com} respectively such that

$$|\langle\psi_0|\psi_1\rangle_{ABC}| = F(\rho_0^{\mathrm{com}}, \rho_1^{\mathrm{com}}) = 1 - \delta. \tag{7}$$

The strategy of a cheating Alice is the same as in the ideal case. She always prepares the state $|0\rangle$ corresponding to $b = 0$ in step (a) and goes through step (b). She decides on the value of b she likes only in the beginning of the step (c). If she chooses $b = 0$, of course, she can just follow the rule. If she chooses $b = 1$, she applies a unitary transformation to obtain the state $|\psi_0\rangle_{ABC}$ in $H = H_A \otimes H_B \otimes H_C$. Notice that if she were honest, the state would be $|\psi_1\rangle_{ABC}$ instead. Since $|\psi_0\rangle_{ABC}$ and $|\psi_1\rangle_{ABC}$ are so similar to each other (See Eq. (7).), Bob clearly has a hard time in detecting the dishonesty of Alice. Therefore, Alice can cheat successfully with a very large probability.

Yet another equivalent definition of the fidelity, which will be useful in the next section, can be given in terms of positive-operator-valued-measures (POVMs). A POVM is a set $\{\hat{E}_b\}$ of positive operators (i.e., Hermitian operators with non-negative eigenvalues) that satisfy a sort of completeness relation (i.e., $\sum_b \hat{E}_b$ equals the identity operator). A POVM simply represents the most general measurement that can be performed on a system. More concretely, it is implemented by a) placing the system in contact with an auxiliary system or ancilla prepared in a standard state, b) evolving the two by a unitary operator, and c) performing an ordinary von Neumann measurement on the ancilla. In terms of POVMs, the fidelity is defined as

$$F(\rho_0, \rho_1) = \min \sum_b \sqrt{\mathrm{Tr}\rho_0\hat{E}_b}\sqrt{\mathrm{Tr}\rho_1\hat{E}_b}, \tag{8}$$

where the minimization is over all POVMs, $\{\hat{E}_b\}$. Eq. (8) will be useful in the next section.

3 Quantum coin tossing

Suppose that Alice and Bob are having a divorce and that they are living far away from each other. They would like to decide by a coin flip over the telephone who is going to keep the house. Of course, if one of them is tossing a real coin, there is no way for the other to tell if he/she is cheating. Therefore, there must be something else that is simulating the coin flip. Just like bit commitment, coin tossing can be done in classical cryptography either through trusted intermediaries or by accepting some unproven cryptographic assumptions. The question is: Can quantum mechanics help to remove those requirements? In other words, do coin tossing schemes whose security is based solely on the law of quantum physics exist?

Notice that a secure bit commitment protocol can be used trivially to implement a secure coin tossing protocol[3] but the converse is not true. Coin tossing is a weaker protocol for which we have a weaker result—*ideal* quantum coin tossing schemes do not exist. The idea of our proof is simple. We use backward induction. Let us assume that an ideal quantum coin tossing can be done with a fixed and finite number, N, rounds of communication between Alice and Bob. We will prove that it can be done in $N - 1$ rounds. By repeated induction, it can be done

[3] Alice chooses a bit and commits it to Bob. Bob simply tells Alice his guess for her bit. Alice then opens her commitment to see if Bob has guessed correctly.

without any communication between Alice and Bob at all. This clearly leads to a contradiction. The crucial step is the backward induction from N rounds to $N-1$ rounds, which we will discuss below.

Suppose that there exists an ideal quantum coin tossing protocol which involves N alternate rounds of communication between Alice and Bob. Let us concentrate on the N-th round of the communication. Without much loss of generality, let us assume that it is Alice's turn to send quantum signals through the channel C in the N-th round. Since this is the last round, Alice must know the outcome of the coin tossing even before her signals are sent. On the other hand, Bob is supposed to learn the outcome of the coin tossing through the combined state in $H_B \otimes H_C$. However, Alice may attempt to alter Bob's outcome by changing the mixed state in H_C that she is sending through the channel. Alice's ability to cheat successfully depends on the value of the fidelity $F(\rho_0^B, \rho_1^B)$ between the two density matrices corresponding to $b = 0$ and 1 respectively. For *ideal* quantum coin tossing, we demand the probability of Alice cheating successfully should be exactly zero. This implies, with the definition of fidelity in Eq. (6), that $F(\rho_0^B, \rho_1^B) = 0$. It then follows from Eq. (8) that ρ_0^B and ρ_1^B have orthogonal supports and can be completely distinguished from each other even without the last round of transmission from Alice. Therefore, we have reduced an N-round ideal coin tossing scheme to an $N-1$-round one. This completes our inductive proof. We conclude that ideal quantum coin tossing is impossible.

