What is going on with Quantum Bit Commitment?

Claude Crépeau *

Université de Montréal †

Abstract

Recent results in quantum physics indicate that Quantum Bit Commitment is impossible in a scenario where the participants have the full power of quantum mechanics to attack the protocol. This implies that *all existing protocols* for this task *can be cheated* in theory. In the current paper, we review the state of the art in quantum cryptographic protocols, and analyze the impact of this new result from a theoretical and practical point of view.

1 Introduction

The idea of using quantum physics to achieve security in cryptographic protocols marked the birth of quantum cryptography with the work of Wiesner [29] who introduced the notion of a *multiplexing channel*. Such a channel may be used by a party $\mathcal{A}$ to transmit two pieces of information w_0, w_1 to another party $\mathcal{B}$ who chooses to receive either w_0 or w_1 but cannot get both. $\mathcal{A}$ never finds out which information $\mathcal{B}$ got. This small primitive later known as one-out-of-two Oblivious Transfer by cryptographers [24, 13] can be used to implement very general cryptographic tasks of the same flavour [16, 14, 11].

Prompted by Wiesner's work, Bennett and Brassard [1] later introduced two new cryptographic applications of quantum mechanics: quantum key distribution and quantum coin-flipping. Quantum coin-flipping allows $\mathcal{A}$ and $\mathcal{B}$ to flip a coin at a distance in such a way that neither of them can force the outcome of the flip by himself but such that both of them will agree on the outcome despite the fact that they do not trust each other. Implicitly, their solution builds up on the idea of a quantum bit commitment. A *bit commitment* is a scheme allowing $\mathcal{A}$ to send a piece of information to $\mathcal{B}$ that commits her to a bit b in such a way that $\mathcal{B}$ cannot tell what b is, but such that $\mathcal{A}$ can later prove him what b originally was. You

---

* Supported in part by Québec's FCAR and Canada's NSERC.

† Département IRO, Université de Montréal, C.P. 6128, succursale "centre-ville", Montréal (Québec), Canada H3C 3J7. e-mail: crepeau@iro.umontreal.ca.

may think of this scheme as $\mathcal{A}$ sending a note with the value b written on it in a strong-box to $\mathcal{B}$ and later revealing him the combination to the safe.

A rather surprising fact is that both Wiesner's multiplexing channel and Bennett–Brassard's coin-flipping came with precise quantum mechanical instructions to break these schemes! In those early days, only the security of quantum key distribution was conceivable. We will look more closely at the quantum bit commitment scheme behind Bennett–Brassard's coin-flipping protocol and its attack in section 2.

More recently, Crépeau and Kilian [12] have presented an alternative protocol for one-out-of-two Oblivious Transfer. Crépeau [9, 10] showed that this protocol is secure if neither parties can store photons for long periods of time and if only Von Neumann measurements are allowed. Alternatively, the first restriction may be dropped if we have a secure bit commitment protocol. A more robust version of this protocol that deals with transmission errors may be found in [2]. Mayers and Salvail [22] have later shown that the second restriction may be reduced to general measurements involving only one photon at a time, and finally Yao [30] showed that no restrictions on the type of measurements is necessary. Lately, Mayers [21] has shown a result similar to Yao's for the more robust protocol of [2].

Similarly, a new protocol for quantum bit commitment has been developed by Brassard and Crépeau [6] in order to close the gap and obtain a secure one-out-of-two Oblivious Transfer. Moreover, an extension due to Brassard, Crépeau, Jozsa and Langlois of this protocol that deals with transmission errors was claimed to be *provably unbreakable by both parties* [7]. Unfortunately, it turns out that this claim was wrong. The protocol of [7] may be broken in theory for similar reasons as the protocol of Bennett and Brassard as demonstrated by Mayers [20]. Note that a similar weaker result was later achieved by Lo and Chau [17]. Indeed, a more general result of Mayers [19] suggests that no quantum bit commitment scheme may be secure. The ideas behind this work will be covered in sections 3 and 4.

Section 4.1 considers the practical consequences of this result and some new approaches to bypass Mayers' result are analyzed in section 5. A new quantum bit commitment protocol is presented with potential scenarios under which it could be secure. Possibilities under consideration are to rely temporarily on a computational assumption or to obtain security without assumptions in a multiprover model.

