Heads or Tails? Quantum Bit Commitment (fails)

Pablo Funes

October 9, 1999

1 Quantum Cryptography

Quantum cryptography began in 1984 with the description by Bennett and Brassard of their famous Quantum Key Distribution (QKD) protocol [1]. The central idea behind QKD is that, according to quantum physics, observation necessarily modifies the state of what is being observed. This implies that two parties can be clever enough to set up a communication scheme which allows them to detect any eavesdropping — because they will be able to observe the disturbances introduced by such enemy action.

Papers on cryptography discuss scenarios involving three fictional characters: Alice (or simply A) who tries to send a message to Bob (B), and Eve, who is the evil eavesdropper trying to intercept their conversation (figure 1).

The same seminal paper of Bennett and Brassard contained a quantum coin tossing protocol. Here, Eve is not present; Alice and Bob are college students who want to flip a coin over the (quantum) phone to decide who is going to do the homework for the other. Alice flips the coin but she needs some means to convince Bob that she is telling him the truth about the outcome of the toss.

Bennett and Brassard's work generated a huge field of research, both on

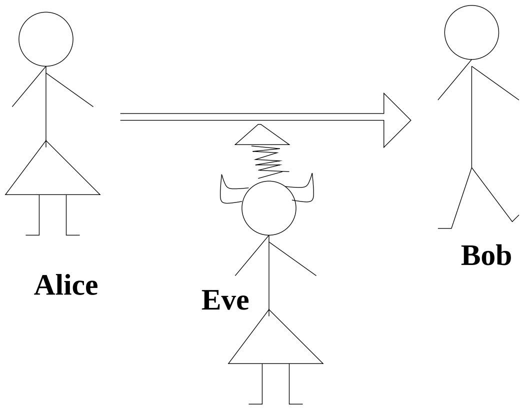

Figure 1: Alice, Bob and Eve[2]

the better known QKD protocols as in Quantum Bit Commitment (QBC), which followed from the coin flipping scenario. Both seemed to follow more or less parallel trends, with improved protocols, error correction, proofs of security, and so on, until QBC was — much to the embarrassment of those who had published "proofs" of its robustness — shown to be insecure and beyond all possible repair. The present paper is a brief account of this story.

2 Quantum Computing

Quantum computing is to computation as quantum cryptography is to encryption: it tries to take advantage of quantum mechanical properties of the world to enable things that were not possible before. Here, the central idea is that of quantum parallelism, namely, the fact that "entangled" states can be thought of as probabilistic superpositions of classical states. An algorithm could carry out computations on all possible inputs at the same time. The idea and foundations for this hypothetical machines were laid out during the early nineties ([9], [3]), and P. Shor's 1994 paper [19] brought it to the spotlight with his quantum algorithm for factoring integer numbers in polynomial time. This work shocked the cryptography world as well, because today's better security protocols rely upon the difficulty of factoring large integers.

Quantum cryptography, quantum computation, quantum information are nowadays hot research areas, both in the theory, foundations and algorithms aspects as in actual devices to implement them. In this respect, quantum cryptography and transmission are far ahead: there have been already several demonstrations of quantum communications channels spanning distances of several kilometers ([18], [6]). Quantum computing lags behind, and only primitive demonstrations of one or two quantum bits have taken place [15]. It seems that quantum key distribution could be of practical use very soon, whereas the quantum computer is farther away in the future, if it ever becomes a reality.

3 "Post-Cold War" Cryptographic Scenarios

The classical application of cryptography occurs on war or espionage scenarios, Alice-Eve-Bob, where A needs to send secret information to B over channels that may be insecure. Other cryptographic problems are sometimes referred to as "post-cold-war", or "peaceful". Remote coin tossing is one. Another example is that of two would-be business partners who wish to know whether or not their combined capitals are enough for a certain joint venture, without revealing their individual amounts to each other.

Cryptography research is concerned with finding fundamental operations and protocols which can be used as building blocks for the more elaborate problems. "Trap-door" or "one-way" functions for example, which are bijective functions easy to compute in one direction, but infeasible in the other, allow for the description of various protocols without dealing with the details of which particular function one would prefer to use.

Bit commitment (BC) is one such basic protocol which can be used as a foundation for all the so-called post war cryptography:

- Bit Commitment

1. Commitment Phase: Alice chooses one bit b, zero or one, in a way that guarantees to Bob that she has made her decision already and it is not subject to change. She will probably give Bob some *proof of commitment.*

2. Disclosure Phase: Later in time, Alice tells Bob what b was. Bob is satisfied that this is the same value that b had at the end of phase 1.

