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]). One of his ideas was that it would be possible to use a stream of polarized photons to transmit two messages 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], and it even predates Rabin's notion of oblivious transfer [Rab81] by more than a decade. In the late 1970's, Wiesner's invention was brought back to life by the work of Charles H. Bennett and Gilles Brassard, which resulted in a CRYPTO '82 paper [BBBW82]. Subsequently, Bennett and Brassard used quantum cryptographic principles to implement basic cryptographic protocols, such as secret key exchange and coin tossing by telephone [BB84]. There has been recently much excitement in the field of 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.

*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.

A.J. Menezes and S.A. Vanstone (Eds.): Advances in Cryptology - CRYPTO '90, LNCS 537, pp. 49-61, 1991.

While such primitives are usually built under computational complexity assumptions, it is sometimes possible to build them based on assumptions of a different nature, as pointed out by [Wie83, BBBW82, BB84, CK88]. 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.

2 Physics background

For a complete coverage of the physics of quantum cryptography, please consult [BB84] or chapter 6 of [Bra88]. 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 $[0°, 180°)$, only specific boolean (two states) predicates 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 $\Theta = 0°$?" can be measured accurately for these two quantum states (at least in principle). 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 constraint on the set of possible values for Θ, then the result of *any* apparatus designed to decide whether $\Theta = 0°$ will be a probabilistic answer dependent on the value of Θ, but no certainty can be achieved. It is not a matter of technology, it is not that no one has a good enough apparatus to figure out Θ; quantum theory tells us that it is **impossible** to determine this value with certainty.

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

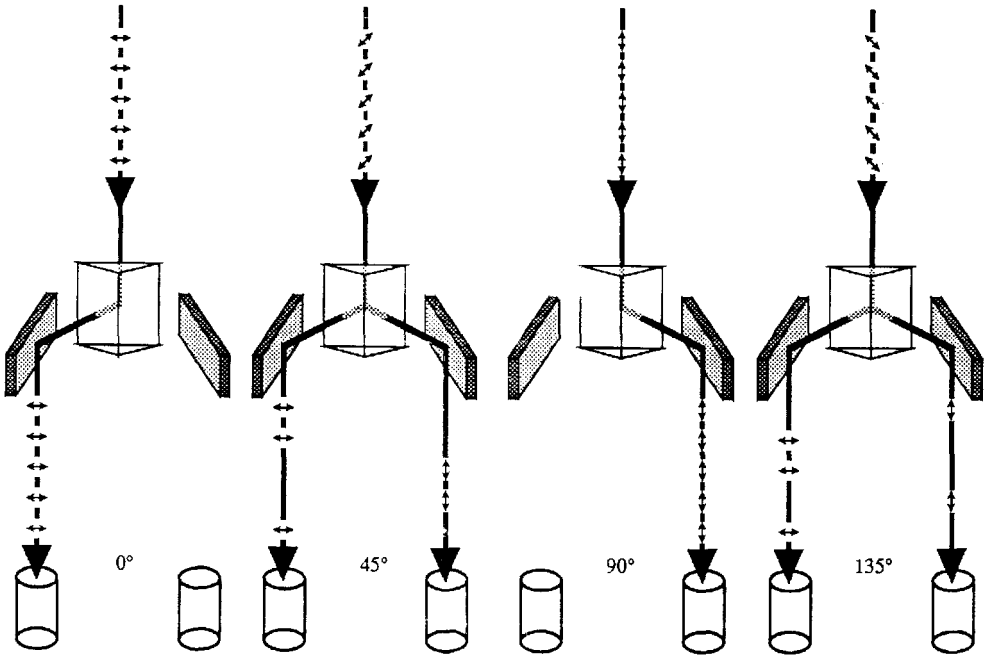

Figure 1: Photons passing through a Wollaston prism set at angle 0°.

3 Review of earlier quantum protocols

3.1 A bit commitment scheme

Consider two parties: a *sender* $\mathcal{S}$ and a *receiver* $\mathcal{R}$. Assume that $\mathcal{S}$ has a bit b in mind, to which she[1] 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. At a later time, however, it must be possible for $\mathcal{S}$ to *open* the commitment, that is to show $\mathcal{R}$ which bit she had committed to, and convince him that this is indeed the genuine bit that she had in mind when she committed.

