On the security of the quantum oblivious transfer and key distribution protocols

Dominic Mayers

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

Abstract. No quantum key distribution (QKD) protocol has been proved fully secure. A remaining problem is the eavesdropper's ability to make *coherent* measurements on the joint properties of large composite systems. This problem has been recently solved by Yao in the case of the security of a quantum oblivious transfer (QOT) protocol. We consider an extended OT task which, in addition to $\mathcal{A}$lice and $\mathcal{B}$ob, includes an eavesdropper $\mathcal{E}$ve among the participants. An honest $\mathcal{E}$ve is inactive and receives no information at all about Alice's input when $\mathcal{B}$ob and $\mathcal{A}$lice are honest. We prove that the security of a QOT protocol against $\mathcal{B}$ob implies its security against $\mathcal{E}$ve as well as the security of a QKD protocol.

1 Introduction

The goal of quantum cryptography is to design cryptographic protocols that are secure against unlimited quantum or classical computational power. At present, the quantum protocols that have been designed are commitment [BC, BCJL], oblivious transfer [Cr87, Cr94, BBCS, MS, Yao], key distribution [BB84, BBBSS, BBBW] and identification [CS]. Furthermore, prototypes for implementing some of these protocols have been built [BBBSS, MT, To94, TRT1, TRT2].

However, the full security of some of these protocols has not yet been proved. One of the difficulties in providing a full security proof is the cheaters' ability to execute *coherent* measurements on many photons at a time. At present, security against coherent measurements has been obtained in the case of commitment [BCJL] and bit oblivious transfer [Yao]. The security of QKD against coherent measurements has not yet been addressed in the literature and it is not clear whether the techniques used by Yao in [Yao] for a QOT protocol may be easily used for a QKD protocol. In any case, we do not use Yao's techniques. We show that the security against $\mathcal{B}$ob of a QOT protocol implies its security against eavesdropping and, as a corollary, the security of a key distribution protocol. The level of security against eavesdropping that we obtain for QOT (and QKD) depends upon the level of security of QOT against $\mathcal{B}$ob, and, in particular, full security against $\mathcal{B}$ob implies full security against eavesdropping.

The security of a QOT protocol against an eavesdroper is interesting in itself because it allows the protocol to be executed securely over a long quantum channel by an honest $\mathcal{A}$lice and an honest $\mathcal{B}$ob. The above implication works with a string QOT protocol, that is, a QOT protocol that transfers a string rather than only a single bit. The implication requires that the QOT protocol tolerates errors in the quantum channel and that the classical announcements in the QKD protocol are made on a faithful *public* channel between $\mathcal{A}$lice and $\mathcal{B}$ob. It does not require any unrealistic physical assumption such as zero error in the quantum channel.

2 The QOT protocol and the security of OT

There are two types of OT: the ordinary OT and the $\binom{1}{2}$-OT. We consider the string version of both types. In the ordinary OT, $\mathcal{A}$lice inputs a string s, $\mathcal{B}$ob receives a random bit $c \in \{0,1\}$ and, if $c = 0$, the string s. In the $\binom{1}{2}$-OT, $\mathcal{A}$lice inputs two string s_1 and s_2, $\mathcal{B}$ob inputs a bit c_B and receives the string s_{c_B}.

In this paper, from the security against $\mathcal{B}$ob and tolerance against errors of an ordinary QOT protocol, we obtain its security against $\mathcal{E}$ve and, as a corollary, the security of a QKD protocol. This is significant in particular because Yao has proved the security against $\mathcal{B}$ob of an ordinary QOT protocol [Yao].

2.1 The protocol

In the discussion below, a dishonest $\mathcal{B}$ob and a dishonest $\mathcal{E}$ve, have been included. Both appear in the same description, but the security of the protocol against any one of them is based upon the assumption that the other is inactive.

For $b, \theta \in \{0,1\}$, let $|b\rangle_\theta$ be the state of a photon polarized at $b \times 90 + \theta \times 45$ degrees. In the BB84 coding scheme, b is the bit coded in the state $|b\rangle_\theta$ and θ determines the basis used to code this bit: $\theta = 0$ corresponds to the basis $\{0°, 90°\}$ whereas $\theta = 1$ corresponds to the basis $\{45°, 135°\}$.

