Quantum Bit Commitment and Coin Tossing Protocols

Gilles Brassard *

Département d'informatique et de R.O.
Université de Montréal
C.P. 6128 succ. "A"
Montréal, Québec CANADA H3C 3J7

Claude Crépeau †

Laboratoire de Recherche en Informatique
Université de Paris-Sud
Bâtiment 490
91405 Orsay FRANCE

1 Introduction

In the late 1960's a physicist, Stephen Wiesner, had the idea that the uncertainty principle could be used for cryptography (though he published his result much later [Wie83]). His idea was that it would be possible to transmit the values of two pieces of information using beams of photons in a way that would make only one of them readable at the receiver's choosing. This notion, which he called "multiplexing" is remarkably similar to the "one-out-of-two Oblivious Transfer" to be reinvented many years later [EGL83]. A decade after his original invention, Charles H. Bennett and Gilles Brassard brought Wiesner's idea back to life in a CRYPTO '82 talk. Subsequently, they used quantum cryptographic principles to implement basic cryptographic protocols, such as secret key exchange and coin flipping by telephone [BB84]. There has been very recently renewed interest in quantum cryptography because a working prototype of the quantum key exchange channel has been successfully built at the IBM T. J. Watson Research Laboratory, Yorktown Heights [BBBSS90].

In recent times, the importance of cryptographic primitives has been brought to light by the work of many researchers whose goal is to characterize precisely the primitives sufficient for the implementation of various cryptographic protocols. One of these primitives is a Bit Commitment Scheme. The importance and usefulness of such a primitive is enlightened by the work of [GMW86,BCC88] to mention just a few.

While such primitives are usually built under computational complexity assumptions, it is sometimes possible to build such things based on assumptions of a different nature as pointed out by the work mentioned earlier of [Wie83,BB84]. The current paper presents the state-of-the-art in the technology of building a bit commitment scheme on a quantum mechanical assumption. The applications are numerous, including secure two-party computation.

*Supported in part by Canada NSERC grant A4107.

†Supported in part by NSERC Postgraduate and Postdoctorate Scholarships. This research was performed in part while the author was a graduate student at M.I.T. and while visiting the IBM Almaden Research Center.

Figure 1: The behaviour of a photon passing through a Wallaston prism

2 Physics background

For a complete coverage of the physics of quantum cryptography, please consult [BB84]. The linear polarization of photons is a quantum state. In general, the value of this variable cannot be determined exactly. According to quantum mechanics, although the value of the polarization can be any angle in the (real) interval $[0^\circ, 180^\circ)$, only a boolean (two states) predicate can be measured about this variable. Moreover, only one such measurement can be performed on any given photon because the measurement itself necessarily destroys the information. For instance, let Θ be the polarization of a photon. Assuming that it is known *a priori* that Θ is either 0° or 90°, the predicate "Is $\Theta = 0^\circ$?" can be measured accurately for these two quantum states. On the other hand, even if Θ is known to be either 0° or 45°, then no measuring apparatus can distinguish between these two states with certainty, although some probabilistic information can be obtained. If we have no constrain on the set of possible values for Θ then answering "Is $\Theta = 0^\circ$?" will result in a probabilistic answer determined by the value of Θ: it will always be "yes" if $\Theta = 0^\circ$, otherwise it will be "no" with a probability that ranges from 0 to 1 as Θ ranges from 0° to 90°.

It is not a matter of technology, it is not that no one has a good enough device to figure out Θ; quantum theory claims that it is **impossible** to determine this value with certainty. In a sense, the value does not really exist: it is just a probability distribution.

However, it *is* possible to build a device that always says "yes" if $\Theta = 0^\circ$ and always says "no" when $\Theta = 90^\circ$. In general, with such a device, $\text{Prob}(\text{device says "yes"} | \Theta) = \cos^2(\Theta)$. This can be obtained by combining a Wallaston prism with two photomultipliers (photon detectors). See figure 1. Consider a Wallaston prism set for distinguishing polarization angles φ from $\varphi + 90^\circ$. A photon polarized at angle Θ will come out of this Wallaston prism on the right side with probability $\cos^2(\Theta - \varphi)$ (and will then be repolarized at angle φ) and on the left side with complement probability $\sin^2(\Theta - \varphi)$ (and will then be repolarized at angle $\varphi + 90^\circ$). According to quantum mechanics, this device is the best that can be built with respect to measuring Θ.

3 Review of earlier quantum protocols

3.1 A bit commitment scheme

Consider two parties: $\mathcal{S}$ and $\mathcal{R}$. Assume that $\mathcal{S}$ has a bit b in mind, to which she would like to be committed toward $\mathcal{R}$. That is, $\mathcal{S}$ wishes to provide $\mathcal{R}$ with a piece of evidence that she has a bit in mind and that she cannot change it. Meanwhile, $\mathcal{R}$ should not be able to tell from that evidence what b is.

