To appear in the Journal of Modern Optics' special issue on Quantum Cryptography, 1994

Quantum Oblivious Transfer

Claude Crépeau
École Normale Supérieure *
Université de Montréal †

Abstract

In a One-out-of-two Oblivious Transfer, a party *Alice* has two messages m_0, m_1 that she sends to another party *Bob* in such a way that he can decide to get either of them at his choosing but not both. *Alice* never finds out which message *Bob* received. First introduced by Wiesner as "conjugate coding" this cryptographic tool was later introduced to the world of public-key cryptography, first by Rabin (in a slightly different flavour) and then by Even, Goldreich and Lempel who named it after Rabin's primitive called Oblivious Transfer. The One-out-of-two Oblivious Transfer was later showed extremely powerful to design general cryptographic tools.

The current paper presents a new design of a One-out-of-two Oblivious Transfer based on the transmission of polarized light, improving the work of Wiesner [17] and Bennett, Brassard, Breidbart and Wiesner [3] and shows that the scheme is robust to general attacks.

1 Introduction

In his now celebrated paper [17] Stephen Wiesner not only introduced the idea that quantum mechanics could be useful to cryptography but also introduced a new cryptographic tool that he called "conjugate coding". Little did he suspect how powerful his inventions were! Conjugate coding was independently reinvented a decade later by Even, Goldreich and Lempel [12] who named it "one-out-of-two Oblivious Transfer" after another cryptographic tool of similar flavour put forward by Rabin [16] and called "Oblivious Transfer".

Informally speaking in an Oblivious Transfer, *Alice* sends a message to *Bob* that he receives half the time (this fact is out of their control). *Alice* does not find out what happened. *Bob* knows if he got the message or nothing. Similarly, in a One-out-of-two Oblivious Transfer, *Alice* has two messages m_0, m_1 that she sends to *Bob* in such a way that he can decide to get either of them at his choosing but not both. *Alice* never finds out which message *Bob* received.

* Laboratoire d'Informatique de l'École Normale Supérieure (CNRS URA1327),
45 rue d'Ulm, 75230 Paris CÉDEX 05, France. e-mail:crepeau@dmi.ens.fr.
†Département IRO, Université de Montréal,
C.P. 6128, succursale centre-ville, Montréal (Québec) Canada H3C 3J7

These two simple cryptographic tools have been extensively studied by several researchers because they turned out to be elementary blocks to build more elaborate cryptographic tasks known as "secure computations". This idea introduced by Yao [18] allows $\mathcal{A}lice$ and $\mathcal{B}ob$ to compute a two-argument function on data they would like to keep secret from one another. They find out the output of the function but not their respective inputs. It was shown in a *computational* model that One-out-of-two Oblivious Transfer suffices to perform general secure computations by Goldreich, Micali and Wigderson [13] and later in an abstract (not necessarily computational) model by Kilian [14]. I showed [7] that indeed Rabin's Oblivious Transfer can also do the job by describing a general technique to turn an Oblivious Transfer into a One-out-of-two Oblivious Transfer. The result of the current paper is an extension of that technique.

Although quite remarkable, Wiesner's idea of a conjugate coding seemed rather vague. In particular Wiesner's construction for conjugate coding suffered several major flaws:

- it is trivial to get parts of both messages m_0 and m_1
- his construction relies on error correcting codes that may not even exist
- he himself suggested that general measurements on several photons at once or POVMs could extract both messages completely

The same flaws applied to the scheme of Bennett, Brassard, Breidbart and Wiesner [3] as well. Because of these reasons, it seemed necessary to the author to approach the problem with fresh ideas. One important simplification that Wiesner was not aware of, is that it suffices to have a conjugate coding for one-bit long messages which can be extended to longer strings by the result of [6, 10]. The result of this current paper is to exhibit a protocol for the binary version of One-out-of Two Oblivious Transfer, from now on denoted $\binom{2}{1}$–OT_2, whose security relies on quantum mechanics. Earlier versions of this work were presented in [9, 8].

2 Formal Problem

Formally speaking we describe a two-party protocol that satisfies the natural constraints (see below) of *correctness* and *privacy* of a $\binom{2}{1}$–OT_2. For a more thorough description of these concepts, we refer the reader to [8], but some intuition follows. Let $V_P(H, b_0, b_1, c)$ be the random variable that describes the information that a party P has at the end of its interaction through the protocol executed on inputs b_0, b_1, c and where H (for History) is the random variable describing the a priori information the party P has before entering the protocol. Finally, we denote $\mathbf{H}(X) = -\sum_x \mathbf{P}[X = x] \log \mathbf{P}[X = x]$ the entropy function of the random variable X.