A useful analogy for bit commitment is that of a safe box and a key: Alice writes down her bit in a piece of paper and puts it in a safe box, which she locks. She gives Bob the box but not the key. For the disclosure stage, Alice gives Bob the key so he can open the box and verify what the bit was. Since he has been holding the box all the time, he can be sure that the paper has not changed. Also, Alice kept the key, so she is sure that Bob was not able to peek inside.

With today's cryptography one would do this using a trap-door function, as in the following example:

- BC implemented with RSA:

1. Commitment Phase:

   (a) A chooses two large primes, p and q, and reveals $n = pq$ along with a public k such that $(k, (p-1)(q-1)) = 1$.

   (b) A chooses her bit b and a random integer $0 < z < n$ such that $z \equiv b \mod 2$.

   (c) A broadcasts $x = z^k \mod n$.

2. Disclosure Phase

   (a) A reveals b and z

(b) B observes that $z \equiv b \mod 2$ and computes $z^k \mod n$ to verify that it equals x.

Commitments like this are at the heart of many everyday games and business applications. In an international bid for example, contractors send in their quotations with the prices they would charge to do some public works enterprise, such as a bridge. All bids are kept in closed envelopes and open at the same time. The contractor with the lower price is the one hired for the task. This high-profile protocols are threatened by espionage, corruption and the like, and the sealed envelopes are not always that much sealed nor the information they contained is that much of a constant.

It is easy to define a remote coin tossing protocol if one has a BC protocol ready:

- Remote Coin Tossing based upon Bit Commitment

1. Alice chooses a random bit b and commits to it.
2. Once Bob received a proof of commitment, he chooses a random bit b' himself and announces it to Alice
3. b is now disclosed. If $b = b'$ then Bob wins the coin toss, otherwise Alice wins.

The original Bennett and Brassard protocol for Quantum Bit Commitment (QBC) was presented as a coin tossing protocol, but can be easily rephrased into the better known form of bit commitment discussed below.

Yao [20] has shown that a secure QBC can be used to implement a secure *Oblivious Transfer* which in turn is a foundation for the more general problem of *Secure Two-party Computation* [10], also known as *Discreet Decision Making*. Here two parties A and B wish to compute the value of a function $f(x, y)$ for x known by A and y known by B, without revealing more information to B (resp. A) than what he can already deduct by knowing $\{y, f(x, y)\}$

(resp $\{x, f(x,y)\}$). The joint capital problem mentioned above is one of this kind.

4 Quantum Bit Commitment

The BB84 QBC protocol by Bennett and Brassard [1] is quite similar to the well-known BB84 QKD protocol:

- BB84 Quantum Bit Commitment Protocol[1]

1. Commitment Phase

   (a) A chooses her bit b and s random bits $\{b_i\}$. Then proceeds to send s particles to B, each one encoding b_i with respect to the basis $\{\rightarrow, \uparrow\}$ (if $b = 0$) or $\{\nearrow, \nwarrow\}$ (if $b = 1$)

   (b) B chooses s random bits $\{b'_i$ and measures the qubits received with respect to the basis $\{\rightarrow, \uparrow\}$ (when $b_i\prime = 0$) or $\{\nearrow, \nwarrow\}$ (when $b_i\prime = 1$).

2. Disclosure Phase

   (a) A reveals b and $\{b_i\}$. B verifies that b was measured for all i such that $b_i = b_i\prime$.

Table 1 enumerates the probabilities of measuring either 0 or 1 depending on the values of b, b_i and $b_i\prime$.

Here b is hidden in the basis, either horizontal or rotated by 45 degrees. Alice is sending a mixture of orthogonal states to confuse Bob, who can not tell whether is receiving mixed $\rightarrow$'s and $\uparrow$'s or mixed $\nearrow$'s and $\nwarrow$'s. It all

[1] The original BB84 talked about photons and their polarizations. As I am not addressing the actual physical implementations, I will speak of "qubits", "photons" or "particles" as if they were synonyms.