The first quantum bit commitment scheme ever proposed is due to Bennett and Brassard [BB84] (actually, the protocol they describe is only claimed to implement coin tossing, but it is obvious how to modify it in order to implement bit commitment). Let us briefly review this protocol and its main weakness before describing our new scheme in Section 4. Assume that $\mathcal{S}$ wishes to commit to bit b toward $\mathcal{R}$. Let s be a security parameter.

Protocol 3.1 (BB-commit(b))

1: $\mathcal{S}$ chooses a vector $B = (b_1, b_2, \ldots, b_s)$ of s random bits

2: $\mathcal{R}$ chooses a vector $\Theta = (\varphi_1, \varphi_2, \ldots, \varphi_s)$ of s random $\varphi_i \in \{0°, 45°\}$

3: $\mathop{\mathbf{DO}}\limits_{i=1}^{s}$ $\mathcal{S}$ sends a photon with polarization $b \times 45° + b_i \times 90°$ that $\mathcal{R}$ reads at angle φ_i.

$\mathcal{R}$ sets $b'_i \leftarrow \begin{cases} 0 & \text{if photon came out on the right} \\ 1 & \text{if photon came out on the left} \end{cases}$

4: $\mathcal{R}$ keeps Θ and $B' = (b'_1, b'_2, \ldots, b'_s)$ secret

5: $\mathcal{S}$ keeps b and B secret until (and if) decommittal

Notice that since b_i is chosen at random, the received bit b'_i reveals no information about b. Therefore receiving $B' = (b'_1, b'_2, \ldots, b'_s)$ reveals nothing about b. In fact, a much stronger statement can be proved: quantum mechanics tells us that *no* measuring apparatus can distinguish a commitment to 0 from a commitment to 1 unless it is possible to communicate information faster than the speed of light. But why is $\mathcal{S}$ committed?

To open her commitment, $\mathcal{S}$ initiates the following protocol with $\mathcal{R}$.

Protocol 3.2 (BB-decommit($(B, b), (B', \Theta)$))

1: $\mathcal{S}$ reveals b and B to $\mathcal{R}$

2: $\mathop{\mathbf{DO}}\limits_{i=1}^{s}$ $\mathcal{R}$ checks that $b'_i = b_i$ whenever $\varphi_i = b \times 45°$

3: **if** this condition is satisfied for all i **then** $\mathcal{R}$ outputs "accept" **else** $\mathcal{R}$ outputs "reject"

First note that if $\mathcal{S}$ is honest then the condition is always satisfied. Now suppose that a cheating $\mathcal{S}$ tries to "commit" in a way that will enable her to open B as b or $\bar{b}$ at her later choice. In order to achieve this, she must find two strings B^0 and B^1 such that B^b satisfies the condition above when trying to open as $b \in \{0, 1\}$. This implies that $b^0_i = b'_i$ whenever $\varphi_i = 0°$ and that $b^1_i = b'_i$ whenever $\varphi_i = 45°$.

When both $\mathcal{S}$ and $\mathcal{R}$ are honest, $\mathcal{S}$ knows that $\text{Prob}(b_i = b'_i) = \frac{3}{4}$. When only $\mathcal{R}$ is honest, the maximum information that $\mathcal{S}$ may get about each b'_i is by sending her bits b_i using angle $22\frac{1}{2}° + b_i \times 90°$, which gives her $\text{Prob}(b_i = b'_i) = \cos^2(22\frac{1}{2}°) \approx 85\%$ (it is an easy exercise to figure out that this is $\mathcal{S}$'s optimal strategy). Still, $\mathcal{S}$ will always have a probability of $\sin^2(22\frac{1}{2}°) \approx 15\%$

of guessing b'_i incorrectly.

Now for all the indices i where $b_i^0 = b_i^1$, $\mathcal{S}$ has at least probability $\sin^2(22\frac{1}{2}^\circ)$ that $b_i^0 \neq b'_i$ and $b_i^1 \neq b'_i$. When $b_i^0 \neq b_i^1$ it is even worse since one of b_i^0 or b_i^1 is necessarily wrong. Because $\mathcal{S}$ has no information about φ_i, she has no information about which of b_i^0 or b_i^1 she should set as 0 or 1. Therefore her probability of failure in this second case is $\frac{1}{2}$. We conclude that the probability of success that $\mathcal{S}$ builds such B_0 and B_1 is at most $(\cos^2(22\frac{1}{2}^\circ))^s$.