Correctness: It should be that when $\mathcal{A}lice$ and $\mathcal{B}ob$ follow the protocol and start with $\mathcal{A}lice$'s input bits $\langle b_0, b_1\rangle$ and $\mathcal{B}ob$'s input bit $\langle c\rangle$ they finish with $\mathcal{B}ob$ getting b_c.

Intuitively, this constraint means that if the protocol is executed as described, it will accomplish the task it was designed for.

Privacy: It should be that whatever program, $\tilde{\mathcal{A}}$, $\mathcal{A}lice$ runs she does not find out about c, that is for all H, b_0, b_1

$$\mathbf{H}(c|V_{\tilde{\mathcal{A}}}(H, b_0, b_1, c)) = \mathbf{H}(c|H, b_0, b_1)$$

and that whatever program, $\tilde{\mathcal{B}}$, $\mathcal{B}ob$ runs he does not find out information about more than one of b_0, b_1, that is for all H, c, b

$$\mathbf{H}(b_0|V_{\tilde{\mathcal{B}}}(H, b_0, b, c), b) = \mathbf{H}(b_0|H, c, b)$$

or

$$\mathbf{H}(b_1|V_{\tilde{\mathcal{B}}}(H, b, b_1, c), b) = \mathbf{H}(b_1|H, c, b).$$

Intuitively, these constraints mean that if a party is honest it is impossible for his (or her) opponent to gain "illegal" information about his input. For $\mathcal{A}lice$ it simply means that she learns nothing about c. For $\mathcal{B}ob$ it is somewhat more elaborate: in an *ideal* execution of a $\binom{2}{1}$–OT_2 (a situation in which $\mathcal{B}ob$ is simply given b_c and no protocol actually takes place) $\mathcal{B}ob$ would be allowed to obtain a bit b which is either b_0 or b_1. Therefore the rightmost expressions are $\mathcal{B}ob$'s uncertainty about b_0 or b_1 given the other bit b as if it were obtained through the ideal $\binom{2}{1}$–OT_2. On the left side we must consider $\mathcal{B}ob$'s uncertainty about b_0 or b_1 after running the protocol and after being given the other bit b. In particular, a protocol in which $\mathcal{B}ob$ learns $b_0 \oplus b_1$, although it contains no information about neither of b_0 nor b_1 individually, would not be private since $\mathbf{H}(b_0|V_{\tilde{\mathcal{B}}}(H, b_0, b, c), b) = \mathbf{H}(b_1|V_{\tilde{\mathcal{B}}}(H, b, b_1, c), b) = 0$.

The protocol we describe in the next section is of probabilistic nature. We cannot show that this protocol perfectly satisfies the constraints we just mentioned. Nevertheless, we show the next best thing, that the constraints are satisfied in a statistical sense: after an amount of work in $O(n)$ time the protocol will satisfy for some positive constant $\varepsilon < 1$

Statistical Correctness: It should be that, except with probability at most ε^n, when $\mathcal{A}lice$ and $\mathcal{B}ob$ follow the protocol and start with $\mathcal{A}lice$'s input bits $\langle b_0, b_1\rangle$ and $\mathcal{B}ob$'s input bit $\langle c\rangle$ they finish with $\mathcal{B}ob$ getting b_c.

Statistical Privacy: It should be that, except with probability at most ε^n, whatever program, $\tilde{\mathcal{A}}$, $\mathcal{A}lice$ runs she does not find out much about c, that is for all H, b_0, b_1

$$\mathbf{H}(c|V_{\tilde{\mathcal{A}}}(H, b_0, b_1, c)) \geq \mathbf{H}(c|H, b_0, b_1) - \varepsilon^n$$

and that whatever program, $\tilde{\mathcal{B}}$, $\mathcal{B}ob$ runs he does not find out much information about more than one of b_0, b_1, that is for all H, c, b

$$\mathbf{H}(b_0|V_{\tilde{\mathcal{B}}}(H, b_0, b, c), b) \geq \mathbf{H}(b_0|H, c, b) - \varepsilon^n$$

or

$$\mathbf{H}(b_1|V_{\tilde{\mathcal{B}}}(H, b, b_1, c), b) \geq \mathbf{H}(b_1|H, c, b) - \varepsilon^n.$$

3 Protocol for Quantum Oblivious Transfer

Let Ⓒ denote the random variable that takes the binary value 0 with probability $\frac{1}{2}$ and 1 with probability $\frac{1}{2}$. Also, denote by $[\ ]_i$ the selection function such that $[a_0, a_1, ..., a_k]_i = a_i$. Let $\oplus = (|\leftrightarrow\rangle, |\updownarrow\rangle)$ and $\boxtimes = (|\nearrow\rangle, |\nwarrow\rangle)$ denote respectively the bases of rectilinear and diagonal polarization in the quantum state space of a photon.