It is intuitively very plausible that non-ideal quantum coin tossing do not exist neither. However, we have so far been unable to write down a rigorous proof. This should be an important subject for future investigations.

4 A constraint on two-party secure computation

Let us consider the issue of two-party secure computation in a more general setting. The idea of two-party secure computation is the following: Alice has a secret x and Bob has another secret y. Both would like to know the result $f(x, y)$ at the end of a computation and be sure that the result is correct. However, neither side wishes the other side to learn more about its own secret than what can be deduced from the output $f(x, y)$. As mentioned earlier, classical cryptographic schemes can implement two-party secure computation at the cost of introducing trusted intermediaries or accepting unproven cryptographic assumptions. Our results in the last two sections strongly suggest that, in principle at least, quantum cryptography would not be useful for getting rid of those requirements in two-party secure computation. Even if quantum mechanics does not help, one may ask if there is *any* way of implementing a two-party computation that is secure from an information-theoretic point of view? In particular, if quantum mechanics turned out to be wrong and were replaced by a new physical theory, would it be conceivable that two-party secure computation can be done in this new theory? Here we argue that if Alice and Bob are shameless enough to declare their dishonesty and stop the computation whenever one of them has a slightest advantage over the other in the amount of mutual information he/she has on the function $f(x, y)$, a two-party secure computation can never be implemented.

For simplicity, let us normalize everything and assume that initially both Alice and Bob have no information about $f(x, y)$ and at the end of the computation, both have 1 bit of information about $f(x, y)$. Let us suppose further than Alice and Bob are unkind enough to stop the computation whenever one of them has an ϵ bit of information more than the other. Any realistic scheme must involve a finite number say N alternate rounds of communication between Alice and Bob. An analogy is that two persons, Alice and Bob, are walking in discrete alternate steps from the starting point 0 to the finishing line set at 1. Altogether N steps are made and it is demanded that Alice and Bob will never be separated from each other for more than a distance ϵ.[4] Clearly, this implies $N\epsilon \geq 1$ or $N \geq 1/\epsilon$. Therefore, the smaller the tolerable relative informational advantage ϵ is, the larger the number of rounds of communication N is needed. Notice that the constraint $N\epsilon \geq 1$ applies to *any* two-party secure computation scheme. In particular, it remains valid even if quantum mechanics is wrong.

5 Summary

We have shown that all realistic quantum bit commitment and ideal quantum coin tossing protocols are, *in principle*, insecure. The basic problem is that the users can cheat using an EPR-type of attack. Our results totally contradict well-known claims of "provably unbreakable" schemes in the literature, whose analyses on EPR attack were flawed, and provide strong evidence against the security of quantum cryptography in "post-cold-war" applications, at least *in principle*. The early optimism in the subject is, therefore, misplaced. Nevertheless, quantum bit commitment schemes that are secure *in practice* do exist[5] because it is notoriously difficult for cheaters with current technology to store quantum signals for an

[4] Actually, there is a minor subtlety in quantum cryptography. Each time when one user, say Alice, advances, the other user, say Bob, may slip backwards. The point is: the quantum "no-cloning theorem" states that quantum signals cannot be copied. When Bob sends signals to Alice, he loses control over the signals that he sends. In other words, Bob's available information tends to decrease whenever he sends signals to Alice.

[5] We thank C. H. Bennett for a discussion about this point.

arbitrary length of time. Therefore, we can trade the traditional complexity assumption with an assumption on the inability of the cheater to store quantum signals for a long period of time. This subject deserves further investigations. In contrast, modulo the issue of privacy amplification, the security of quantum *key distribution* has been established [9, 16, 18] and quantum cryptography is useful at least for this purpose. We expect that quantum key distribution will remain a fertile subject for years to come.