3.2 Coin tossing

Bennett and Brassard used this bit commitment scheme in order to implement a protocol for coin tossing by (quantum!) "telephone" [Blu81] as follows:

Protocol 3.3 (BB-cointoss)

1: $\mathcal{S}$ chooses a random bit b_0 and uses BB-commit(b_0) with $\mathcal{R}$

2: $\mathcal{R}$ chooses a random bit b_1 and sends it to $\mathcal{S}$

3: $\mathcal{S}$ runs BB-decommit(b_0) with $\mathcal{R}$

4: $\mathcal{R}$ wins the coin toss if and only if $b_1 = b_0$

The resulting protocol can be broken exactly if the bit commitment scheme can be broken.

3.3 The problem of dependence

As mentioned in [BB84] the bit commitment scheme of section 3.1 and the resulting coin tossing protocol can be defeated in theory using the consequences of the Einstein-Podolsky-Rosen "paradox". The interested reader can consult their paper for a more detailed explanation. We call this problem "dependence" because E-P-R is based on the fact that it is possible to create pairs of photons with a dependence relation between their polarizations (it is possible to have some correlation between measurements). In practice, this kind of attack is rather improbable because the technology necessary to perform it is far beyond the current available technology, and because even a small failure in the cheater's technology will result in loss of his possibility of cheating. Nevertheless, from a theoretical point of view, it is important to get around this difficulty.

In the next section we offer our new bit commitment scheme, which cannot be broken through E-P-R.

4 A new bit commitment scheme

4.1 How to commit

In order to commit to a bit b, $\mathcal{S}$ builds a random $s \times s$ boolean matrix:

$$B = \begin{pmatrix} b_{1,1} & \dots & b_{1,s} \\ \vdots & \ddots & \vdots \\ b_{s,1} & \dots & b_{s,s} \end{pmatrix} \tag{1}$$

with the following property:

$$\forall 1 \le i \le s \ [\bigoplus_{j=1}^{s} b_{i,j} = b] \tag{2}$$

and sends it to $\mathcal{R}$ using the following protocol.

Protocol 4.1 (BC-commit(b))

1: $\mathcal{S}$ builds a random $s \times s$ boolean matrix B as indicated above

2: $\mathop{\mathbf{DO}}_{i=1}^{s}\mathop{\mathbf{DO}}_{j=1}^{s}$ $\mathcal{S}$ chooses a random $\varphi_{i,j} \in \{0°, 45°\}$ and $\mathcal{R}$ chooses a random $\varphi_{i,j} \in \{0°, 45°\}$

3: $\mathop{\mathbf{DO}}_{i=1}^{s}\mathop{\mathbf{DO}}_{j=1}^{s}$ $\mathcal{S}$ sends a photon with polarization $\varphi_{i,j} + b_{i,j} \times 90°$ that $\mathcal{R}$ reads at angle $\varphi_{i,j}$.

$\mathcal{R}$ sets $b'_{i,j} \leftarrow \begin{cases} 0 & \text{if photon came out on the right} \\ 1 & \text{if photon came out on the left} \end{cases}$

4: $\mathcal{R}$ keeps B' and Θ (see below) secret

5: $\mathcal{S}$ keeps b, B and Φ (see below) secret until (and if) decommittal

where

$$B' = \begin{pmatrix} b'_{1,1} & \dots & b'_{1,s} \\ \vdots & \ddots & \vdots \\ b'_{s,1} & \dots & b'_{s,s} \end{pmatrix}, \Theta = \begin{pmatrix} \theta_{1,1} & \dots & \theta_{1,s} \\ \vdots & \ddots & \vdots \\ \theta_{s,1} & \dots & \theta_{s,s} \end{pmatrix}, \Phi = \begin{pmatrix} \varphi_{1,1} & \dots & \varphi_{1,s} \\ \vdots & \ddots & \vdots \\ \varphi_{s,1} & \dots & \varphi_{s,s} \end{pmatrix} \tag{3}$$

If both participants are honest, B' is such that

$$\forall 1 \le i \le s, 1 \le j \le s \ [\text{Prob}(b_{i,j} = b'_{i,j}) = \frac{3}{4}] \tag{4}$$

However, if $\mathcal{R}$ uses angle $\varphi_{i,j} = 22\frac{1}{2}°$ he will end up getting maximum information about B. That is $\forall 1 \le i \le s, 1 \le j \le s$ $[\text{Prob}(b_{i,j} = b'_{i,j}) = \cos^2(22\frac{1}{2}°)]$. Nevertheless, even then the matrix B' reveals very little about b. We measure this fact by computing $\text{Prob}(b = 0|B')$ and $\text{Prob}(b = 1|B')$ for every possible B'. We are satisfied if there exists a positive constant $\alpha < 1$ such that

$$|\text{Prob}(b = 0|B') - \text{Prob}(b = 1|B')| \le \alpha^s$$

for every B'. Since $\text{Prob}(b = 0|B') + \text{Prob}(b = 1|B') = 1$, the following condition is sufficient for this result:

Theorem 4.1 *There exists a positive constant $\alpha < 1$ such that*

$$\frac{1}{2} - \alpha^s \le \text{Prob}(b = 0|B') \le \frac{1}{2} + \alpha^s$$

Proof.