Table 1: BB84 Protocol.

b	b_i	qubit sent	$b_i\prime$	measurement basis	P(0 measured)	P(1 measured)
0	0	$\rightarrow$	0	$\{\rightarrow,\uparrow\}$	1	0
0	0	$\rightarrow$	1	$\{\nearrow,\nwarrow\}$	$\frac{1}{2}$	$\frac{1}{2}$
0	1	$\uparrow$	0	$\{\rightarrow,\uparrow\}$	0	1
0	1	$\uparrow$	1	$\{\nearrow,\nwarrow\}$	$\frac{1}{2}$	$\frac{1}{2}$
1	0	$\nearrow$	0	$\{\rightarrow,\uparrow\}$	$\frac{1}{2}$	$\frac{1}{2}$
1	0	$\nearrow$	1	$\{\nearrow,\nwarrow\}$	1	0
1	1	$\nwarrow$	0	$\{\rightarrow,\uparrow\}$	$\frac{1}{2}$	$\frac{1}{2}$
1	1	$\nwarrow$	1	$\{\nearrow,\nwarrow\}$	0	1

will make sense, however, when the list of initial polarizations is sent: he will have measured 50% of the particles with the correct basis, providing a certain measure. If any of those turns out to be incorrect, he will know that cheating was involved.

Before the disclosure takes place, B gains no information at all from the protocol, as illustrated by table 1. He could try to cheat by using any arbitrary basis, but whatever measurements he does, the randomness of $\{b_i\}$ implies that he cannot guess the value of b before the disclosure phase (table 2). Due to the orthogonality of the measurement basis, we know that

Table 2: B tries to gain early information

b	b_i	qubit sent	measurement basis	P(0 measured)	P(1 measured)
0	0	$\rightarrow$	$\{(\xi_0,\xi_1),(\eta_0,\eta_1)\}$	$\lvert\xi_0\rvert^2$	$\lvert\eta_0\rvert^2$
0	1	$\uparrow$	$\{(\xi_0,\xi_1),(\eta_0,\eta_1)\}$	$\lvert\xi_1\rvert^2$	$\lvert\eta_1\rvert^2$
1	0	$\nearrow$	$\{(\xi_0,\xi_1),(\eta_0,\eta_1)\}$	$\frac{1}{2}+\Re(\xi_0\overline{\xi_1})$	$\frac{1}{2}+\Re(\eta_0\overline{\eta_1})$
1	1	$\nwarrow$	$\{(\xi_0,\xi_1),(\eta_0,\eta_1)\}$	$\frac{1}{2}-\Re(\xi_0\overline{\xi_1})$	$\frac{1}{2}-\Re(\eta_0\overline{\eta_1})$

$|\xi_0|^2 = (1-|\eta_0|^2) = |\eta_1|^2 = (1-|\xi_1|^2)$ and also $\Re(\xi_0\overline{\xi_1}) = -\Re(\xi_0\overline{\xi_1})$, so the probabilities of measuring 0 and 1 when $b_i = 0$ are reciprocal to those obtained when $b_i = 1$. All put together, whatever measurement B does, he gains no information on b without knowing b_i[2].

When A reveals the list of $\{b_i\}$, B is able to confirm that indeed all his measurements gave the right value for the approximately $\frac{s}{2}$ times that b_i was equal to $b_{i'}$.

Also, A cannot cheat, for table 3 suggests that whatever she sends will have a probability equal to $|\beta|^2$ of being caught if she tries to make believe it was a zero, and of $\frac{1}{2} - \Re(\alpha\overline{\beta})$ if she tries to make believe it was a one (when it happens to be measured with the aligned basis). The only way to be certain that B will accept the protocol is to either make $|\beta|^2 = 0$ by sending $\rightarrow$ and committing to zero or make $\frac{1}{2} - \Re(\alpha\overline{\beta}) = 0$ by sending $\nwarrow$ and committing to one.

Table 3: Alice sends Bob treacherous data

qubit sent	$b_{i'}$	measurement basis	P(0 measured)	P(1 measured)
(α,β)	0	$\{\rightarrow,\uparrow\}$	$\lvert\alpha\rvert^2$	$\lvert\beta\rvert^2$
(α,β)	1	$\{\nearrow,\nwarrow\}$	$\frac{1}{2} - \Re(\alpha\overline{\beta})$	$\frac{1}{2} + \Re(\alpha\overline{\beta})$

If A would be willing to take risks, she would face a situation as in figure 2, where we have set $(\alpha,\beta) = (\cos(\theta), \sin(\theta))$[3]. With $\theta = \frac{\pi}{8}$ for example, the probability of error is $\cong 0.15$ for both measurements, so A would not be caught with a probability of $\cong (.15)^{s/2}$ which rapidly approaches zero when the protocol is done with a sufficiently large number s of iterations.