Whether this means that secure quantum cryptography is from now on solely restricted to quantum key distribution is debatable. The purpose of this paper is to explain the theoretical and practical consequences of Mayers' result and exhibit current research directions to find reasonable assumptions under which quantum bit commitment and other protocols that are built from it may still be shown secure.

For the rest of this paper we assume that the reader is familiar with quantum cryptography and some basic notions of quantum physics. We suggest some readings [7, 23] if you need introduction to the topic.

2 The BB84 Bit Commitment

We first review the bit commitment scheme of [1]. Let $|\leftrightarrow\rangle, |\swarrow\!\!\nearrow\rangle, |\updownarrow\rangle, |\nwarrow\!\!\searrow\rangle$ be the four states of light polarization of angles $0°, 45°, 90°, 135°$. For simplicity, we denote these four states $|0,0\rangle, |1,0\rangle, |0,1\rangle, |1,1\rangle$.

Protocol 2.1 (BB84(b))

1: $\mathbf{\underset{i=1}{\overset{n}{DO}}}$ *$\mathcal{A}$ picks a bit m_i and sends a photon π_i with polarization $|b, m_i\rangle$ to $\mathcal{B}$,*

2: $\mathbf{\underset{i=1}{\overset{n}{DO}}}$ *$\mathcal{B}$ picks a bit b'_i and measures π_i with basis $[\leftrightarrow, \updownarrow]$ if $b'_i = 0$ and $[\swarrow\!\!\nearrow, \nwarrow\!\!\searrow]$ otherwise.*

Let $|b'_1, m'_1\rangle, |b'_2, m'_2\rangle, ..., |b'_n, m'_n\rangle$ be $\mathcal{B}$'s outcomes. At each round, if $b'_i = b$, he observes $m'_i = m_i$, but if $b'_i \neq b$, m'_i and m_i are not correlated. At a later time, $\mathcal{A}$ may unveil her bit by disclosing b and $m_1, m_2, ..., m_n$ to $\mathcal{B}$ who accepts this commitment only if for all i such that $b'_i = b$, he observed $m'_i = m_i$.

If $\mathcal{A}$ behaves as described in this protocol her bit is not disclosed to $\mathcal{B}$ whatever he does. The reason for this fact is that quantum ensembles (systems with various possibilities) are characterized by a *density matrix* (please consult [7] if you are not familiar with this notion). In this case the density matrix ρ_0 connected to the possible ways in which $\mathcal{A}$ may commit to $b = 0$ is identical to the density matrix ρ_1 connected to the possible ways in which $\mathcal{A}$ may commit to $b = 1$. When two systems are characterized by the same density matrix, no measurement whatsoever can tell them apart. Nevertheless in practice, $\mathcal{B}$ is able to tell the two possibilities apart whenever by accident he receives more than one photon at a single round (it is merely impossible to control the quantum system well enough that only single photons will go across). If he measures both photons along a single basis and get two different answers, it implies that the incoming photons where polarized in the other basis and thus reveal b.

The fact that $\mathcal{A}$ is committed to a bit via this protocol is more difficult to prove. If she created the photons has described above she would be since she does not know how $\mathcal{B}$ measured each of them, but indeed with a different behaviour she is not committed at all! As explained in [1], $\mathcal{A}$ may send at each round of step 1 one particle from an EPR-pair and keep its twin for later measurement. If $\mathcal{A}$ wants to unveil $b = 0$ she measures all her particles with basis $[\leftrightarrow, \updownarrow]$ and $[\swarrow\!\!\nearrow, \nwarrow\!\!\searrow]$ to unveil $b = 1$. If she observes $|b, z_i\rangle$ then she sets $m_i = \bar{z}_i$. The EPR-property guarantees that when $b'_i = b$, $\mathcal{B}$ observed $m'_i = \bar{z}_i$ as required.

In consequence, $\mathcal{B}$ can cheat this protocol in practice and $\mathcal{A}$ can cheat this protocol in theory. The next protocol had been designed to solve these two problems. For a while most people were convinced this goal was reached. Unfortunately, only the first attack is solved by this protocol.