3.1 The formal protocol

Protocol 3.1 ($\binom{2}{1}$–$\mathbf{OT}_2(b_0, b_1)(c)$)

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

- *Alice picks a random bit* $r_i \leftarrow$ Ⓒ
- *Alice picks a random bit* $\beta_i \leftarrow$ Ⓒ *and defines her emission basis* $(|\varphi_i\rangle, |\varphi_i^\perp\rangle) \leftarrow [\oplus, \boxtimes]_{\beta_i}$
- *Alice sends to Bob a photon* π_i *with polarization* $[|\varphi_i\rangle, |\varphi_i^\perp\rangle]_{r_i}$
- *Bob picks a random bit* $\beta'_i \leftarrow$ Ⓒ *and measures photon* π_i *in basis* $(|\theta_i\rangle, |\theta_i^\perp\rangle) \leftarrow [\oplus, \boxtimes]_{\beta'_i}$
- *Bob sets* $r'_i \leftarrow \begin{cases} 0 & \textit{if } \pi_i \textit{ is observed as } |\theta_i\rangle \\ 1 & \textit{if } \pi_i \textit{ is observed as } |\theta_i^\perp\rangle \end{cases}$

2: *Alice announces her choices* $\beta_1\beta_2...\beta_n$ *to Bob.*

3: *Bob randomly selects two subsets* $I_0, I_1 \subset \{1, 2, ..., n\}$ *subject to* $|I_0| = |I_1| = n/3$, $I_0 \bigcap I_1 = \emptyset$ *and* $\forall i \in I_0, \beta_i = \beta'_i$, *and he announces* $\langle I_c, I_{\overline{c}}\rangle$ *to Alice*

4: *Alice receives* $\langle J_0, J_1\rangle$, *computes and sends* $\hat{b}_0 \leftarrow b_0 \oplus \bigoplus_{j\in J_0} r_j$ *and* $\hat{b}_1 \leftarrow b_1 \oplus \bigoplus_{j\in J_1} r_j$

5: *Bob receives* $\langle \hat{b}_0, \hat{b}_1\rangle$ *and computes* $b_c \leftarrow \hat{b}_c \oplus \bigoplus_{j\in I_0} r'_j$

3.2 Intuition behind the protocol

Intuitively, random bits $r_1r_2...r_n$ are chosen by *Alice* in step 1 and are sent to *Bob* via an ambiguous coding referred to as the BB84 coding [1]: when *Alice* and *Bob* choose the same emission and reception basis, the bit received is the same as what was sent and uncorrelated otherwise. Given that *Bob* finds out *Alice*'s choices of bases at step 2, he can tell in which situation each bit was. *Bob* then builds two subsets: one I_0 that will allow him to get b_c, and one I_1 that will spoil $b_{\overline{c}}$. The calculations of steps 4–5 are such that all the bits in a subset *must be known* by *Bob* in order for him to be able to obtain the output bit connected to that subset.

4 Analysis

In the basic version of the protocol we make the strong assumption that $\mathcal{B}ob$ *must* read the photons sent by $\mathcal{A}lice$ *as they come*: he cannot wait and read them later, individually or together. We shall remove this assumption later. We also assume that the channel used for the quantum transmission is free of errors, so that it is guaranteed that $r_i' = r_i$ whenever $\beta_i' = \beta_i$. We now show that under these assumptions this protocol satisfies the statistical version of the above constraints.

4.1 Correctness

We show that most of the time the output is correct if the parties abide to their prescribed protocol. In a given run of the protocol, $\mathcal{B}ob$ will succeed in computing b_c properly provided $\#\{i|\beta_i = \beta_i'\} \geq n/3$ because in that case he can form I_0 as prescribed and then he can compute the output bit as $\hat{b}_c \oplus \bigoplus_{j\in I_0} r_j'$ which is

$$\hat{b}_c \oplus \bigoplus_{j\in I_0} r_j' = b_c \oplus \bigoplus_{j\in J_c} r_j \oplus \bigoplus_{j\in I_0} r_j' = b_c \oplus \bigoplus_{j\in I_0} r_j \oplus r_j'$$

because J_c is I_0. Since $\beta_i = \beta_i' \rightarrow r_j \oplus r_j' = 0$ makes all the right terms vanish, we end up with

$$\hat{b}_c \oplus \bigoplus_{j\in I_0} r_j' = b_c.$$

Therefore the protocol gives the correct output unless $\#\{i|\beta_i = \beta_i'\} < n/3$ in which case $\mathcal{B}ob$ is unable to form the set I_0 as prescribed. The probability of this event is given by

$$\mathbf{P}\left[\#\{i|\beta_i = \beta_i'\} < n/3\right] = \mathbf{P}\left[\sum_{i=1}^{n} \beta_i \oplus \beta_i' > 2n/3\right] \leq \mathbf{P}\left[|n/2 - \sum_{i=1}^{n} \beta_i \oplus \beta_i'| > n/6\right]$$

Given that $\mathbf{P}\left[\beta_i \oplus \beta_i' = 1\right] = \frac{1}{2}$ this earlier expression can be easily bounded by

$$\leq 2e^{-n/36} \leq (0.973)^n$$

using Bernstein's law of large numbers [15].