This protocol looks as secure as Quantum Key Distribution, at a first glance. It does have a failure, however, as Bennett and Brassard realized from the beginning.

[2] Crépeau suggested [8] that quantum transmition of photons is prone to duplication. I.e., sometimes Alice will inadvertedly send two photons (with identical polarization) instead of just one. In this lucky situation, Bob should measure both particles with respect to the same basis. If he happens to obtain two different answers, he will know that the photons were not aligned with that base, which means, the other base was used to encode them. b is revealed.

[3] A tedious but straightforward calculation shows that we can restrict ourselves to real-valued α, β pairs only (thanks to I. Armendariz at NYU).

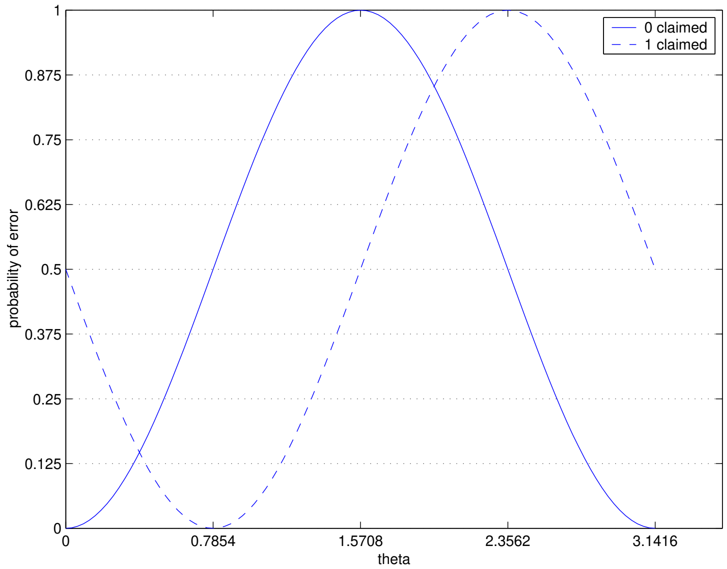

Figure 2: Alice's chances of being caught, per qubit sent.

5 The EPR paradox steps in or, the quantum daemon bites its own tail.

The famous EPR (Einstein-Podolsky-Rosen) paradox describes a rather counterintuitive quality of quantum physics: the quantum state space of a set of several particles is the direct product of their individual spaces, and not the direct sum as one would expect. As a consequence, if A and B have separate particles a and b, which happen to be in an *entangled* state, then A may be able to gain information on B's measurement of b by measuring a.

It is possible for A to exploit this in order to cheat. Here's A's cheating scheme:

- EPR cheating scheme for BB84

1. Commitment Phase

    - A fabricates s pairs of entangled qubits $\frac{1}{\sqrt{2}}\left|\rightarrow\rightarrow\right\rangle + \frac{1}{\sqrt{2}}\left|\uparrow\uparrow\right\rangle$ and sends one particle in the pair to B while keeping the other.

2. Disclosure Phase

- A measures her own qubits with respect to basis $\{\rightarrow, \uparrow\}$ if she wants to disclose a zero and $\{\nearrow, \nwarrow\}$ if she wants to disclose a one. She sends the "disclosed" bit along with the results $\{\widetilde{b_i}\}$ of her measurements.

A measurement collapses the state of a quantum system into the subspace that is compatible with the value obtained. A exploits the fact that the state $\frac{1}{\sqrt{2}}|\rightarrow\rightarrow\rangle + \frac{1}{\sqrt{2}}|\uparrow\uparrow\rangle = \frac{1}{\sqrt{2}}|\nearrow\nearrow\rangle + \frac{1}{\sqrt{2}}|\nwarrow\nwarrow\rangle$ is fully entangled with respect to both bases.

When Alice measures her qubit with respect to the horizontal basis, she gets either a zero or a one with 50% chance. However, this projects the entire state space of the entangled pair to either $|\rightarrow\rightarrow\rangle$ or $|\uparrow\uparrow\rangle$ (since the $|\rightarrow\uparrow\rangle$ and $|\uparrow\rightarrow\rangle$ components are zero from the start), which means that Bob will obtain the same result[4]. This is exactly the EPR paradox (table 4).