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; here, we proceed the other way around). Let us briefly review this protocol and its main weaknesses before describing our new scheme in Section 4. Let s be a security parameter. In order to commit to bit b toward $\mathcal{R}$, $\mathcal{S}$ initiates the following protocol.

[1] For the sake of convenience, we shall refer to $\mathcal{S}$ as a "she" and to $\mathcal{R}$ as a "he".

Protocol 3.1 (BB-commit(b))

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

2: $\mathcal{R}$ chooses a vector $\Theta = (\theta_1, \theta_2, ..., \theta_s)$ of s random $\theta_i \in \{0°, 45°\}$

3: $\overset{s}{\underset{i=1}{\mathbf{DO}}}$ $\mathcal{S}$ sends a photon with polarization $b \times 45° + b_i \times 90°$,
which $\mathcal{R}$ reads at angle θ_i

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

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

5: $\mathcal{S}$ keeps b and B secret until (and if) she later opens her commitment

Notice that since b_i is chosen at random, the received bit b'_i reveals no information about b. Therefore receiving $B' = (b'_1, b'_2, ..., b'_s)$ reveals nothing about b. But of course, $\mathcal{R}$ could be dishonest and perform a different measurement on the photons sent by $\mathcal{S}$ in the hope of learning something about b. In fact, a very strong 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. It is impossible to obtain even a probabilistic bias about which bit was committed to. Therefore, the privacy of $\mathcal{S}$'s bit b is unconditionally protected. But why is $\mathcal{S}$ committed?

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

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

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

2: $\overset{s}{\underset{i=1}{\mathbf{DO}}}$ $\mathcal{R}$ checks that $b'_i = b_i$ whenever $\theta_i = b \times 45°$

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, provided that no transmission errors have occurred due to imperfections of the apparatus (the possibility of transmission errors in practice is addressed in section 3.3). Now suppose that a cheating $\mathcal{S}$ tries to "commit" in a way that will enable her to open B as 0 or 1 at her later choice. In order to achieve this, she may prefer to send her photons at angles

that are not among $\{0°, 45°, 90°, 135°\}$. A *strategy* for a cheating $\mathcal{S}$ consists of a vector $\Phi = (\phi_1, \phi_2, ..., \phi_s)$ of values in the real interval $[0°, 180°)$ together with two binary vectors $B^0 = (b_1^0, b_2^0, ..., b_s^0)$ and $B^1 = (b_1^1, b_2^1, ..., b_s^1)$. In order to use this strategy, $\mathcal{S}$ sends her i^{th} photon with polarization angle ϕ_i during protocol BB-commit. If she wishes to open the commitment as $b \in \{0, 1\}$, she runs BB-open with (B^b, b) as her share of the input. The strategy is *successful* if

$$\forall i \left[(\theta_i = 0°) \Rightarrow (b_i^0 = b_i') \text{ and } (\theta_i = 45°) \Rightarrow (b_i^1 = b_i') \right]. \quad (1)$$

An *optimal* strategy is one that has the highest probability of being successful.

We leave it for the reader to verify that for all choices of B^0 and B^1, there is exactly one choice of Φ that will maximize $\mathcal{S}$'s probability of success. In that optimal choice, it is always the case that all ϕ_i's belong to $\{22\frac{1}{2}°, 67\frac{1}{2}°, 112\frac{1}{2}°, 157\frac{1}{2}°\}$. For example, if $b_i^0 = 1$ and $b_i^1 = 0$, then it is best to set $\phi_i = 67\frac{1}{2}°$ because b_i' is likely to be 1 if $\mathcal{R}$'s reading angle θ_i was 0° whereas b_i' is likely to be 0 if θ_i was 45°. With this strategy, $\mathcal{S}$'s probability of failure is $\sin^2(22\frac{1}{2}°) \approx 15\,\%$ for each i. Therefore, whichever strategy is used, the probability that equation 1 holds is at most $(\cos^2(22\frac{1}{2}°))^s$, which can be made arbitrarily small. (If $\mathcal{R}$ follows his protocol blindly, $\mathcal{S}$'s simplest optimal strategy is to set $\phi_i = 22\frac{1}{2}°$ and $b_i^0 = b_i^1 = 0$ for all i. However, a human $\mathcal{R}$ might become suspicious. Therefore, it is safer to choose B^0 and B^1 randomly and to set Φ accordingly.)