3 The BCJL93 Bit Commitment

In [7] a new protocol (based on [6]) was introduced to fix the above attacks together with a "proof" of security. We first present vaguely the structure of the protocol. The details are omitted as they are irrelevant to the attack we describe next. We invite the reader to consult [18] for more details about codes.

Protocol 3.1 (BCJL93(b) **)**

1: *$\mathcal{B}$ chooses a code C and announces it to $\mathcal{A}$,*

2: *$\mathcal{A}$ chooses a mapping $f : C \rightarrow \{0, 1\}$ and announces it to $\mathcal{B}$,*

3: *$\mathcal{A}$ picks an n-bit codeword c from C such that $f(c) = b$,*

4: $\underset{i=1}{\overset{n}{\textbf{DO}}}$

- *$\mathcal{A}$ picks a bit b_i and sends to $\mathcal{B}$ a photon π_i with polarization $|b_i, c_i\rangle$,*
- *$\mathcal{B}$ picks a bit b'_i and measures π_i with basis $[\leftrightarrow, \updownarrow]$ if $b'_i = 0$ and $[\nearrow, \nwarrow]$ otherwise.*

Let $|b'_1, c'_1\rangle, |b'_2, c'_2\rangle, ..., |b'_n, c'_n\rangle$ be $\mathcal{B}$'s outcomes. At each round, if $b'_i = b_i$, he observes $c'_i = c_i$, but if $b'_i \neq b_i$, c'_i and c_i are not correlated. At a later time, $\mathcal{A}$ may unveil her bit by disclosing b, $b_1, b_2, ..., b_n$ and $c_1, c_2, ..., c_n$ to $\mathcal{B}$ who accepts this commitment only if c is a codeword and for almost all i such that $b'_i = b_i$, he observed $c'_i = c_i$ (this allows errors).

As for the BB84 protocol, if $\mathcal{A}$ behaves as described in this protocol her bit is not disclosed to $\mathcal{B}$ whatever he does. In this case the density matrix ρ_0 connected to the possible ways in which $\mathcal{A}$ may commit to $b = 0$ is not strictly identical to the density matrix ρ_1 connected to the possible ways in which $\mathcal{A}$ may commit to $b = 1$. Nevertheless these matrices are so close that they cannot be distinguished efficiently [7].

The part of the "proof" of [7] that goes wrong is the fact that $\mathcal{A}$ is committed to a bit. The paper shows that $\mathcal{A}$ is unable to know *at the same time* information to unveil the commitment as $b = 0$ and as $b = 1$ and concludes that $\mathcal{A}$ cannot change her mind. The first part of the statement is correct, but not the conclusion. As a matter of fact, the first part of the statement is also true of the BB84 protocol and we know that it can be broken!

What is going on?

The correct statement should have been that $\mathcal{A}$ is unable to know *at her choosing* information to unveil the commitment as $b = 0$ or as $b = 1$, but not at the same time. This is precisely what she can do in the BB84 protocol: postpone this choice to the moment of unveiling her bit. The same cheat will work here as we now explain.

4 The general attack of Mayers

The attack to this protocol due to Mayers [20] is based on a recent theorem of Hughston, Jozsa, and Wootters about classification of quantum ensembles [15] that we now review.

Theorem 4.1 *Let $\psi_1, \psi_2, ..., \psi_m$ and $\varphi_1, \varphi_2, ..., \varphi_n$ be two sets of possible quantum states with associated probabilities described by an identical density matrix ρ. It is possible to construct a composite system $\alpha \otimes \beta$ such that β alone has density matrix ρ and such that there exists a pair of measurements M_ψ, M_φ with the property that applying M_ψ (resp. M_φ) to α yields an index i of state ψ_i (resp. φ_i) to which β will have collapsed.*

A simple application of this theorem is the earlier stated attack against the BB84 bit commitment scheme: in that case β is the set of EPR-particles that $\mathcal{A}$ sent to $\mathcal{B}$, while α is the EPR-twins she kept for herself. The two measurements M_ψ, M_φ are the Von Neumann measurement along bases $[\leftrightarrow, \updownarrow]$ and [⤢, ⤡].