4.2 Privacy

We analyse the privacy of each party individually as if he or she were facing a malicious opponent.

4.2.1 Privacy for $\mathcal{B}ob$

In order to show the protocol private for $\mathcal{B}ob$ we show that no malicious $\tilde{\mathcal{A}}$ can find out information about c. Indeed we show that

Theorem 4.1 *For all H, b_0, b_1*

$$\boldsymbol{H}(c|V_{\tilde{\mathcal{A}}}(H, b_0, b_1, c)) = \boldsymbol{H}(c|H, b_0, b_1).$$

Proof. The only things $\tilde{\mathcal{A}}$ gets through the protocol are the sets J_0, J_1. Therefore we have that her final information is $V_{\tilde{\mathcal{A}}} = \langle H, b_0, b_1, J_0, J_1 \rangle$. Now notice that the distribution of J_0, J_1 depends only on the fact that the β_i's announced by $\tilde{\mathcal{A}}$ are or not the same as the β_i''s used by $\mathcal{B}ob$ and not at all on c. Since the β_i's are chosen randomly and independently by $\mathcal{B}ob$, J_0 and J_1 will have uniform distribution over all possible pairs of disjoint subsets of size $n/3$ for $c = 0$ as well as for $c = 1$. Therefore since $\tilde{\mathcal{A}}$ learns nothing about the β_i''s

$$\mathbf{H}(c|V_{\tilde{\mathcal{A}}}(H, b_0, b_1, c)) = \mathbf{H}(c|\langle H, b_0, b_1, J_0, J_1 \rangle) = \mathbf{H}(c|H, b_0, b_1).$$

4.1 ■

4.2.2 Privacy for *Alice*

Without loss of generality, since we assume that $\tilde{\mathcal{B}}$ is limited to making immediate measurements in each iteration of step 1, we might as well assume that he makes a complete Von Neumann measurement for some orthogonal basis $(|\theta_i\rangle, |\theta_i^\perp\rangle)$ since any gentler measurement would give him only lower success probability with respect to guessing r_i. We can therefore analyse only those $\tilde{\mathcal{B}}$ that follow such a strategy because other ones could not do better. We may also denote, without loss of generality, r_i' to be the result of his measurement as defined in step 1. Let $S_5(H, b_0, b_1, c)$ be $\tilde{\mathcal{B}}$'s information before step 5 of the protocol. By the end of the protocol he gets $V_{\tilde{\mathcal{B}}}(H, b_0, b_1, c) = \langle S_5(H, b_0, b_1, c), \hat{b}_0, \hat{b}_1 \rangle$. When no confusion arise we simply write S_5 and $V_{\tilde{\mathcal{B}}}$ instead of these complete expressions. Let m be such that

$$\left| \prod_{j \in J_m} (\|\langle \theta_j | [\leftrightarrow, \nearrow]_{\beta_j} \rangle\|^2 - 1/2) \right| \leq \left| \prod_{j \in J_{\overline{m}}} (\|[\langle \theta_j | [\leftrightarrow, \nearrow]_{\beta_j} \rangle\|^2 - 1/2) \right|. \qquad (1)$$

We show that

Theorem 4.2 *There exists a positive $\varepsilon < 1$ such that for all $H, c, b_{\overline{m}}$ we get*

$$\boldsymbol{H}(b_m|V_{\tilde{\mathcal{B}}}(H, b_0, b_1, c), b_{\overline{m}}) \geq \boldsymbol{H}(b_m|H, c, b_{\overline{m}}) - \varepsilon^n.$$

Proof.

$$\begin{aligned}
\mathbf{H}(b_m|V_{\tilde{\mathcal{B}}}, b_{\overline{m}}) &= \mathbf{H}(b_m|S_5, \hat{b}_0, \hat{b}_1, b_{\overline{m}}) \\
&= \mathbf{H}(b_m|S_5, \hat{b}_m, b_{\overline{m}}) \\
&\quad \text{Since } \hat{b}_{\overline{m}} \text{ contains solely imperfect information about } b_{\overline{m}}, \\
&\quad \text{it cannot be informative about } b_m \text{ in a way that } b_{\overline{m}} \text{ would not.} \\
&= \mathbf{H}(b_m|S_5, b_{\overline{m}}) + \mathbf{H}(b_m|S_5, \hat{b}_m, b_{\overline{m}}) - \mathbf{H}(b_m|S_5, b_{\overline{m}}) \\
&= \mathbf{H}(b_m|H, c, b_{\overline{m}}) + \mathbf{H}(b_m, S_5, \hat{b}_m, b_{\overline{m}}) - \mathbf{H}(S_5, \hat{b}_m, b_{\overline{m}}) - \mathbf{H}(b_m, S_5, b_{\overline{m}}) + \mathbf{H}(S_5, b_{\overline{m}}) \\
&\quad \text{the leftmost term is due to the fact that } b_0, b_1 \text{ are not used by } \mathcal{A}lice \text{ until step 5} \\
&= \mathbf{H}(b_m|H, c, b_{\overline{m}}) + \mathbf{H}(\hat{b}_m|S_5, b_0, b_1) - \mathbf{H}(\hat{b}_m|S_5, b_{\overline{m}})
\end{aligned}$$