3.2 Coin tossing

Bennett and Brassard used this technique 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-open(b_0) with $\mathcal{R}$

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

This protocol can be broken exactly if the bit commitment scheme can be broken. Of course, $\mathcal{S}$ could refuse to cooperate at step 3 if she decides that she does not wish the result of the coin toss to become known to $\mathcal{R}$.

3.3 The problems with this scheme

The bit commitment scheme of section 3.1 and the resulting coin tossing protocol have major defects both in principle and in practice.

As mentioned in [BB84], these schemes can be defeated in theory using the consequences of the Einstein–Podolsky–Rosen so-called "EPR paradox" [EPR35]. The interested reader can consult [BB84] for a more detailed explanation. Let us only say here that this kind of attack is rather implausible in practice because the apparatus 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 the loss of her[2] possibility of cheating. Nevertheless, from a theoretical point of view, it is important to design a protocol that is not subject to the EPR threat. This is precisely the main purpose of the current paper, as we shall proceed to explain in the next section.

In addition to the theoretical weakness described above, the schemes of [BB84] suffer from two problems in practice. One of these problems is easy to deal with but the other is not. The first practical problem is that it is not reasonable to expect in protocol BB-open that $b'_i = b_i$ every single time that $\theta_i = b \times 45°$. Indeed, transmission errors will necessarily occur in practice. Such errors can be due to misalignment of $\mathcal{S}$'s and $\mathcal{R}$'s apparatuses, to dark currents in $\mathcal{R}$'s photomultipliers and to photons repolarizing for one reason or another while in transit. Also, photomultipliers do not have perfect efficiency, and therefore $\mathcal{R}$ will receive nothing at all most of the time (in which case he knows that he did not receive the photon, unless he is fooled by his own photomultipliers' dark current — a reasonably rare event). Fortunately, the actual apparatus built in Yorktown Heights to demonstrate the feasibility of the quantum key exchange protocol [BBBSS90] shows that it is entirely reasonable to expect an error rate below 5 % when a photon is received (or thought to be received). On the other hand, recall that $\mathcal{S}$'s optimal cheating strategy would give her the value of each relevant b'_i with probability roughly 85 % (even if no transmission errors occur). Therefore, the protocol remains safe against $\mathcal{S}$'s cheating attempts even if $\mathcal{R}$ accepts provided that $b'_i = b_i$ at least 90 % of the times when the photon is detected and $\theta_i = b \times 45°$. The only price to pay for this increased robustness is that the security parameter s must be chosen larger in order to attain the same small probability of undetected cheating.

The other practical problem with the schemes of [BB84] is much more serious. Recall that the protocol calls for $\mathcal{S}$ to send single polarized photons to $\mathcal{R}$. Although this is possible in principle, it is very difficult to achieve in practice. It is much easier to send very dim pulses of polarized photons, as with the experimental quantum key exchange apparatus. Unfortunately, such dim pulses will sometimes contain more than one photon, and all the photons in any single pulse will be polarized at the same angle. These multiphoton pulses are of no consequences for key exchange, but they spell doom on the bit commitment scheme described above. Indeed, whenever

[2] Only $\mathcal{S}$ can take advantage of the EPR loophole. As previously stated, $\mathcal{R}$ has no possibility of cheating whatsoever.

$\mathcal{R}$ reads a pulse at angle θ_i and detects photons coming out *both* on the right and the left, it is very likely to mean that the pulse contained more than one photon and that they were all polarized either at angle $45° - \theta_i$ or $135° - \theta_i$. In either case, the value of b becomes known to $\mathcal{R}$. There is no known way to get around this difficulty in practice with the bit commitment scheme of Bennett and Brassard. In sharp contrast, the new scheme that we now describe remains secure even if a small number of multiphoton pulses occur.