Table 4: Alice cheats on BB84

qubit pair	A's basis	$\widetilde{b_i}$	new state	$b_i\prime$	$B's$ basis	P(0)	P(1)
$\frac{1}{\sqrt{2}}|\rightarrow\rightarrow\rangle$	$\{\rightarrow, \uparrow\}$	0	$|\rightarrow\rightarrow\rangle$	0	$\{\rightarrow, \uparrow\}$	1	0
$+$				1	$\{\nearrow\nwarrow\}$	$\frac{1}{2}$	$\frac{1}{2}$
$\frac{1}{\sqrt{2}}|\uparrow\uparrow\rangle$	$\{\rightarrow, \uparrow\}$	1	$|\uparrow\uparrow\rangle$	0	$\{\rightarrow, \uparrow\}$	0	1
$=$				1	$\{\nearrow\nwarrow\}$	$\frac{1}{2}$	$\frac{1}{2}$
$\frac{1}{\sqrt{2}}|\nearrow\nearrow\rangle$	$\{\nearrow, \nwarrow\}$	0	$|\nearrow\nearrow\rangle$	0	$\{\rightarrow, \uparrow\}$	$\frac{1}{2}$	$\frac{1}{2}$
$+$				1	$\{\nearrow\nwarrow\}$	1	0
$\frac{1}{\sqrt{2}}|\nwarrow\nwarrow\rangle$	$\{\nearrow, \nwarrow\}$	1	$|\nwarrow\nwarrow\rangle$	0	$\{\rightarrow, \uparrow\}$	$\frac{1}{2}$	$\frac{1}{2}$
				1	$\{\nearrow\nwarrow\}$	0	1

With this procedure Alice makes sure that whenever $\widetilde{b_i} = b_i$, Bob used the same basis to do his measurement, so he will get an identical result. And

[4]Quantum measurements are symmetric, so it is the same result if we think that Bob measured first.

in the opposite case, as the angle between state and basis is $\frac{\pi}{4}$, he obtains a 50%-50% distribution as expected.

6 Brassard, Crépeau, Jozsa, Langlois: The EPR problem is fixed (temporarily)

A number of papers were published that extended the original BB84 quantum bit commitment protocol. Brassard and Crepéau suggested in 1991 the following protocol to fix the problems with BB84 [4]:

- BC91 Protocol

1. Commitment Phase

   (a) Alice prepares s random bit strings, each one of length s. The parity of each bit string should be equal to the committed bit, b. Each string will be called $b_{i1}, \ldots, b_{is}$.

   (b) Alice encodes each b_{ij} with a random basis φ_{ij}, either $\{\rightarrow, \uparrow\}$ or $\{\nearrow, \nwarrow\}$, and sends to Bob. Bob measures each bit with respect to a randomly chosen basis θ_{ij} , either $\{\rightarrow, \uparrow\}$ or $\{\nearrow, \nwarrow\}$. The results of these measurements will be called $\overline{b_{ij}}$.

2. Disclosure Phase

   (a) Alice tells Bob what b was, and also sends all the values for $\{b_{i,j}\}$ and $\{\varphi_{i,j}\}$.

   (b) Bob verifies that

      i. The parity of all strings $b_{i,1}, \ldots, b_{i,s}$ is indeed b

      ii. Whenever it happened that $\varphi_{ij} = \theta_{ij}$, the value b_{ij} supposedly encoded is indeed equal to the observed $\overline{b_{ij}}$.

Brassard and Crépeau here thought that the EPR attack was nearly impossible in practice, and that they were offering this improved version just for the sake of completeness.

The rationale is that, unlike the earlier protocol, all bases and bits are random, b being encoded in the parity. Alice cannot guess what the decoding bases $\theta_{i,j}$ are, so, would she keep an entangled qubit for herself, measuring it with the wrong basis would yield a 50% probability of error. The authors claimed that this protocol was immune to the EPR attack but were not sure about a higher-scale consequence of quantum physics: "coherent measurements". Without explaining much, what they seem to fear is what ultimately would kill the whole enterprise, namely, that the same kind of phenomenon that enabled the EPR attack, the composite state of sets of two or more particles, applies to the composite state of all the particles involved in the protocol.

For a while, however, this was considered to be a sound protocol and the research focused on adding error correction to it, because actual physical quantum transmission channels were beginning to be built and all of them had error probabilities. In 1993 a paper by Brassard, Crépeau, Jozsa and Langlois appeared, pompously named "A Quantum Bit Commitment Scheme Provably Unbreakable by both Parties" [5] that explained in full detail an extension to BC91 incorporating error correction.