Provided in the journal version of the paper. □

Lemma 4.2 $\frac{1}{2} - s(2p-1)^s \leq \text{Prob}(b|B') \leq \frac{1}{2} + s(2p-1)^s$

Proof. Let B_i and B'_i be the i^{th} line of B and B'. Let $b_i = \bigoplus_{j=1}^{s} b_{i,j}$ and define b'_i similarly.

$$\begin{aligned}
\text{Prob}(b|B') &= \frac{\text{Prob}(B'|b)\text{Prob}(b)}{\text{Prob}(B')} && (5)\\
&= \frac{\text{Prob}(B'|b)\text{Prob}(b)}{\text{Prob}(b)\text{Prob}(B'|b) + \text{Prob}(\bar{b})\text{Prob}(B'|\bar{b})} && (6)\\
&= \frac{\text{Prob}(B'|b)}{\text{Prob}(B'|b) + \text{Prob}(B'|\bar{b})} && (7)\\
&\text{since } \text{Prob}(b) = \text{Prob}(\bar{b}) = \frac{1}{2} \\
&= \frac{1}{1 + \frac{\text{Prob}(B'|\bar{b})}{\text{Prob}(B'|b)}} && (8)
\end{aligned}$$

Now we focus our attention on this ratio:

$$\begin{aligned}
\frac{\text{Prob}(B'|\bar{b})}{\text{Prob}(B'|b)} &= \frac{\text{Prob}(B' \wedge \bar{b})}{\text{Prob}(B' \wedge b)} && (9)\\
&= \frac{\sum_B \text{Prob}(B' \wedge B \wedge \bar{b})}{\sum_B \text{Prob}(B' \wedge B \wedge b)} && (10)\\
&= \frac{\sum_{B|b_1=b_2=\ldots=b_s=\bar{b}} \text{Prob}(B' \wedge B)}{\sum_{B|b_1=b_2=\ldots=b_s=b} \text{Prob}(B' \wedge B)} && (11)\\
&= \frac{\sum_{B_i|b_i=\bar{b},1\leq i\leq s} \text{Prob}(B'_1 \wedge B_1 \wedge \ldots \wedge B'_s \wedge B_s)}{\sum_{B_i|b_i=b,1\leq i\leq s} \text{Prob}(B'_1 \wedge B_1 \wedge \ldots \wedge B'_s \wedge B_s)} && (12)\\
&= \frac{\sum_{B_i|b_i=\bar{b},1\leq i\leq s} \text{Prob}(B'_1 \wedge B_1)\ldots\text{Prob}(B'_s \wedge B_s)}{\sum_{B_i|b_i=b,1\leq i\leq s} \text{Prob}(B'_1 \wedge B_1)\ldots\text{Prob}(B'_s \wedge B_s)} && (13)\\
&\text{since these events are all independent} \\
&= \prod_{i=1}^{s} \frac{\sum_{B_i|b_i=\bar{b}} \text{Prob}(B'_i \wedge B_i)}{\sum_{B_i|b_i=b} \text{Prob}(B'_i \wedge B_i)} && (14)\\
&= \prod_{i=1}^{s} \frac{\sum_{B_i|b_i=\bar{b}} \text{Prob}(B'_i|B_i)}{\sum_{B_i|b_i=b} \text{Prob}(B'_i|B_i)} && (15)
\end{aligned}$$

but this ratio is

$$\frac{\sum_{B_i|b_i=\bar{b}} \mathrm{Prob}(B_i'|B_i)}{\sum_{B_i|b_i=b} \mathrm{Prob}(B_i'|B_i)} = \begin{cases} \frac{\mathrm{Prob}(\text{an even number of errors occurred})}{\mathrm{Prob}(\text{an odd number of errors occurred})} & \text{if } b_i' = \bar{b} \\ \\ \frac{\mathrm{Prob}(\text{an odd number of errors occurred})}{\mathrm{Prob}(\text{an even number of errors occurred})} & \text{if } b_i' = b \end{cases} \tag{16}$$

$$= \left(\frac{\mathrm{Prob}(\text{an odd number of errors occurred})}{\mathrm{Prob}(\text{an even number of errors occurred})}\right)^{(-1)^{b_i'\oplus b}} \tag{17}$$

$$= \left(\frac{\sum_{j=0}^{\lfloor\frac{s-1}{2}\rfloor} \binom{s}{2j+1} p^{s-2j-1}(1-p)^{2j+1}}{\sum_{j=0}^{\lfloor\frac{s}{2}\rfloor} \binom{s}{2j} p^{s-2j}(1-p)^{2j}}\right)^{(-1)^{b_i'\oplus b}} \tag{18}$$