Protocol $OT(s)$

1 Honest $\mathcal{B}$ob: He chooses and commits to a *random* string $\hat{\theta} = (\hat{\theta}_1, \ldots, \hat{\theta}_{4n}) \in_R \{0,1\}^{4n}$.
Dishonest $\mathcal{B}$ob: He cannot gain any advantage from being dishonest at this step.

2 Until $4n$ pulses are detected by $\mathcal{B}$ob:

2.1 $\mathcal{A}$lice: She sends a pulse to $\mathcal{B}$ob in which a random bit is coded using a random base in the BB84 coding scheme.

2.2 Dishonest $\mathcal{E}$ve: She transfers some information from this pulse into her own quantum system and she uses that information to modify the residual state of the pulse which is sent to $\mathcal{B}$ob. The entire operation may be represented by a single unitary transformation on the product state of the photon and $\mathcal{E}$ve's system.

2.3 Let us assume that, thus far, $i-1$ pulses have been detected by an honest $\mathcal{B}$ob or declared as such by a dishonest $\mathcal{B}$ob.
Honest $\mathcal{B}$ob: He executes on this pulse a von Neumann measurement

in the basis $\hat{\theta}_i$ and, if the pulse is detected, he obtains a bit $\hat{b}_i$ that he commits to $\mathcal{A}$lice.

Dishonest $\mathcal{B}$ob: He executes a coherent measurement on this pulse and the previous pulses in order to determine:

- whether or not he declares this pulse as detected and, if he declares this pulse as detected,
- the bit $\hat{b}_i$ that he commits to $\mathcal{A}$lice.

Typically, $\mathcal{B}$ob executes an incomplete measurement.

The string of bits coded in these $4n$ detected pulses is $b \in_R \{0,1\}^{4n}$ and the associated string of bases is $\theta \in_R \{0,1\}^{4n}$.

3 $\mathcal{A}$lice: She chooses a random string $open \in_R \{0,1\}^{4n}$ and publicly announces it. For each i, if $open_i = 1$ she asks $\mathcal{B}$ob to open the commitments $\hat{\theta}_i$ and $\hat{b}_i$. She publicly announces the string $error$ where

$$error_i = \begin{cases} 1 \text{ if } \theta_i = \hat{\theta}_i \wedge b_i \neq \hat{b}_i \wedge open_i = 1 \\ 0 \text{ otherwise} \end{cases}$$

If $\#error$ and the number of undetected pulses (another kind of error) are not too large, the remainder of protocol is executed, and $\mathcal{P}ass$ is set to 1 otherwise $\mathcal{A}$lice refuses to continue and $\mathcal{P}ass$ is set to 0.

4 $\mathcal{A}$lice: She publicly announces the string $\theta = (\theta_1, \ldots, \theta_{4n})$.

5 Honest $\mathcal{B}$ob: He chooses a random bit c_B. He deterministically computes an ordered pair (e_0, e_1) such that $e_0 \cup e_1 = \{i | open_i = 0\}$, $|\#e_0 - \#e_1| \leq 1$ and

$$(\forall i \in e_{c_B})\, \theta_i = \hat{\theta}_i \quad \vee \quad (\forall i \in e_{\bar{c}_B})\, \theta_i \neq \hat{\theta}_i,$$

and publicly announces this ordered pair. For our proof, it is convenient to consider that $\mathcal{B}$ob's deterministic algorithm to compute (e_0, e_1) returns the same output if $\hat{\theta}$ and c_B are both complemented (this is easy to accomplish).

Dishonest $\mathcal{B}$ob: Having learnt the string θ, he executes a first post-test measurement of his choice and uses the outcome to compute an ordered pair (e_0, e_1) such that $e_0 \cup e_1 = \{i | open_i = 0\}$ and $|\#e_0 - \#e_1| \leq 1$, and publicly announces the ordered pair.

For all $d \in \{0,1\}$, the string coded by $\mathcal{A}$lice in e_d is denoted w_d.

6 $\mathcal{A}$lice: She chooses and publicly announces a random bit c_A and a hash function g from $\{0,1\}^{\#e_{c_A}}$ to $\{0,1\}^r$. The integer r is the length of the string to be sent via QOT. She also publicly announces $a = g(w_{c_A}) \oplus s$ and $Syn(w_{c_A})$, the syndrome of w_{c_A} which is needed by $\mathcal{B}$ob for error correction.