Mayers [20] has applied this theorem to the BCJL93 protocol and thus demonstrated its weakness: Let $\psi_1, \psi_2, ..., \psi_m$ and $\varphi_1, \varphi_2, ..., \varphi_m$ be two sets of possible quantum states describing what $\mathcal{A}$ would send to $\mathcal{B}$ to commit to $b = 0$ and $b = 1$. They respectively have density matrix ρ_0 and ρ_1. In principle $\mathcal{A}$ can create a composite system $\alpha \otimes \beta$ where β has density matrix ρ_0, that she can send to $\mathcal{B}$ in order to later force β to collapse to one of the ψ_i's to unveil $b = 0$ or one of the φ_i's to unveil $b = 1$ by measuring α appropriately. Mayers showed that this can be done despite the small difference between ρ_0 and ρ_1 (a subtlety overlooked in [17]). The fact that $\mathcal{B}$ may or not make measurements on β *before* $\mathcal{A}$ causes it to collapse to a specific state is irrelevant; $\mathcal{B}$'s outcomes would be the same.

For similar reasons, any bit commitment scheme where $\mathcal{B}$ is unable to tell whether the committed bit is $b = 0$ or $b = 1$, can be cheated by $\mathcal{A}$ using a theorem similar to the above. This result of Mayers [19] clearly indicate that quantum bit commitment is jeopardized.

4.1 Practical Impact

Question: How much impact does this theorem have in practice? **Answer:** Little.
The technology required to implement the general attack of Mayers seems to be more or less the power of a quantum computer [4]. (Nevertheless, it is *not proven* that breaking a specific system such as BCJL93 is as hard as building a quantum computer.) Standard cryptosystems like RSA [25] would also collapse if such machines were built [28]. Indeed, most of public-key cryptography would be wiped out by the quantum computer. Therefore, Mayers' attack has little practical consequence unless standard public-key cryptosystems can be broken as well. Using today's technology it is fairly easy to implement BCJL93's bit commitment. This protocol is perfectly secure against $\mathcal{B}$'s attacks and secure against $\mathcal{A}$'s attacks she can implement with today's technology.

Contrary to constructions of bit commitment and other cryptographic protocols from computational assumptions that can be cracked retroactively when a quantum computer becomes available, constructions based on quantum physics will only be breakable starting at the time where the quantum computer is realized.

Salvail has recently showed [26] that a protocol similar to BCJL93 is secure against attacks from both parties in a model where only measurements on single photons at a time are permitted. Thus only major improvements in quantum technology may eventually yield attacks against the scheme.

5 Alternative approaches

Of course, relying on technological limits is not at all satisfying from a theoretical view point. One approach we have considered is to rely temporarily on a different kind of bit commitment (computational for instance) in order to limit the measurements of the players and later drop this short-term assumption to obtain a quantum bit commitment not relying on any long-term assumption.

We first present a protocol inspired from Crépeau's protocol for one-out-of-two Oblivious Transfer[10] without the temporary bit commitment in order to explain clearly its features and then proceed with the full protocol.

Protocol 5.1 (C96(b) **)**

1: $\mathop{\mathbf{DO}}_{i=1}^{n}$ *$\mathcal{A}$ picks bits b_i, m_i and sends a photon π_i with polarization $|b_i, m_i\rangle$ to $\mathcal{B}$,*

2: $\mathop{\mathbf{DO}}_{i=1}^{n}$ *$\mathcal{B}$ picks a bit b'_i and measures π_i with basis $[\leftrightarrow, \updownarrow]$ if $b'_i = 0$ and $[\nearrow, \nwarrow]$ otherwise,*

3: $\mathop{\mathbf{DO}}_{i=1}^{n}$ *$\mathcal{B}$ reveals b'_i,*

4: *$\mathcal{A}$ selects from $\{1, 2, ..., n\}$ two disjoint sets J_0, J_1 of size $n/2$ such that $\forall j \in J_0, [b_j = b'_j]$ or $\forall j \in J_1, [b_j \neq b'_j]$ and announces $J_b, J_{\bar{b}}$ to $\mathcal{B}$.*