Now notice that

$$\sum_{j=0}^{\lfloor\frac{s}{2}\rfloor} \binom{s}{2j} p^{s-2j}(1-p)^{2j} + \sum_{j=0}^{\lfloor\frac{s-1}{2}\rfloor} \binom{s}{2j+1} p^{s-2j-1}(1-p)^{2j+1} \tag{19}$$

$$= \sum_{j=0}^{s} \binom{s}{j} p^{s-j}(1-p)^{j} \tag{20}$$

$$= 1 \tag{21}$$

and

$$\sum_{j=0}^{\lfloor\frac{s}{2}\rfloor} \binom{s}{2j} p^{s-2j}(1-p)^{2j} - \sum_{j=0}^{\lfloor\frac{s-1}{2}\rfloor} \binom{s}{2j+1} p^{s-2j-1}(1-p)^{2j+1} \tag{22}$$

$$= \sum_{j=0}^{s} \binom{s}{j} p^{s-j}(p-1)^{j} \tag{23}$$

$$= (2p-1)^s \tag{24}$$

therefore we get by adding these two equations

$$\sum_{j=0}^{\lfloor\frac{s-1}{2}\rfloor} \binom{s}{2j+1} p^{s-2j-1}(1-p)^{2j+1} = \frac{1-(2p-1)^s}{2} \tag{25}$$

$$\sum_{j=0}^{\lfloor\frac{s}{2}\rfloor} \binom{s}{2j} p^{s-2j}(1-p)^{2j} = \frac{1+(2p-1)^s}{2} \tag{26}$$

returning to equation 18 we get

$$\frac{\sum_{B_i|b_i=\bar{b}} \mathrm{Prob}(B_i'|B_i)}{\sum_{B_i|b_i=b} \mathrm{Prob}(B_i'|B_i)} = \left(\frac{1-(2p-1)^s}{1+(2p-1)^s}\right)^{(-1)^{b_i'\oplus b}} \tag{27}$$

using equation 15 and defining for simplicity $\varepsilon = \frac{(2p-1)^s}{2}$.

$$\begin{aligned}\frac{\mathrm{Prob}(B'|\bar{b})}{\mathrm{Prob}(B'|b)} &= \prod_{i=1}^{s}\left(\frac{1-2\varepsilon}{1+2\varepsilon}\right)^{(-1)^{b'_i\oplus b}} & (28)\\ &= \left(\frac{1-2\varepsilon}{1+2\varepsilon}\right)^{\sum_{i=1}^{s}(-1)^{b'_i\oplus b}} & (29)\end{aligned}$$

Now, we bound this ratio in the following way

$$\begin{aligned}
\left(\frac{1-2\varepsilon}{1+2\varepsilon}\right)^{s} &\leq \frac{\mathrm{Prob}(B'|\bar{b})}{\mathrm{Prob}(B'|b)} \leq \left(\frac{1-2\varepsilon}{1+2\varepsilon}\right)^{-s} & (30)\\
\left(\frac{1-2\varepsilon}{1+2\varepsilon}\right)^{s} &\leq \frac{\mathrm{Prob}(B'|\bar{b})}{\mathrm{Prob}(B'|b)} \leq \left(\frac{1+2\varepsilon}{1-2\varepsilon}\right)^{s} & (31)\\
\left(1-\frac{4\varepsilon}{1+2\varepsilon}\right)^{s} &\leq \frac{\mathrm{Prob}(B'|\bar{b})}{\mathrm{Prob}(B'|b)} \leq \left(1+\frac{4\varepsilon}{1-2\varepsilon}\right)^{s} & (32)\\
\sum_{i=0}^{s}\binom{s}{i}\left(\frac{-4\varepsilon}{1+2\varepsilon}\right)^{i} &\leq \frac{\mathrm{Prob}(B'|\bar{b})}{\mathrm{Prob}(B'|b)} \leq \sum_{i=0}^{s}\binom{s}{i}\left(\frac{4\varepsilon}{1-2\varepsilon}\right)^{i} & (33)\\
1-\sum_{i=1}^{s}\binom{s}{i}\left(\frac{4\varepsilon}{1+2\varepsilon}\right)^{i} &\leq \frac{\mathrm{Prob}(B'|\bar{b})}{\mathrm{Prob}(B'|b)} \leq 1+\sum_{i=1}^{s}\binom{s}{i}\left(\frac{4\varepsilon}{1-2\varepsilon}\right)^{i} & (34)\\
1-\sum_{i=1}^{s}\left(\frac{4s\varepsilon}{1+2\varepsilon}\right)^{i} &\leq \frac{\mathrm{Prob}(B'|\bar{b})}{\mathrm{Prob}(B'|b)} \leq 1+\sum_{i=1}^{s}\left(\frac{4s\varepsilon}{1-2\varepsilon}\right)^{i} & (35)\\
1-\sum_{i=1}^{\infty}\left(\frac{4s\varepsilon}{1+2\varepsilon}\right)^{i} &\leq \frac{\mathrm{Prob}(B'|\bar{b})}{\mathrm{Prob}(B'|b)} \leq 1+\sum_{i=1}^{\infty}\left(\frac{4s\varepsilon}{1-2\varepsilon}\right)^{i} & (36)\\
1-\frac{\frac{4s\varepsilon}{1+2\varepsilon}}{1-\frac{4s\varepsilon}{1+2\varepsilon}} &\leq \frac{\mathrm{Prob}(B'|\bar{b})}{\mathrm{Prob}(B'|b)} \leq 1+\frac{\frac{4s\varepsilon}{1-2\varepsilon}}{1-\frac{4s\varepsilon}{1-2\varepsilon}} & (37)
\end{aligned}$$