7 Honest $\mathcal{B}$ob: Let $c = c_A \oplus c_B$ (this is the c that appears in the description of the task). If $c = 0$, he uses $Syn(w_{c_A})$ to correct the error in $w_{c_B} = w_{c_A}$ and then he computes $s = g(w_{c_B}) \oplus a$.

Dishonest $\mathcal{B}$ob: Using the information obtained at step 6, he executes a second and final post-test measurement and obtains the outcome $j_{\mathcal{B}\text{ob}}$. This provides information about $s = a \oplus g(w_d)$, for $d = 0, 1$.

8 Dishonest $\mathcal{E}$ve: She measures her system and obtains the outcome $j_{\mathcal{E}\text{ve}}$. This provides information about $s = a \oplus g(w_d)$, for $d = 0, 1$.

We adopt the following notation: the random values $s, b, \theta, \hat{b}$, etc. associated with an execution of the protocol are values taken by random variables $S, B, \Theta, \hat{B}$, etc.

The remainder of the section contains the formal definitions of security that we use in our proof. As for the definition of security for $\binom{1}{2}$-*OT* found in [Cr94], our definitions are formulated in terms of the amount of information received by a given participant. Any initial information about s that may have this participant, $\mathcal{B}$ob in sections 2.2 and 2.4 and $\mathcal{E}$ve in section 2.3, corresponds to an apriori probability distribution on S which is implicit in our definitions.

Due to their relative complexity, we understand that the reader may have the impression that the following definitions are more complicated than necessary. However, these are the most simple and yet complete definitions that we could express in terms of mutual information. A more complete discussion on this subject, including a connection with definitions expressed in terms of statistical indistinguishability, will appear in another paper.

2.2 Security of *OT* against $\mathcal{B}$ob

Let $V_{\mathcal{B}\text{ob}}$ represents all the information received or generated by $\mathcal{B}$ob in the protocol. A *QOT* protocol is secure against $\mathcal{B}$ob if $(\exists \alpha > 0)(\exists n_0)$ such that, $(\forall n > n_0)$, for every $\mathcal{B}$ob, for every $\mathcal{C}$hannel, there exists a binary random variable $\tilde{C}$ (defined when $Pass = 1$) such that

$$I(S; V_{\mathcal{B}\text{ob}} | \tilde{C} = 1 \wedge Pass = 1) \times \Pr(Pass = 1) \leq 2^{-\alpha n} \quad (1)$$

$$\Pr(\tilde{C} = 1 | Pass = 1) = 1/2 \quad (2)$$

$$I(S; V_{\mathcal{B}\text{ob}} | Pass = 0) \times \Pr(Pass = 0) \leq 2^{-\alpha n} \quad (3)$$

$$I(S; \tilde{C}, Pass) \leq 2^{-\alpha n} \quad (4)$$

Let us remark that at step 5 a dishonest $\mathcal{B}$ob does not even have to choose a bit C_B. If $\mathcal{B}$ob does not choose a bit C_B, the bit $C = C_A \oplus C_B$ associated with an honest $\mathcal{B}$ob is meaningless. Therefore, in the above definition, $\tilde{C}$ has, in general, nothing to do with the bit C associated with an honest $\mathcal{B}$ob.

Statement 1 says that, if $\mathcal{B}$ob passes the test with a significant probability, then, in the context where $\mathcal{B}$ob passes the test and $\tilde{C} = 1$, $\mathcal{B}$ob learns almost nothing about S. Statement 2 says that, in the context where $\mathcal{B}$ob passes the test, $\tilde{C}$ is perfectly random. Statement 3 says that, if $\mathcal{B}$ob fails the test with a significant probability, then, in the context where $\mathcal{B}$ob fails the test, $\mathcal{B}$ob learns almost nothing about S. Statement 4 says that the information $(\tilde{C}, Pass)$, where $\tilde{C}$ is not given to $\mathcal{B}$ob in the protocol but could eventually be given to $\mathcal{B}$ob outside the protocol, says almost nothing about S.