4 A new bit commitment scheme

4.1 How to commit

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

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

which is random subject to the following property:

$$\forall 1 \leq i \leq s \quad \left[\bigoplus_{j=1}^{s} b_{i,j} = b \right]. \tag{2}$$

She 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: $\overset{s}{\underset{i=1}{\mathrm{DO}}}\ \overset{s}{\underset{j=1}{\mathrm{DO}}}$ $\mathcal{S}$ chooses a random $\phi_{i,j} \in \{0°, 45°\}$ and
$\mathcal{R}$ chooses a random $\theta_{i,j} \in \{0°, 45°\}$

3: $\overset{s}{\underset{i=1}{\mathrm{DO}}}\ \overset{s}{\underset{j=1}{\mathrm{DO}}}$ $\mathcal{S}$ sends a photon with polarization $\phi_{i,j} + b_{i,j} \times 90°$,
which $\mathcal{R}$ reads at angle $\theta_{i,j}$
$\mathcal{R}$ sets $b'_{i,j} \leftarrow \begin{cases} 0 & \text{if photon came out on the left} \\ 1 & \text{if photon came out on the right} \end{cases}$

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

5: $\mathcal{S}$ keeps b, B and Φ (see below) secret until (and if) she later opens her commitment

where

$$B' = \begin{pmatrix} b'_{1,1} & \cdots & b'_{1,s} \\ \vdots & \ddots & \vdots \\ b'_{s,1} & \cdots & b'_{s,s} \end{pmatrix}, \Theta = \begin{pmatrix} \theta_{1,1} & \cdots & \theta_{1,s} \\ \vdots & \ddots & \vdots \\ \theta_{s,1} & \cdots & \theta_{s,s} \end{pmatrix}, \text{ and } \Phi = \begin{pmatrix} \phi_{1,1} & \cdots & \phi_{1,s} \\ \vdots & \ddots & \vdots \\ \phi_{s,1} & \cdots & \phi_{s,s} \end{pmatrix}.$$

If both participants are honest, B' is such that

$$\forall 1 \leq i \leq s, 1 \leq j \leq s \; [\text{Prob}(b'_{i,j} = b_{i,j}) = \tfrac{3}{4}].$$

However, if $\mathcal{R}$ uses angle $\theta_{i,j} = 22\frac{1}{2}^\circ$, he will end up getting more information about B. It is an easy exercise to prove that this is the optimal strategy for a cheating $\mathcal{R}$. With such measurements, $\forall 1 \leq i \leq s, 1 \leq j \leq s \; [\text{Prob}(b'_{i,j} = b_{i,j}) = \cos^2(22\frac{1}{2}^\circ)]$. 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

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

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*

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

Proof.

Provided in the journal version of the paper. □

4.2 How to open

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, hence $\mathcal{R}$ may at best learn an exponentially small bias about bit b. But for this to be a commitment, it should be possible for $\mathcal{S}$ to convince $\mathcal{R}$ of what bit she has committed to. She should not be able to open the "commitment" to show a bit of her choice.

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

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

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

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

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

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

In order to prove that $\mathcal{S}$ cannot cheat, one must once again take account of all the possible ways in which $\mathcal{S}$ could deviate from her prescribed behaviour, not only in BC-open but also in BC-commit. In particular, she could bypass the choice of matrices B and Φ at steps 1 and 2 in BC-commit, and send photons with arbitrary polarization angles at step 3. In general, a *strategy* for a cheating $\mathcal{S}$ consists of a matrix $\tilde{\Phi}$ of arbitrary angles, together with two pairs of matrices B^0, Φ^0 and B^1, Φ^1 such that B^0 and B^1 are boolean, whereas Φ^0 and Φ^1 contain only $0°$ and $45°$. In order to use this strategy, $\mathcal{S}$ sends her photons with polarization angles according to $\tilde{\Phi}$ during protocol BB-commit. If she wishes to open the commitment as $b \in \{0,1\}$, she runs BB-open with (B^b, Φ^b, b) as her share of the input. A strategy is *successful* if

$$\forall i \left[\bigoplus_{j=1}^{s} b^0_{i,j} = 0 \quad \text{and} \quad \bigoplus_{j=1}^{s} b^1_{i,j} = 1 \right], \text{ and} \tag{3}$$

$$\forall i,j \left[(\phi^0_{i,j} = \theta_{i,j}) \Rightarrow (b^0_{i,j} = b'_{i,j}) \text{ and } (\phi^1_{i,j} = \theta_{i,j}) \Rightarrow (b^1_{i,j} = b'_{i,j}) \right]. \tag{4}$$

Theorem 4.2 *There exists a constant $\alpha < 1$ such that the probability of success of any strategy is at most α^s.*

Proof.