in order to get

$$\begin{aligned}
2-\frac{\frac{4s\varepsilon}{1+2\varepsilon}}{1-\frac{4s\varepsilon}{1+2\varepsilon}} &\leq 1+\frac{\mathrm{Prob}(B'|\bar{b})}{\mathrm{Prob}(B'|b)} \leq 2+\frac{\frac{4s\varepsilon}{1-2\varepsilon}}{1-\frac{4s\varepsilon}{1-2\varepsilon}} & (38)\\
\left(2+\frac{\frac{4s\varepsilon}{1-2\varepsilon}}{1-\frac{4s\varepsilon}{1-2\varepsilon}}\right)^{-1} &\leq \mathrm{Prob}(b|B') \leq \left(2-\frac{\frac{4s\varepsilon}{1+2\varepsilon}}{1-\frac{4s\varepsilon}{1+2\varepsilon}}\right)^{-1} & (39)\\
\frac{1-\frac{4s\varepsilon}{1-2\varepsilon}}{2-\frac{4s\varepsilon}{1-2\varepsilon}} &\leq \mathrm{Prob}(b|B') \leq \frac{1-\frac{4s\varepsilon}{1+2\varepsilon}}{2-\frac{12s\varepsilon}{1+2\varepsilon}} & (40)\\
\frac{1}{2}-\frac{\frac{2s\varepsilon}{1-2\varepsilon}}{2-\frac{4s\varepsilon}{1-2\varepsilon}} &\leq \mathrm{Prob}(b|B') \leq \frac{1}{2}+\frac{\frac{2s\varepsilon}{1+2\varepsilon}}{2-\frac{12s\varepsilon}{1+2\varepsilon}} & (41)\\
\frac{1}{2}-\frac{s\varepsilon}{1-2\varepsilon-2s\varepsilon} &\leq \mathrm{Prob}(b|B') \leq \frac{1}{2}+\frac{s\varepsilon}{1+2\varepsilon-6s\varepsilon} & (42)\\
\frac{1}{2}-2s\varepsilon &\leq \mathrm{Prob}(b|B') \leq \frac{1}{2}+2s\varepsilon & (43)
\end{aligned}$$

this last statement is true if $s\varepsilon < \frac{1}{6}$. Finally by definition of ε we get

$$\frac{1}{2}-s(2p-1)^s \leq \mathrm{Prob}(b|B') \leq \frac{1}{2}+s(2p-1)^s \qquad (44)$$

□

The theorem follows immediately by choosing $\alpha = \sqrt{2p-1}$, as long as s is chosen large enough for $s(2p-1)^{\frac{s}{2}} < 1$. □

4.2 How to decommit

The above theorem shows that an honest $\mathcal{S}$ does not reveal much about her secret bit b by sending the matrix B through the quantum channel. But now, for this to be a commitment to b, it should be possible for $\mathcal{S}$ to convince $\mathcal{R}$ of what bit she has just committed to. She should not be able to convince him of the contrary (that she committed to $\bar{b}$).

To open her commitment, $\mathcal{S}$ initiates the following protocol with $\mathcal{R}$.