Let $|b'_1, m'_1\rangle, |b'_2, m'_2\rangle, ..., |b'_n, m'_n\rangle$ be $\mathcal{B}$'s outcomes. At each round, if $b'_i = b_i$, he observes $m'_i = m_i$, but if $b'_i \neq b_i$, m'_i and m_i are not correlated. When $\mathcal{A}$ finds out $\mathcal{B}$'s measuring bases at step 3 she learns which m_i are correlated and which are not. Thus she is able at step 4 to create the two subsets one of which is completely known or completely unknown. At a later time, $\mathcal{A}$ may unveil her bit by disclosing b, J_0, J_1 and $b_1, b_2, ...b_n, m_1, m_2, ..., m_n$ to $\mathcal{B}$ who accepts this commitment only if for almost all $i \in J_0$ we have $b'_i = b_i$ and he observed $m'_i = m_i$. Of course he also checks that he received J_0, J_1 when $b = 0$ and J_1, J_0 when $b = 1$.

The idea behind this protocol is that if $\mathcal{A}$ really behaves as described in the protocol, $\mathcal{B}$ is unable to tell b since he does not know the b_i's and $\mathcal{A}$ is unable to change her mind because half of $\mathcal{B}$'s photons are not correlated from what she sends in the beginning of the protocol. Unfortunately, it is very easy for a misbehaving $\mathcal{A}$ to cheat this protocol using EPR-pairs as for the BB84 scheme.

The complete version of the protocol is a proposal for quantum bit commitment built from the assumption that we already have a temporary bit commitment (TMP(b)) of another nature to bootstrap the process. The short-term bit commitments are used to force $\mathcal{A}$ to have correct behaviour as in the above simple protocol.

Protocol 5.2 (C96+(b))

1: $\mathop{\mathbf{DO}}\limits_{i=1}^{n}$ *$\mathcal{A}$ picks bits b_i, m_i and sends a photon π_i with polarization $|b_i, m_i\rangle$ to $\mathcal{B}$,*

2: $\mathop{\mathbf{DO}}\limits_{i=1}^{n}$ *$\mathcal{B}$ picks a bit b'_i and measures π_i with basis $[\leftrightarrow, \updownarrow]$ if $b'_i = 0$ and $[\nearrow\!\!\!\swarrow, \nwarrow\!\!\!\searrow]$ otherwise,*

3: *$\mathcal{A}$ commits via $TMP(b_1), TMP(m_1), TMP(b_2), TMP(m_2), ..., TMP(b_n), TMP(m_n)$,*

4: *$\mathcal{B}$ picks from $\{1, 2, ..., n\}$ two disjoint sets I_0, I_1 of size $n/2$ and announces them to $\mathcal{A}$,*

5: *For each $i \in I_0$, $\mathcal{A}$ unveils b_i, m_i,*

6: *$\mathcal{B}$ is willing to continue if for almost all $i \in I_0$ such that $b_i = b'_i$ he observed $|b'_i, m_i\rangle$,*

7: $\mathop{\mathbf{DO}}\limits_{i=1}^{n}$ *$\mathcal{B}$ reveals b'_i,*

8: *$\mathcal{A}$ selects from I_1 two disjoint sets J_0, J_1 of size $n/4$ such that $\forall j \in J_0, [b_j = b'_j]$ or $\forall j \in J_1, [b_j \neq b'_j]$ and announces $J_b, J_{\bar{b}}$ to $\mathcal{B}$.*

The test of steps 3 to 6 convinces $\mathcal{B}$ that $\mathcal{A}$ *knows* precisely the states of each individual photons she sent in step 1. We now review some possibilities we have considered for the temporary bit commitment.

5.1 Computational Bit Commitment

A way to implement the above protocol is to use a computational bit commitment for TMP (consult [5] for several examples). If we do this assuming that $\mathcal{B}$ is computationally limited, he may eventually break this assumption and figure out $\mathcal{A}$'s commitments of step 3, and thus find out her global commitment to b as well. Thus the whole protocol is only computationally secure and there is no point using anything quantum at all!