First notice that there are no probabilities associated with whether a strategy satisfies equation 3. Thus, we may as well assume that this equation holds, which implies that B^0 and B^1 differ at least once in each row. Therefore, there are at least s bits that are different between these two matrices. Let i and j be such that $b^0_{i,j} \neq b^1_{i,j}$. First consider the case in which $\phi^0_{i,j} = \phi^1_{i,j} = \phi$. With probability $\frac{1}{2}$, the reading angle $\theta_{i,j}$ is equal to ϕ. If this occurs, equation 4 is necessarily violated. Also with probability $\frac{1}{2}$, $\theta_{i,j} \neq \phi$, in which case equation 4 is (vacuously) satisfied for such values of i and j. Therefore, the choice of $\tilde{\phi}_{i,j}$ is irrelevant when $b^0_{i,j} \neq b^1_{i,j}$ and $\phi^0_{i,j} = \phi^1_{i,j}$, and the probability that this will cause the strategy to be rejected is always $\frac{1}{2}$.

Now consider the case in which $\phi^0_{i,j} \neq \phi^1_{i,j}$. In order to maximize her chances of satisfying equation 4, $\mathcal{S}$'s optimal strategy is to send the corresponding photon at an angle $\tilde{\phi}_{i,j}$ that will simultaneously maximize her chances that it will be read as $b^0_{i,j}$ if measured at angle $\phi^0_{i,j}$, whereas it will be read as $b^1_{i,j}$ if measured at angle $\phi^1_{i,j}$. That angle is easily seen to be $67\frac{1}{2}^\circ$ if $b^0_{i,j} = 0$ and $\phi^0_{i,j} = 45^\circ$ or if $b^0_{i,j} = 1$ and $\phi^0_{i,j} = 0^\circ$. The angle $157\frac{1}{2}^\circ$ is optimal for the other two cases. In all cases, equation 4 is violated with probability $\sin^2(22\frac{1}{2}^\circ) \approx 15\,\%$.

This shows clearly that it is always preferable to set $\phi^0_{i,j} \neq \phi^1_{i,j}$ whenever $b^0_{i,j} \neq b^1_{i,j}$, but that even then the probability of success is at most $\cos^2(22\frac{1}{2}^\circ) \approx 85\,\%$ for each such pair (i,j). Since there must be at least s such pairs in order to satisfy equation 3, we conclude that no strategy can succeed with probability greater than $(\cos^2(22\frac{1}{2}^\circ))^s$, which can be made arbitrarily small. □

4.3 The problems with this new scheme

Recall that the original bit commitment scheme of Bennett and Brassard [BB84] suffered from problems in principle as well as in practice. Unfortunately, this is also the case with our new scheme. However, the new protocol is somewhat of a dual to he old one because the problems that were serious with the old scheme are of no consequence with the new scheme, and *vice versa*. Also, the only party that had a possibility of cheating in an ideal implementation of the old scheme was $\mathcal{S}$, whereas now it is $\mathcal{R}$. We shall see in section 5 how to capitalize on this role reversal.

One thing that is not ruled out by quantum mechanics is the possibility of evaluating predicates on several photons at once. Such possibility is known in 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 $f(\phi_1, \phi_2)$ than what can be obtained by applying f (or perhaps another function) to what can be measured about ϕ_1 and ϕ_2 separately. Such a possibility would make the commitment scheme described above totally insecure if the $\oplus$ of the values carried by many photons could be measured at once, even if only a reasonably good estimate on the answer could be obtained. Indeed, the value of b could then be recovered easily using equation 2: $b = \bigoplus_{j=1}^{s} b_{i,j}$ and taking majority on the rows.

Fortunately, not only is no technology available to do coherent measurements, but its availability is not predicted for any foreseeable future. In fact, physicists do not even know how to get photons to interact in ways that could lead to such measurements. Therefore, although such a possibility exists in principle for $\mathcal{R}$ to cheat, there should be very little concern that the protocol be broken this way in practice. On the other hand, it is easy to see that the EPR threat that allowed $\mathcal{S}$ to cheat the protocol of Bennett and Brassard does not apply to the new scheme even in principle. (And conversely, coherent measurements could not help break the old scheme even in principle.)