Protocol 4.2 (BC-decommit$((B, \Phi, b), (B', \Theta))$)

1: $\mathcal{S}$ reveals b, B and Φ to $\mathcal{R}$

2: $\underset{i=1}{\overset{s}{\mathbf{DO}}}$ $\mathcal{R}$ checks that $\bigoplus_{j=1}^{s} b_{i,j} = b$

3: $\underset{i=1}{\overset{s}{\mathbf{DO}}}\underset{j=1}{\overset{s}{\mathbf{DO}}}$ $\mathcal{R}$ checks that $b'_{i,j} = b_{i,j}$ whenever $\varphi_{i,j} = \varphi_{i,j}$

4: **if** this condition is satisfied for all i and j, **then** $\mathcal{R}$ outputs "accept" **else** $\mathcal{R}$ outputs "reject"

If s is chosen large enough, when $\mathcal{S}$ tries to change b to $\bar{b}$, she will create errors in the revealed matrix with high probability. Let $b_i = \bigoplus_{j=1}^{s} b_{i,j}$ and define b'_i similarly. It is extremely unlikely that $\mathcal{S}$ finds two pairs of matrices B^0, Φ^0 and B^1, Φ^1 such that each of the b_i^0's is 0, while each of the b_i^1's is 1 and such that

$$\forall i, j[(\varphi^0_{i,j} = \varphi_{i,j}) \Rightarrow (b^0_{i,j} = b'_{i,j}) \text{ and } (\varphi^1_{i,j} = \varphi_{i,j}) \Rightarrow (b^1_{i,j} = b'_{i,j})]$$

Theorem 4.3 *The probability that $\mathcal{S}$ finds two pairs of matrices B^0, Φ^0 and B^1, Φ^1 that could be both accepted by $\mathcal{R}$ is at most α^s for some $\alpha < 1$.*

Proof.

Let $\tilde{B}$ be the best approximation to B' that $\mathcal{S}$ can get. When both $\mathcal{S}$ and $\mathcal{R}$ are honest, $\tilde{B} = B$ and $\mathcal{S}$ knows that $\text{Prob}(b_{i,j} = b'_{i,j}) = \frac{3}{4}$. To increase her knowledge of B', $\mathcal{S}$ can cheat and send $\tilde{B}$ by using some angles $\tilde{\varphi}_{i,j}$ that are not $0°$ or $45°$. When only $\mathcal{R}$ is honest, the maximum information that $\mathcal{S}$ may get about each $b'_{i,j}$ is by sending her bits $\tilde{b}_{i,j}$ using angle $22\frac{1}{2}^{\circ} + \tilde{b}_{i,j} \times 90°$, which gives her $\text{Prob}(\tilde{b}_{i,j} = b'_{i,j}) = \cos^2(22\frac{1}{2}^{\circ})$. Still, $\mathcal{S}$ will always have a probability of $\sin^2(22\frac{1}{2}^{\circ})$ of guessing $b'_{i,j}$ incorrectly.

Whichever way $\tilde{B}$ is chosen, we get that at least one of B^0 or B^1 must have $\frac{s}{2}$ lines that do not match with $\tilde{B}$. This is true because B^0 and B^1 have s lines that do not match. Assume without lost of generality that B^0 has at least as many lines not matching $\tilde{B}$ as B^1.

Each time $\mathcal{S}$ changes a bit $\tilde{b}_{i,j}$ to its complement in order to claim B^0 instead of $\tilde{B}$ she has probability $\frac{1}{2}$ of revealing an angle $\varphi^0_{i,j} = \varphi_{i,j}$ in which case she has at least probability $\sin^2(22\frac{1}{2}^{\circ})$ that $b^0_{i,j} \neq b'_{i,j}$. Therefore for each bit changed, $\mathcal{S}$ will create an error with probability at least $\frac{\sin^2(22\frac{1}{2}^{\circ})}{2}$. Her probability of creating no error when revealing B^0 is therefore at most $\left(\sqrt{1 - \frac{\sin^2(22\frac{1}{2}^{\circ})}{2}}\right)^s$.

From this we conclude that $\mathcal{S}$ may succeed in opening B in both ways with probability at most α^s for some $\alpha < 1$. □

Notice, however, that even a few transmission errors will lead $\mathcal{R}$ to believe that $\mathcal{S}$ is cheating and thus to reject her commitments even when she is honest. The solution to this problem is not at all addressed in the current paper and will be the topic of another paper dealing with transmission errors in quantum protocols. That paper is currently in preparation with Charles Bennett [BBC90].

Finally, we have

Theorem 4.4 *This protocol cannot be broken using E-P-R.*

Proof.

Provided in the journal version of the paper. □

4.3 Can this new scheme be broken?

One thing not ruled out by quantum mechanics is the possibility of evaluating predicates on several photons at once. Such a possibility is known to the world of quantum mechanics as *coherent measurements*. For instance, there are functions f such that given two photons of polarization φ_1 and φ_2, there might exist a way to find out more about $f(\varphi_1, \varphi_2)$ than what can be obtained by applying f to what can be measured about φ_1 and φ_2 separately.