If we do this assuming that $\mathcal{A}$ is computationally limited (again consult [5] for several examples), it seems that she must break this assumption on-line in order to cheat using Mayers' attack. Nevertheless, Brassard and Mayers [8] have shown that Mayers' attack stretches to this situation and $\mathcal{A}$ may arrange to open as $b = 0$ or $b = 1$ *without breaking the computational assumption*! The computational approach is apparently a dead end but several options are still to be analyzed.

5.2 Multiprover Bit Commitment

Salvail has recently suggested [27] to combine the above protocol with a multiprover model as introduced in [3]. In this setting, the committing party is split in two entities $\mathcal{A}$ and $\mathcal{A}'$ collaborating but physically separated for a short period of time. They could either be spatially separated or isolated in Faraday cages to avoid any kind of classical communication between them. Commitment in such a model is easy: $\mathcal{A}$ and $\mathcal{A}'$ a priori share a bit x; later if $\mathcal{A}$ wishes to commit to $b = 0$ she sends x to $\mathcal{B}$ while to commit to $b = 1$ she sends $\bar{x}$; to unveil this commitment $\mathcal{A}'$ discloses x. The multiprover approach is very promising and will be detailed in a future paper.

6 General Cryptographic Protocols

From a theoretical view point, Mayers' result has completely obliterated the possibility of a secure quantum bit commitment with no further assumption. Does that imply the same for general cryptographic protocols? In a classical model, one-out-of-two oblivious transfer can be used to implement a bit commitment, therefore if the later is not possible, the former would not be either. However, in the quantum model, the standard reduction of bit commitment to one-out-of-two oblivious transfer may not work: in the light of Mayers' result this standard reduction might be cheated as well. Thus, the possibility of a quantum oblivious transfer is not discarded directly by Mayers' result. Nevertheless, the power of this primitive would clearly not be the same as in the classical model and therefore current reductions of general cryptographic protocols to one-out-of-two oblivious transfer may no longer work. Some cryptographic protocols may still be achieved, some may not.

On the other hand, if we are willing to make extra (temporary) assumptions it may very well be that both bit commitment and oblivious transfer can be achieved and using standard reductions [16, 11], all cryptographic protocols as well. From a practical point of view, the same remarks as before apply: unless an adversary can build a quantum computer, we may still reason as before and implement bit commitment, oblivious transfer and general cryptographic protocols securely.

7 Conclusion

Mayers has showed that in theory quantum bit commitment is impossible in a context were the parties involved may use the full power of quantum mechanics to attack the protocol. We have seen that unless one can actually build a quantum computer, this has little practical impact. Some alternatives have been considered: temporary extra assumptions such as multiprover systems may save the game.

The big lesson to learn from all this is that reasoning about quantum information is always more elaborate than its classical counterpart and that extra care must be taken when analyzing quantum cryptographic protocols.

Acknowledgments

I thank Don Beaver, Gilles Brassard, Jeroen van de Graaf, Dominic Mayers and Louis Salvail for several exciting discussions about this work.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public-key distribution and coin tossing", In *Proceedings of the International Conference on Computers, Systems and Signal Processing*, Bangalore, India, December 1984, pp. 175 – 179.

[2] C. H. Bennett, G. Brassard, C. Crépeau and M.–H. Skubiszewska, "Practical quantum oblivious transfer", *Advances in Cryptology: Crypto '91 Proceedings*, Springer-Verlag, 1992, pp. 351 – 366.

[3] M. Ben-Or, S. Goldwasser, J. Kilian and A. Wigderson, "Multi-Prover Interactive Proofs: How to Remove Intractability Assumptions", *Proceedings of 20th Annual ACM Symposium on Theory of Computing*, 1988, pp. 113 – 132.

[4] G. Brassard, "A quantum jump in computer science", in *Computer Science Today*, J. van Leeuwen (editor), Lecture Notes in Computer Science, Vol. 1000 (special anniversary volume), Springer-Verlag, Berlin, 1995, pp. 1 – 14.

[5] G. Brassard, D. Chaum and C. Crépeau, "Minimum disclosure proofs of knowledge", *Journal of Computer and System Sciences*, Vol. 37, no. 2, 1988, pp. 156 – 189.

[6] 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, Springer-Verlag, 1991, pp. 49 – 61.

[7] 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 Foundations of Computer Science*, November 1993, pp. 362 – 371.