6 Acknowledgments

We thank M. Ardehali, C. H. Bennett, C. A. Fuchs, R. Jozsa, J. Kilian, D. Mayers, J. Preskill, M. H. Rubin, A. Wigderson, F. Wilczek, and A. Yao for helpful conversations.

References

[1] Ardehali, M., "A perfectly secure quantum bit commitment protocol", Los Alamos preprint archive quant-ph/9505019 (May, 1995).

[2] Ardehali, M., "A simple quantum oblivious transfer protocol", Los Alamos preprint archive quant-ph/9512026 (Dec., 1995).

[3] Bennett, Charles H, Francois Bessette, Giles Brassard, Louis Salvail, and John Smolin, "Experimental Quantum Cryptography", *Journal of Cryptology* **5**, (1992), 3-28.

[4] Bennett, Charles H, and Giles Brassard, "Quantum key distribution and coin tossing", *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, (1984), 175-179.

[5] Bennett, Charles H, and Giles Brassard, Claude Crépeau, and M.-H. Skubiszewska, "Practical quantum oblivious transfer", *Proceedings of Crypto '91*, Lecture Notes in Computer Science, Vol. 576, (Springer-Verlag, 1992), 351-366.

[6] Bennett, Charles H, Giles Brassard, and Artur K. Ekert, "Quantum cryptography", *Scientific American* (Oct. 1992), 50-57 and references therein.

[7] Brassard Giles, and Claude Crépeau, "Quantum bit commitment and coin tossing protocols", *Advances in Cryptology: Proceedings of Crypto '90*, Lecture Notes in Computer Science, Vol. 537, (Springer-Verlag, 1995), 49-61.

[8] Brassard Giles, and Claude Crépeau, Richard Jozsa, and Denis Langlois, "A quantum bit commitment scheme provably unbreakable by both parties", *Proceedings of 1993 IEEE Annual Symposium on Foundations of Computer Science*, (1993), 362-371.

[9] Deutsch, David *et al.*, "Quantum privacy amplification and the security of quantum cryptography over noisy channels", Los Alamos preprint archive quant-ph/9604039 (April, 1996).

[10] Ekert, Artur K., *Phys. Rev. Lett* **67**, (1991) 661-663.

[11] Fuchs, Christopher A., "Distinguishability and Accessible Information in Quantum Theory", Ph. D. thesis, University of New Mexico, (1995).

[12] Griffiths, Robert B. and Chi-Sheng Niu, "Semiclassical Fourier Transform for Quantum Computation", *Phys. Rev. Lett.* **76**, (1996) 3228-3231.

[13] Hughston L. P., R. Jozsa and W. K. Wootters, "A complete classification of quantum ensembles having a given density matrix", *Phys. Lett.* **A183**, (1993) 14-18.

[14] Jozsa, Richard, *Journal of Modern Optics* **41**, (1994) 2315-2323.

[15] Kilian, Joe, "Founding cryptography on oblivious transfer", *Proceedings of 1988 ACM Annual Symposium on Theory of Computing*, (May, 1988), 20-31.

[16] Lo, Hoi-Kwong, and H. F. Chau, "Quantum cryptography in noisy channels", Los Alamos preprint archive quant-ph/9511025 (Nov., 1995).

[17] Lo, Hoi-Kwong, and H. F. Chau, "Is quantum bit commitment really possible?", Los Alamos preprint archive quant-ph/9603004 (March, 1996).

[18] Mayers, Dominic, "On the security of the quantum oblivious transfer and key distribution protocols", *Advances in Cryptology: Proceedings of Crypto '95*, Lecture Notes in Computer Science, Vol. 963, (Springer-Verlag, 1995), 124-135.

[19] Mayers, Dominic, "The trouble with quantum bit commitment", Los Alamos preprint archive quant-ph/9603015 (March, 1996).

[20] Wiesner, Stephen, "Conjugate coding", *Sigact News* **15** (1983), 77-88. Manuscript written in 1970.

[21] Yao, Andrew Chi-Chih, "Security of quantum protocols against coherent measurements", *Proceedings of 1995 ACM Symposium on Theory of Computing* (May, 1995), 67-75.