I won't describe BCJL93 in detail here because the error correction protocol makes equations difficult to follow. This paper contains a proof of security ([5], theorem 3.7) that turned out to be flawed. Crépeau made this comment three years later ([8], page 197):

> The part of the "proof" that goes wrong is the fact that A is committed to a bit. The paper shows that A is unable to know *at the same time* information to unveil the commitment as $b = 0$ and as $b = 1$ and concludes that 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!

7 The Quantum Computer bites the Quantum Cryptographer

Three years passed before Lo and Chau, and Mayers discovered the flaws of BCJL93, more or less simultaneously. The advances in quantum computing theory provided them with better formalisms on quantum physics and quantum computations and allowed them to frame the problem with a clearer perspective. Their papers were first published online ([16], [11]) and later appeared together on *Physical Review Letters* ([17], [12]). To prove that quantum bit commitment is impossible, a general structure or scheme of a QBC protocol is needed, encompassing all possible such protocols. The authors at the time had doubts on the generality of the ones they had used. Lo and Chau's 1998 article [13] and review [7] have definitively settled the issue.[5]

The general idea of a protocol involves three quantum systems, one for Alice, one for Bob, and one for a communications channel. According to quantum physics, the state of each one of these is a unitary[6] vector on a Hilbert[7] space, so we must consider state spaces H_A, H_B, and H_C for each of this characters. The complete state of all of them put together is a vector in the direct (tensor) product of the three, namely the space $H_A \otimes H_B \otimes H_C$. Note that in as much as quantum physics encompasses classical physics, this is also a description for any classical (or mixed) protocol. The protocol will require A and B to prepare and manipulate their states, which involves computing and storage. Once again, from the point of view of quantum

[5] Allah knows better.

[6] of norm one.

[7] Complex Euclidean vector space of finite or infinite dimension.

physics, the most general description of these are quantum computers. The assumption is, then, that A and B have a quantum computer each. With this gadgets they are able to perform manipulations on their state-spaces, namely, to rotate the state by any unitary transformation[8].

- LC98 general Quantum Bit Commitment protocol

1. Preparation of states.

   (a) Alice chooses b. She sets H_A to one of two states specified by the protocol. Call them $|0\rangle$ and $|1\rangle$. Thus Alice sets H_A to $|A_{initial}\rangle$ which is either $|0\rangle$ or $|1\rangle$.

   (b) Bob sets the initial states of both the communications channel and his side of the protocol. These initial states will be called $|C_{initial}\rangle$ and $|B_{initial}\rangle$, respectively. So $H_B \otimes H_C = H_{BC}$ is set to state $|B_{initial}\rangle \otimes |C_{initial}\rangle = |BC_{initial}\rangle$.

   (c) $|0\rangle$, $|1\rangle$ and $|BC_{initial}\rangle$ are all specified by the protocol and known to both parties.

2. Commitment.

   (a) Here Alice and Bob execute a commitment protocol. Each one of them, in turn, perform a unitary transformation involving their side and the communications channel. So Alice "sees" $H_A \otimes H_C$ whereas Bob acts on $H_B \otimes H_C$. Each of these operations, of course, result in a unitary transformation of the whole state $H_{ABC} = H_A \otimes H_B \otimes H_C$.

[8] A unitary transformation is one that preserves orthogonality and norm, such as a rotation for example. Quantum physics states that the evolution of quantum states occurs only by unitary operations. The quantum computing formalism indicates that: (1) Any unitary transformation can in principle be built (from elementary quantum gates) and (2) any classical computation or algorithm can be "compiled" into a quantum operation, replacing boolean gates with quantum gates.

If we label this transformations U_{A_1}, U_{B_1}, ... ,U_{A_n}, U_{B_n} we conclude that the final state is[9]

$$\begin{aligned} |ABC_{final}\rangle &= U_{A_n}U_{B_n}\cdots U_{A_1}U_{B_1}\left(|A_{initial}\rangle \otimes |BC_{initial}\rangle\right) \\ &= U\,|A_{initial}\rangle \otimes |BC_{initial}\rangle \\ &= \begin{cases} |0_{final}\rangle = U\,|0\rangle \otimes |BC_{initial}\rangle & (b=0) \\ |1_{final}\rangle = U\,|1\rangle \otimes |BC_{initial}\rangle & (b=1) \end{cases} \end{aligned}$$

3. Disclosure

   (a) Alice sends Bob all her quantum particles and Bob takes a measurement on the composite system which convinces him of what the commitment was.