[8] G. Brassard and D. Mayers, *Personal Communication*, 1996.

[9] C. Crépeau, "Correct and private reductions among oblivious transfers", PhD thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 1990. (Supervised by Silvio Micali.)

[10] C. Crépeau, "Quantum oblivious transfer", *Journal of Modern Optics*, Vol. 41, no. 12, December 1994, pp. 2445 – 2454.

[11] C. Crépeau, J. van de Graaf and A. Tapp, "Committed oblivious transfer and private multi-party computations", *Advances in Cryptology: Crypto '95 Proceedings*, Springer-Verlag, 1995, pp. 110 – 123.

[12] C. Crépeau and J. Kilian, "Achieving oblivious transfer using weakened security assumptions", *Proceedings of 29th Annual IEEE Symposium on Foundations of Computer Science*, 1988, pp. 42 – 52.

[13] S. Even, O. Goldreich and A. Lempel, "A randomized protocol for signing contracts", *Advances in Cryptology: Proceedings of Crypto '82*, Plenum Press, New York, 1983, pp. 205 – 210.

[14] O. Goldreich, S. Micali and A. Wigderson, "How to play any mental game, or: A completeness theorem for protocols with honest majority", *Proceedings of 19th Annual ACM Symposium on Theory of Computing*, 1987, pp. 218 – 229.

[15] L.P. Hughston, R. Jozsa and W.K. Wootters, "A complete classification of quantum ensembles having a given density matrix", *Physics Letters A*, vol. 183, 1993, pp. 14 – 18.

[16] J. Kilian, "Founding cryptography on oblivious transfer", *Proceedings of 20th Annual ACM Symposium on Theory of Computing*, 1988, pp. 20 – 31.

[17] H.–K. Lo and H.F. Chau, "Is Quantum Bit Commitment Really Possible?", manuscript posted on Los Alamos reprint archive quant-ph, March 96.

[18] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[19] D. Mayers, "Unconditionally Secure Quantum Bit Commitment is Impossible", submitted to PHYSCOMP96, Boston MA, 1996; manuscript posted on Los Alamos reprint archive quant-ph, May 96.

[20] D. Mayers, "The trouble with Quantum Bit Commitment", manuscript posted on Los Alamos reprint archive quant-ph, March 96; first presented at a workshop on quantum information theory, Montréal, October 1995.

[21] D. Mayers, "Quantum Key Distribution and String Oblivious Transfer on Noisy Channels", manuscript posted on Los Alamos reprint archive quant-ph, June 96; To appear in *Advances in Cryptology: Proceedings of Crypto '96*, Lecture Notes in Computer Science, Springer-Verlag, 1996.

[22] D. Mayers and L. Salvail "Quantum Oblivious Transfer is Secure Against Individual Measurements", *Proceedings of the Third Workshop on Physics and Computation — PhysComp '94*, Dallas, November 1994, IEEE Computer Society Press, 1994, pp. 69 – 76.

[23] A. Peres, "Quantum Theory: Concepts and Methods", Fundamental Theories of Physics, Vol. 57, Kluwer Academic Publisher, 1993.

[24] M. O. Rabin, "How to exchange secrets by oblivious transfer", Technical Memo TR–81, Aiken Computation Laboratory, Harvard University, 1981.

[25] R.L. Rivest, A. Shamir and L.M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, Vol. 21, No. 2, Feb 1978, pp. 120 – 126.

[26] L. Salvail, "Variations sur le transfert inconscient en cryptographie quantique" to appear as a Ph.D. Thesis, Département d'Informatique et de Recherche Opérationnelle, Université de Montréal, 1996.

[27] L. Salvail, *Personal Communication*, 1996.

[28] P. Shor, "Algorithms for quantum computation: Discrete logarithm and factoring", *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, 1994, pp. 124 – 134.

[29] S. Wiesner, "Conjugate coding", *Sigact News*, Vol. 15, no. 1, 1983, pp. 78 – 88. Original manuscript written circa 1970.

[30] A. Yao, "Security of Quantum Protocols Against Coherent Measurements", *Proceedings of the 26th Symposium on the Theory of Computing,* June 1995, pp. 67 – 75.