Therefore it suffices to show

$$\mathbf{H}(\hat{b}_m|S_5, b_{\overline{m}}) - \mathbf{H}(\hat{b}_m|S_5, b_0, b_1) \leq \varepsilon^n.$$

For that purpose we compute

$$\mathbf{P}\left[\hat{b}_m = 0 \mid S_5, b_0, b_1\right] = \mathbf{P}\left[\bigoplus_{j\in J_m} r_j = b_m \middle| S_5, b_0, b_1\right]$$

We see that this is almost the same whatever b_m is:

$$\begin{aligned}
\mathbf{P}\left[\bigoplus_{j\in J_m} r_j = 0 \middle| S_5, b_0, b_1\right] &= \mathbf{P}\left[\bigoplus_{j\in J_m} r_j = 0 \middle| r'_1...r'_n\theta_1...\theta_n\beta_1...\beta_n\right] \\
&\quad \text{since the } r_i\text{'s are only dependent on the } r'_i\text{'s, } \theta_i\text{'s and } \beta_i\text{'s.} \\
&= \frac{1}{2} \pm \frac{1}{2}\left(\prod_{j\in J_m} 2\mathbf{P}\left[r'_j = r_j\right] - 1\right) \\
&\quad \text{the sign is "+" if } \bigoplus_{j\in J_m} r'_j = 0\text{, and it is "}-\text{" otherwise.} \\
&= \frac{1}{2} \pm \frac{1}{2}\left(\prod_{j\in J_m} 2\|\langle\theta_j|[\leftrightarrow, \nearrow]_{\beta_j}\rangle\|^2 - 1\right) \\
&\quad \text{since } \mathbf{P}\left[r'_j = r_j\right] = \|\langle\theta_j|[\leftrightarrow, \nearrow]_{\beta_j}\rangle\|^2.
\end{aligned}$$

We get the same result by setting $b_m = 1$ instead of 0 but with the opposite sign.
We conclude from this that for $b \in \{0, 1\}$

$$\left|\mathbf{P}\left[\hat{b}_m = b|S_5, b_0, b_1\right] - \frac{1}{2}\right| \leq \frac{1}{2}\left|\prod_{j\in J_m} 2\|\langle\theta_j|[\leftrightarrow, \nearrow]_{\beta_j}\rangle\|^2 - 1\right|$$

Now based on the fact that m was chosen so to satisfy equation (1) it suffices to show that

$$\left|\prod_{j\in J_0\cup J_1} 2\|\langle\theta_j|[\leftrightarrow, \nearrow]_{\beta_j}\rangle\|^2 - 1\right| \leq \alpha^n \tag{2}$$

for some $\alpha < 1$ to conclude that

$$\left|\prod_{j\in J_m} 2\|\langle\theta_j|[\leftrightarrow, \nearrow]_{\beta_j}\rangle\|^2 - 1\right| \leq \left(\sqrt{\alpha}\right)^n. \tag{3}$$

Finally to prove that claim we need the following easily proven fact:

Fact 4.3 *For any Von Neumann measurement* $(|\theta_j\rangle, |\theta_j^\perp\rangle)$ *at least one of the following holds*

$$\frac{\sqrt{2}-1}{2\sqrt{2}} \leq \|\langle\theta_j|\leftrightarrow\rangle\|^2 \leq \frac{\sqrt{2}+1}{2\sqrt{2}} \quad \textit{or} \quad \frac{\sqrt{2}-1}{2\sqrt{2}} \leq \|\langle\theta_j|\nearrow\rangle\|^2 \leq \frac{\sqrt{2}+1}{2\sqrt{2}}$$

This means that because the β_j are chosen at random, in each position j

$$\mathbf{P}\left[\left|2\|\langle\theta_j|[\leftrightarrow,\swarrow\!\!\!\nearrow]_{\beta_j}\rangle\|^2 - 1\right| \le \frac{1}{\sqrt{2}}\right] \ge \frac{1}{2}$$