Such a possibility could make the commitment scheme described above totally insecure if the $\oplus$ of the values carried by many photons could be evaluated at once. The value of b could be recovered easily using equation 2: $\bigoplus_{j=1}^{s} b_{i,j} = b$ and taking majority on the rows.

Actually this possibility is, as far as the authors know, the only possible way to cheat our protocol. Fortunately, not only is no technology available to do coherent measurements, but also physicists do not even know how to get photons to interact in ways that could lead to such a measurement. Therefore, although such a possibility exists in theory, in practice there should be very little concern that the protocol be broken this way.

5 Have we won anything?

As it turns out, having two different schemes is better than one: One can build a Coin Tossing Protocol that can be broken only if one can implement *both* the E-P-R attack and coherent measurements. Consider the following protocol:

Protocol 5.1 (BC-cointoss)

1: $\mathcal{S}$ chooses a random bit b_0 and uses BB-commit(b_0) with $\mathcal{R}$

2: $\mathcal{R}$ chooses a random bit b_1 and uses BC-commit(b_1) with $\mathcal{S}$
(the roles of $\mathcal{R}$ and $\mathcal{S}$ are temporarily interchanged)

3: $\mathcal{S}$ runs BB-decommit(b_0) with $\mathcal{R}$

4: $\mathcal{R}$ runs BC-decommit(b_1) with $\mathcal{S}$

5: $\mathcal{R}$ wins the coin toss if and only if $b_1 = b_0$

This protocol can be broken only if $\mathcal{S}$ can implement the E-P-R attack **as well as** the coherent measurement attack. $\mathcal{R}$ has no way to cheat whatsoever, unless he can design an apparatus that can transmit information faster than the speed of light. The proof of these claims will be provided in the journal version of the paper.

6 Conclusion

In the light of ongoing progress in physics, it is reasonable to fear that the E-P-R attack on the bit commitment scheme (or coin flipping protocol) of [BB84] could be implemented. The commitment scheme we have presented in this paper does not yield to this attack. Unfortunately, we can still describe a possible attack on this new scheme, which is based on an unverified belief about quantum mechanics (unlike E-P-R, which has been verified experimentally). Can one build such a scheme, unbreakable in an absolute way, based solely on the equations of quantum mechanics? We cannot answer this question at this time.

Still we have been able to build a coin-tossing protocol that is secure unless both attacks can be implemented. This seems to indicate that maybe Bit Commitment is more than Coin-Tossing since, at this time, we are unable to offer a Bit Commitment scheme with this same level of security.

7 Acknowledgements

We wish to thank Charles H. Bennett and Joe Kilian for suggestions and comments on this work. Claude would especially like to thank Silvio Micali for the collossal work he contributed while writing and polishing this text which first appeared in part in Claude's Ph.D. thesis.

References

[BBBSS90] Bennett, C. H., F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography", *Advances in Cryptology: Proceedings of Eurocrypt '90*, Aarhus, Denmark, Springer–Verlag, to appear, 1990.

[BB84] Bennett, C. H. and G. Brassard, "Quantum cryptography: public key distribution and coin tossing", *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, pp. 175–179, 1984.

[BBC90] Bennett, C. H., G. Brassard, and C. Crépeau, "Practical Quantum Oblivious Transfer", *in preparation.*

[BCC88] Brassard, G., D. Chaum, and C. Crépeau, "Minimum disclosure proofs of knowledge", *Journal of Computer and System Sciences*, Vol. 37, no. 2 pp. 156–189, 1988.

[Blu81] Blum, M., "Three applications of the oblivious transfer: Part I: Coin flipping by telephone; Part II: How to exchange secrets; Part III: How to send certified electronic mail", Technical Report, Department of EECS, University of California, Berkeley, CA, 1981.

[EGL83] Even, S., O. Goldreich, and A. Lempel. "A randomized protocol for signing contracts", In R. L. Rivest, A. Sherman, and D. Chaum, editors, *Proceedings CRYPTO 82*, pages 205–210, New York, 1983. Plenum Press.

[GMW86] Goldreich, O., S. Micali, and A. Wigderson, "Proofs that yield nothing but their validity and a methodology of cryptographic protocol design", *Proceedings of the 27th IEEE Symposium on Foundations of Computer Science*, pp. 174–187, Toronto, 1986.

[Wie83] Wiesner, S., "Conjugate coding", *Sigact News*, Vol. 15, no. 1, pp. 78–88, 1983. manuscript written *circa* 1970, unpublished until it appeared in Sigact News.