From a practical point of view, however, notice 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. Because occasional transmission errors are technologically unavoidable, it is important to be able to deal with them if this scheme is ever to be used in practice. We do not know of any simple solution to solve this difficulty because it would be easy for $\mathcal{S}$ to cheat if $\mathcal{R}$ were willing to tolerate that $b'_{i,j} \neq b_{i,j}$ even occasionally when $\theta_{i,j} = \phi_{i,j}$. Nevertheless, this problem will be addressed in another paper whose purpose is to deal with transmission errors in quantum protocols. That paper, which is currently in preparation with Charles H. Bennett [BBC90], solves not only the question of practical quantum bit commitment, but also that of practical quantum oblivious transfer.

On the other hand, recall that the bit commitment scheme of Bennett and Brassard was seriously impaired in practice by the difficulty of producing single polarized photons. A more careful analysis in the proof of theorem 4.1 shows that this is not a worry with the new protocol presented here. Our protocol works just as well if multiphoton pulses happen, provided that their occurrence is not too frequent (at the cost of using a slightly larger security parameter s).

5 Have we gained anything?

As it turns out, having two different schemes is better than one even if each of them can be broken in principle. Indeed, one can build a coin tossing protocol that can be broken only if one can implement *both* the EPR 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-open(b_0) with $\mathcal{R}$

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

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

In principle, this protocol can be broken only if $\mathcal{S}$ can implement the EPR attack **as well as** the coherent measurement attack. $\mathcal{R}$ has no way of cheating whatsoever, unless he can design an apparatus that can transmit information faster than the speed of light. The proof of this claim will be provided in the journal version of the paper.

6 Conclusion and open problems

In the light of ongoing progress in experimental physics [AG86], it is reasonable to fear that the EPR attack on the bit commitment scheme (or coin tossing protocol) of [BB84] could be implemented. The bit commitment scheme that we have presented in this paper does not yield to this attack. Unfortunately, we can still describe an attack on this new scheme, which is possible in principle although not in practice, based on coherent measurements. Can one build a bit commitment scheme unbreakable in an absolute way, based solely on the equations of quantum mechanics? We cannot answer this question at this time even if practical considerations are not taken into account.

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 are very grateful to Charles H. Bennett and Joe Kilian for suggestions and comments on this work. Claude would especially like to thank Silvio Micali for the colossal work he contributed while writing and polishing this text, parts of which first appeared in Claude's Ph.D. thesis.

References

[AG86] Aspect, A. and P. Grangier, "Experiments on Einstein – Podolsky – Rosen-type correlations with pairs of visible photons", in *Quantum concepts in space and time* (R. Penrose and C. J. Isham, eds.), Oxford University Press, 1986.

[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. Submitted to *Journal of Cryptology*.

[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.

[BBBW82] Bennett, C. H., G. Brassard, S. Breidbart, and S. Wiesner, "Quantum cryptography, or unforgeable subway tokens", *Advances in Cryptology: Proceedings of Crypto 82*, Plenum Press, pp. 267 – 275, 1983.

[BBC90] Bennett, C. H., G. Brassard, and C. Crépeau, "Practical Quantum Oblivious Transfer", *in preparation*, 1990.

[Bra88] Brassard, G., *Modern Cryptology*, Lecture Notes in Computer Science, Vol. 325, Springer–Verlag, 1988.

[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.

[CK88] Crépeau, C. and J. Kilian, "Achieving oblivious transfer using weakened security assumptions", *Proceedings of the 29th IEEE Symposium on Foundations of Computer Science*, pp. 42–52, 1988.

[EPR35] Einstein, A., P. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?", *Physical Review*, Vol. 47, pp. 777–780, 1935. Reprinted in *Quantum theory and measurement* (J. A. Wheeler and W. Z. Zurek, eds.), Princeton University Press, 1983.

[EGL83] Even, S., O. Goldreich, and A. Lempel, "A randomized protocol for signing contracts", *Advances in Cryptology: Proceedings of Crypto 82*, Plenum Press, pp. 205–210, 1983.

[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, 1986.

[Rab81] Rabin, M. O., "How to exchange secrets by oblivious transfer", Technical Memo TR–81, Aiken Computation Laboratory, Harvard University, 1981.

[Wie83] Wiesner, S., "Conjugate coding", *Sigact News*, Vol. 15, no. 1, pp. 78–88, 1983. manuscript written *circa* 1969, unpublished until it appeared in *Sigact News*.