Therefore the set of positions

$$\left\{j\ :\ \left|2\|\langle\theta_j|[\leftrightarrow,\swarrow\!\!\!\nearrow]_{\beta_j}\rangle\|^2 - 1\right| > \frac{1}{\sqrt{2}}\right\}$$

will have size no more than $\frac{7n}{12}$ except with probability bounded by $2e^{-n/144}$ by Bernstein's law of large number. In that case we have that equations (2) and (3) are satisfied with $\alpha = (\frac{1}{2})^{1/24}$. In conclusion, only with probability no more than $2e^{-n/144}$ will

$$\left|\mathbf{P}\left[\hat{b}_m = 0|S_5, b_0, b_1\right] - 1/2\right| > 2^{-n/48}$$

Therefore $\mathbf{H}(\hat{b}_m|S_5, b_0, b_1)$ will be roughly $1 - (\frac{1}{2})^{n/48}$ and since $\mathbf{H}(\hat{b}_m|S_5, b_0, b_1) \le \mathbf{H}(\hat{b}_m|S_5, b_{\overline{m}}) \le 1$ we conclude that for some positive $\varepsilon < 1$

$$\mathbf{H}(\hat{b}_m|S_5, b_{\overline{m}}) - \mathbf{H}(\hat{b}_m|S_5, b_0, b_1) \le \varepsilon^n.$$

4.2 ■

5 Relaxing our Assumption

In the above proof of privacy for *Alice* we had to make the strong assumption that $\tilde{\mathcal{B}}$ must make his measurements right away when he receives the photons. Of course from a theoretical point of view this assumption is quite unsatisfactory because $\tilde{\mathcal{B}}$ could in principle store the photons sent by *Alice* and wait until she discloses the bases before measuring them, which would allow him to obtain both of *Alice*'s bits with certainty.

However we describe next a variation of the protocol of section 3 that more or less forces $\tilde{\mathcal{B}}$ to make immediate measurements on the received photons. For this we use a *bit commitment scheme*. A bit commitment scheme goes as follows: Assume that *Bob* has a bit x in mind, to which he would like to be committed toward *Alice*. That is, *Bob* wishes, through a procedure *commit*(x), to provide *Alice* with a piece of evidence that he has a bit x in mind and that he cannot change it. Meanwhile, *Alice* should not be able to tell from that evidence what x is. At a later time, *Bob* can reveal, through a procedure *unveil*(x), the value of x and prove to *Alice* that the piece of evidence sent earlier really corresponded to that bit.

Recently Brassard, Crépeau, Jozsa and Langlois [5] have described a bit commitment scheme based on quantum physics that they have proved secure according to the rules of quantum mechanics. This formal proof was the first ever of the security of a cryptographic protocol based on quantum mechanics. Therefore *Bob* and *Alice* can use their quantum channel in the reverse direction to perform the bit commitment necessary for the $\binom{2}{1}$–OT_2 described next. As we will later see in section 6, it turns out that it can even be done without reversing the channel.

The idea behind this modified protocol is that each time $\mathcal{A}lice$ was sending a random r_i to $\mathcal{B}ob$ in the original protocol she now sends two random bits r_i, r_{n+i}. One of them will become r_i, while the other will be used to challenge the fact that $\mathcal{B}ob$ makes immediate measurements of the photons. $\mathcal{A}lice$ gets $\mathcal{B}ob$ to *commit* to the bits that he received and the bases that he used to measure them. Before going ahead with r_i, say, $\mathcal{A}lice$ checks that $\mathcal{B}ob$ had committed properly to r_{n+i} when he read that bit in the basis that she used to encode it. If at any stage $\mathcal{A}lice$ observes a mistake ($\beta_{n+i} = \beta'_{n+i}$ but $r_{n+i} \neq r'_{n+i}$), she stops further interaction with $\mathcal{B}ob$ who is definitely not performing his legal protocol (this should never happen if $\mathcal{B}ob$ follows his protocol). If $\mathcal{B}ob$ manages to keep $\mathcal{A}lice$ satisfied, he must be making immediate measurements that are very close to measuring along the standard bases. The modified protocol is:

Protocol 5.1 ($\binom{2}{1}$–$\mathbf{OT}_2(b_0, b_1)(c)$)

1: $\underset{i=1}{\overset{2n}{\mathbf{DO}}}$

- *$\mathcal{A}lice$ picks a random bit* $r_i \leftarrow$ ⓒ
- *$\mathcal{A}lice$ picks a random bit* $\beta_i \leftarrow$ ⓒ *and defines her emission basis* $(|\varphi_i\rangle, |\varphi_i^\perp\rangle) \leftarrow [\oplus, \boxtimes]_{\beta_i}$
- *$\mathcal{A}lice$ sends to $\mathcal{B}ob$ a photon* π_i *with polarization* $[|\varphi_i\rangle, |\varphi_i^\perp\rangle]_{r_i}$
- *$\mathcal{B}ob$ picks a random bit* $\beta'_i \leftarrow$ ⓒ *and measures photon* π_i *in basis* $(|\theta_i\rangle, |\theta_i^\perp\rangle) \leftarrow [\oplus, \boxtimes]_{\beta'_i}$
- *$\mathcal{B}ob$ sets* $r'_i \leftarrow \begin{cases} 0 & \textit{if } \pi_i \textit{ is observed as } |\theta_i\rangle \\ 1 & \textit{if } \pi_i \textit{ is observed as } |\theta_i^\perp\rangle \end{cases}$