After the commitment phase, the entire system is in one of two states: Either the state originating from an initial $b = 0$, which will be called $|0_{final}\rangle$ or the one generated from $b = 1$, namely, $|1_{final}\rangle$. Since all the protocol is known to both parties, they both know the entire matrix U of the whole computation process, the only difference being that B ignores what the initial state of H_A was.

The key element at this point is that B must get no information whatsoever on what the value of b is. So both states $|0_{final}\rangle$ and $|1_{final}\rangle$ must look identical from *his* point of view. This said in mathematical terms, the trace with respect to H_A of the observable associated with $|0_{final}\rangle$ is identical to that of $|1_{final}\rangle$. We do this with a tool called Schmidt decomposition[7]: there are bases $\{e_i\}$ of H_A and $\{\phi_i\}$ of H_{BC} , and numbers $\{\alpha_i\}$ such that

$$|0_{final}\rangle = \sum \sqrt{\alpha_i}\,|e_i\rangle \otimes |\phi_i\rangle$$

and the trace taken to bring the observable $|0_{final}\rangle\langle 0_{final}|$ down to H_{BC}

[9] In fact, A applies a smaller $\widetilde{U}_{A_i}$, a transformation of H_{AC}, and the bigger state space is modified by $U_{A_i} = \widetilde{U}_{A_i} \otimes I_B$, ($I_B$ being the identity over H_B)

yields[10]

$$Tr_{H_A}\left(|0_{final}\rangle\langle 0_{final}|\right) = \sum \alpha_i |\phi_i\rangle\langle\phi_i|$$

Similarly, there are bases $\{e_{i'}\}$ of H_A and $\{\phi_{i'}\}$ of H_{BC}, and scalars $\{\beta_i\}$ such that

$$|1_{final}\rangle = \sum \sqrt{\beta_i}\, |e_{i'}\rangle \otimes |\phi_{i'}\rangle$$

and

$$Tr_{H_A}\left(|1_{final}\rangle\langle 1_{final}|\right) = \sum \beta_i |\phi_{i'}\rangle\langle\phi_{i'}|$$

But since B cannot tell between each other, it must be the case that for all i, $\alpha_i = \beta_i$ and $\phi_i = \phi_{i'}$. The only difference between the states lies inside H_A which means now that A can manipulate it at will! This is the problem that ruins the whole setup. Alice does not need to have access to H_{BC} in order to cheat. Here's what she should do:

- Alice cheats with a quantum computer

1. Prepare $|0\rangle$ as if she were committing to the bit 0.
2. Go over the protocol with B.
3. When the time comes to open the commitment, if she wishes it to be zero, does nothing. Otherwise uses her quantum computer to apply the basis change operator $C(\{e_i\}, \{e_{i'}\})$ on H_A. Now when B does his measurement, the state is $|1_{final}\rangle$ and he is convinced that Alice was committed to 1 all along.

Perhaps all this quantum mathematical symbols were not even necessary. Suffice to say that, according to quantum mechanics, and according to May-

[10] This is the definition of the Schmidt decomposition.

ers, Lo and Chau, the two requirements for a bit commitment, which are that Bob cannot get early information, and that Alice can't cheat, are mutually exclusive because both "committed" states must be identical from Bob's point of view, so if Alice has the means, such as quantum storage and quantum computers, she can modify things up to the last minute.

8 Aftermath

I have just sketched the protocols without error correction and in the "ideal" case where the information content for Bob is exactly zero. There are extended versions to these proofs that incorporate error correction, probabilistic commitment algorithms and non-zero information.

Since Bit Commitment is a possible foundation upon which other protocols such as coin tossing or two-party computation can be built, those latter protocols are weaker in some sense. The impossibility of BC does not mean that they cannot be secure. However, the same methods of attack can deal with some of them. Other "no-go" theorems been proved, such as (ideal) coin tossing, and some kinds of two-party computation[13].

Although defeated, Brassard, Crépeau and the other "quantum cryptographers" should not be forgotten. Alice's cheating scheme relies upon a machinery for quantum computation and storage that is way beyond the current technology, which is not the case for quantum communication protocols. One could, implement BCJL93 [5] — QBC with error correction — with today's technology, for a very secure bit commitment protocol.