1.5: $\underset{i=1}{\overset{n}{\mathbf{DO}}}$

- *$\mathcal{B}ob$ runs* $commit(r'_i), commit(\beta'_i)$, $commit(r'_{n+i}), commit(\beta'_{n+i})$ *with $\mathcal{A}lice$*
- *$\mathcal{A}lice$ picks* $c_i \leftarrow$ ⓒ *and announces it to $\mathcal{B}ob$*
- *$\mathcal{B}ob$ runs* $unveil(r'_{nc_i+i}), unveil(\beta'_{nc_i+i})$
- *$\mathcal{A}lice$ checks that* $\beta_{nc_i+i} = \beta'_{nc_i+i} \rightarrow r_{nc_i+i} = r'_{nc_i+i}$.
- ***if*** $c_i = 0$ ***then*** *$\mathcal{A}lice$ sets* $\beta_i \leftarrow \beta_{n+i}$ *and* $r_i \leftarrow r_{n+i}$ *and $\mathcal{B}ob$ sets* $\beta'_i \leftarrow \beta'_{n+i}$ *and* $r'_i \leftarrow r'_{n+i}$

2: *$\mathcal{A}lice$ announces ...*

3: *$\mathcal{B}ob$ randomly selects ...*

4: *$\mathcal{A}lice$ receives ...*

5: *$\mathcal{B}ob$ receives ...*

This modified protocol will clearly be as correct as the original since only a few checks are added but basically everything is computed just as before. As for the privacy, it remains just the same for $\mathcal{B}ob$ but things are a little tricky for $\mathcal{A}lice$. It is not completely clear that $\tilde{\mathcal{B}}$ could not adopt a strategy to read each photon with an incomplete measurement very close to the standard bases, but that allows him to *save* a little bit of the information in the photon π_i in such a way that he can later exploit that leftover information and the fact that he learns $\mathcal{A}lice$'s bases to gather significant information on both b_0 and b_1. This seems extremely unlikely since those measurements would have to be close enough to the standard ones so that $\mathcal{B}ob$ would still be able to satisfy $\mathcal{A}lice$'s checks, but such that the leftover information is still rather large. Unfortunately, at this time we do not have a complete proof that such a thing is impossible. Indeed, this problem is more or less equivalent to showing that the *quantum key distribution protocol* of Bennett and Brassard [2] cannot be attacked in a similar fashion.

6 Remarks

First, notice that the protocol can be used directly to implement a one-out-of-three Oblivious Transfer ($\binom{3}{1}$–OT$_2$) since at step 3 $\mathcal{B}ob$ could build three sets I_0, I_1 and I_2 of size $n/3$ instead of only the first two and thus receive one bit out of three. This may be useful in certain applications.

Also, it may seem a limitation that a Quantum Bit Commitment is used from $\mathcal{B}ob$ to $\mathcal{A}lice$ in the current protocol as it implies that the quantum channel is implemented in both directions. As a matter of fact, it is as easy to get a protocol that will have photons only flowing from $\mathcal{B}ob$ to $\mathcal{A}lice$ as suggested by the following variation of the protocol. Based on a simple observation of Louis Salvail, this protocol uses the fact that the distribution of the r_i''s and β_i''s with respect to the r_i's and β_i's is the same whether the photons flow from $\mathcal{A}lice$ to $\mathcal{B}ob$ or vice versa. This protocol is exactly the same as Protocol 5.1 except for the first step, which is accomplished in the reverse direction.

Protocol 6.1 ($\binom{2}{1}$**–OT**$_2(b_0, b_1)(c)$)

1: $\overset{2n}{\underset{i=1}{\textbf{\textit{DO}}}}$

- *$\mathcal{B}ob$ picks a random bit* $r_i' \leftarrow$ ©
- *$\mathcal{B}ob$ picks a random bit* $\beta_i' \leftarrow$ © *and defines his emission basis* $(|\theta_i\rangle, |\theta_i^\perp\rangle) \leftarrow [\oplus, \boxtimes]_{\beta_i'}$
- *$\mathcal{B}ob$ sends to $\mathcal{A}lice$ a photon* π_i *with polarization* $[|\theta_i\rangle, |\theta_i^\perp\rangle]_{r_i'}$
- *$\mathcal{A}lice$ picks a random bit* $\beta_i \leftarrow$ © *and measures photon* π_i *in basis* $(|\varphi_i\rangle, |\varphi_i^\perp\rangle) \leftarrow [\oplus, \boxtimes]_{\beta_i}$
- *$\mathcal{A}lice$ sets* $r_i \leftarrow \begin{cases} 0 & \textit{if } \pi_i \textit{ is observed as } |\varphi_i\rangle \\ 1 & \textit{if } \pi_i \textit{ is observed as } |\varphi_i^\perp\rangle \end{cases}$

...

The fact that the protocol for $\binom{2}{1}$–OT$_2$ in one direction is sufficient to accomplish the same protocol in the reverse direction has been established earlier in the literature by Crépeau and Sántha [11]. Therefore more elaborate protocols involving $\binom{2}{1}$–OT$_2$ in both directions can be implemented with photons flowing in a single direction.

7 Conclusion and Open Questions

We have presented in this paper a protocol for $\binom{2}{1}$–OT_2 based on quantum physics that is proven secure as long as the parties are not allowed to store photons or more precisely the quantum information they carry. We have also presented an improved protocol that apparently removes this restriction but it remains an open problem to provide a proof of this claim. Again, this open problem is very similar to the open problem of demonstrating the security of the *quantum key distribution protocol* of Bennett and Brassard [2] at very low error rates.

This paper has not considered the fact that the actual quantum channel [2] is not error-free and the fact that single photons are hard to generate. These problems are treated in [4].

Acknowledgements

I wish to thank Charles H. Bennett, Gilles Brassard, Artur Ekert, Richard Jozsa, Joe Kilian, Denis Langlois, Silvio Micali, Louis Salvail, Marie–Hélène Skubiszewska, and an anonymous referee for support, suggestions and comments at different stages of this work. I would also like to thank the Rank Foundation (England), the I.S.I. & Elsag-Baley (Italy), and the I.E.S.S. (Germany) for making possible the 1993 workshops on quantum information theory and quantum cryptography that made such research and the writing of this paper possible.

References

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

[2] Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. and Smolin, J., "Experimental quantum cryptography", *Journal of Cryptology*, vol. 5, 1992, pp. 3 – 28.

[3] Bennett, C. H., Brassard, G., Breidbart, S. and Wiesner, S., "Quantum cryptography, or unforgeable subway tokens", In *Proceedings of Crypto 82*, Plenum Press, 1982, pp. 267 – 275.

[4] Bennett, C. H., Brassard, G., Crépeau, C. and Skubiszewska, M.–H., "Practical quantum oblivious transfer", In *Advances in Cryptology: Proceedings of Crypto '91*, Lecture Notes in Computer Science, Vol. 576, pp. 351–366. Springer-Verlag, 1992.

[5] Brassard, G., Crépeau, C., Jozsa, R. and Langlois, D., "A quantum bit commitment scheme provably unbreakable by both parties", In *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science*, November 1993, pp. 362 – 371.

[6] Brassard, G., Crépeau, C. and Robert, J.–M., "Information theoretic reductions among disclosure problems", In *Proceedings of the 27th Annual IEEE Symposium on Foundations of Computer Science*, November 1986, pp. 168 – 173.

[7] Crépeau, C., "Equivalence between two flavours of oblivious transfers", In Advances in Cryptology: Proceedings of Crypto '87, Lecture Notes in Computer Science, August 1987, pp. 350 – 354.

[8] Crépeau, C., *Correct and Private Reductions among Oblivious Transfers*, Ph.D. Thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, February 1990.

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

[10] Crépeau, C. and Sántha, M., "Efficient reduction among oblivious transfer protocols based on new self-intersecting codes", In *Proceedings of Sequences 91: Methods in Communication, Security and Computer Science*, June 1991, pp. 360 – 368, Springer – Verlag.

[11] Crépeau, C. and Sántha, M., "On the reversibility of oblivious transfer", In *Advances in Cryptology: Proceedings of Eurocrypt '91*, volume 547 of *Lecture Notes in Computer Science*, pp. 106–113, Springer-Verlag, 1991.

[12] Even, S., Goldreich, O. and Lempel, A., "A randomized protocol for signing contracts", *Communications of the ACM*, vol. 28, 1985, pp. 637 – 647.

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

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

[15] Kranakis, E., *Primality and Cryptography*, Wiley–Teubner Series in Computer Science, 1986.

[16] Rabin, M. O., "How to exchange secrets by oblivious transfer", technical report tr–81, Aiken Computation Laboratory, Harvard University, 1981.

[17] Wiesner, S., "Conjugate coding", *Sigact News*, vol. 15, no. 1, 1983, pp. 78 – 88; Manuscript written *circa* 1970, unpublished until it appeared in SIGACT News.

[18] Yao, A. C.–C., "Protocols for secure computations", In *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science*, November 1982, pp. 160 – 164.