Quantum key distribution, on the other hand, does not suffer from this problem, and Lo and Chau themselves have a recent paper proving its "unconditional security"[14].

It is still disappointing that QBC seems to have been unable to go beyond what was already given by classic BC: Once the quantum computer becomes available, factoring large numbers becomes a possibility, and classical encryption dies. Here quantum cryptography can come to the rescue and restore security. But for "post cold war cryptography", the same quantum computer that burns factorization-based protocols, could also crack their quantum counterpart. One difference is that all the information can be kept on the classical version, so if sometime in the future we get our hands on a quantum computer, we will be able to go backwards in time, opening all communications ever received. Quantum protocols do not have this "retroactive" deciphering problem.

References

[1] Bennett, C.H. and Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing.* IEEE, New York. pp. 175-179 (1984).

[2] Bennet, C.H. and Shor, P.W. Privacy in a Quantum World. *Science* **284**. pp. 747-748 (30 April 1999)

[3] Bernstein, E. and Vazirani, U. Quantum Complexity Theory. *Proceedings of the 25th CDM Symposium on the Theory of Computation.* pp. 11-20 (1993).

[4] Brassard, G. and Crépeau, C. Quantum Bit Commitment and Coin Tossing Protocols. *Advances in Cryptology: Proceedings of Crypto '90.* Lecture Notes in Computer Science, Vol. 537. Springer-Verlag. pp. 49-61 (1991).

[5] Brassard, G. Crépeau, C., Jozsa, R. and Langlois, D. A Quantum Bit Commitment Scheme Provably Unbreakable by Both Parties. *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science.* IEEE press. pp. 362-371 (1993).

[6] Buttler, W.T., Hughes, R.J., Kwiat, P.G., Lamoreaux, S.K., Luther, G.G., Morgan, G.L., Nordholt, J.E., Peterson, C.G. and Simmons, C.M. Practical Free-Space Quantum Key Distribution over 1 km. *Physical Review Letters* **81**, pp. 3283-3286 (1998).

[7] Chau, H.F. and Lo, H.K. Making an Empty Promise with a Quantum Computer. *Fortschritte der Physik* **46**, 4-5 . pp. 507-519 (1998).

[8] Crépeau, C. What is going on with Quantum Bit Commitment?. *Proceedings of Pragocrypt '96*, Czech Technical University Publishing House, Prague. pp. 193-203 (1996).

[9] Deutsch, D. Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. *Proceedings of the Royal Society of London* **A400** . pp. 96-117 (1985).

[10] Kilian, J. Founding Cryptography on Oblivious Transfer. Proceedings of the 1998 ACM Annual Symposium on Theory of Computing. pp20-31 (1998).

[11] Lo, H.K. and Chau, H.F. Is Quantum Bit Commitment Really Possible?, Los Alamos preprint archive, xxx.lanl.gov/abs/quant-ph/9603004 (1996).

[12] Lo, H.K. and Chau, H.F. Is Quantum Bit Commitment Really Possible? *Physical Review Letters* **78** . pp 3410-3413 (28 April 1997)

[13] Lo, H.K. and Chau, H.F. Why Quantum Bit Commitment and Ideal Quantum Coin Tossing are Impossible. *Physica D* **120** pp. 177-187 (1998).

[14] Lo, H.K. and Chau, H.F. Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. *Science* **283**. pp. 2050-2056 (26 March 1999).

[15] Makhlin, Y. Schön, G. and Shnirman, A. Josephson-junction qubits with controlled couplings. *Nature* **398**, pp. 305-307 (25 March 1999).

[16] Mayers, D. The Trouble with Quantum Bit Commitment, Los Alamos preprint archive, xxx.lanl.gov/abs/quant-ph/9603015. (1996).

[17] Mayers, D. Unconditionally Secure Quantum Bit Commitment is Impossible. *Physical Review Letters* **78** . pp 3414-3417 (28 April 1997).

[18] Ribordy, G. Gautier, J.D., Gisin, N. Guinnard, O. Zbinden, H. Automated "plug & play" Quantum Key Distribution. *Electronics Letters* **34** (22), pp 2116-2117 (1998).

[19] Shor, P.W. Algorithms for Quantum Computation: Discrete Log and Factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science.* IEEE press. pp. 124-134 (1994).

[20] Yao, A.C. Security of quantum protocols against coherent measurements. *Proceedings of the 1995 ACM Symposium on Theory of Computing.* pp. 67-75 (1995).