2.3 Security of the extended *OT* against $\mathcal{E}$ve

Let $V_{\mathcal{E}\text{ve}}$ represents all the information that is available to an eavesdropper $\mathcal{E}$ve. The protocol is secure against $\mathcal{E}$ve, if $(\exists n_0)$ such that, $(\forall n > n_0)$, for every $\mathcal{C}$hannel, for every $\mathcal{E}$ve,

$$I(S; V_{\mathcal{E}\text{ve}}) \leq 2^{-\alpha n}.$$

2.4 Tolerance against errors in *OT*

The protocol is tolerant against errors (the tolerated error rate being indirectly specified by the test) if, $(\exists \alpha > 0)$ $(\exists n_0)$ such that, $(\forall n > n_0)$, for every $\mathcal{C}$hannel, if $\Pr(Pass = 1) > 2^{-\alpha n}$, then

$$I(S; V_{\mathcal{B}\mathrm{ob}} | C = 0 \wedge Pass = 1) > r - 2^{-\alpha n} \tag{5}$$

$$\Pr(C = 0 | Pass = 1) > 1/2 - 2^{-\alpha n} \tag{6}$$

where C is the bit that is received by an honest $\mathcal{B}$ob.

The condition $\Pr(Pass = 1) > 2^{-\alpha n}$ is needed because, if the expected rate of errors in the quantum channel is so high that the probability that $\mathcal{B}$ob passes the test is almost zero, then the protocol does not have to compensate for errors, even in the rare cases where $\mathcal{B}$ob does pass the test. Statement 5 says that, in the context where $C = 0$ and $\mathcal{B}$ob passes the test, $\mathcal{B}$ob must receive almost everything about the string S. This means that the protocol compensates for errors in the quantum channel. Statement 6 says that, in the context where $\mathcal{B}$ob passes the test, the bit C must almost be perfectly random.

3 From $\mathcal{B}$ob to $\mathcal{E}$ve

In this section we prove the following theorem.

Theorem 1. *The security against $\mathcal{B}$ob and tolerance against errors of the above protocol implies its security against $\mathcal{E}$ve.*

Looking ahead to an extension of this result to QKD, we shall be generous and assume that $\mathcal{E}$ve receives $\hat{\Theta}$ and C_B at the same time as she receives the pair (E_0, E_1) (which is thus redundant). The following general purpose lemma is useful.

Lemma 2. *Let $\mathcal{A}$, $\mathcal{B}$,$\mathcal{C}$ be any random variables. We have*

$$I(\mathcal{A};\mathcal{B}) = I(\mathcal{A};\mathcal{C}) + I(\mathcal{B};\mathcal{C}) - I(\mathcal{A},\mathcal{B};\mathcal{C}) + \sum_c I(\mathcal{A};\mathcal{B}|\mathcal{C} = c) \Pr(\mathcal{C} = c).$$

The proof is left to the reader. When we refer to this lemma, we say that the mutual information $I(\mathcal{A};\mathcal{B})$ is partitioned over $\mathcal{C}$. Note that, if $\mathcal{C}$ is a function of $\mathcal{B}$, we obtain $I(\mathcal{B}; C) = I(\mathcal{A},\mathcal{B};\mathcal{C}) = H(\mathcal{C})$ and, therefore,

$$I(\mathcal{A};\mathcal{B}) = I(\mathcal{A};\mathcal{C}) + \sum_c I(\mathcal{A};\mathcal{B}|\mathcal{C} = c) \Pr(\mathcal{C} = c).$$

Proof of Theorem 1. Let α and n_0 be the parameters for the security against $\mathcal{B}$ob. Let α' and n_0' be the parameters for the tolerance. Let $\alpha_m = Max\{\alpha, \alpha'\}$ and n_m be such that

$$r \times 2^{-(\alpha_m/3)n_m} < \frac{1}{6}. \tag{7}$$

We shall see that $n_0'' = Max\{n_0, n_0', n_m\}$ and $\alpha'' = \alpha_m/3$ are adequate parameters for the security against $\mathcal{E}$ve. Partitioning $I(S; V_{\mathcal{E}\text{ve}})$ over $Pass$ we obtain

$$\begin{aligned}
&I(S; V_{\mathcal{E}\text{ve}}) \\
&= I(S; V_{\mathcal{E}\text{ve}} | Pass = 0) \Pr(Pass = 0) \\
&\quad + I(S; V_{\mathcal{E}\text{ve}} | Pass = 1) \Pr(Pass = 1) \\
&\quad + I(S; Pass)
\end{aligned}$$

Using 3 and 4 and the fact that $V_{\mathcal{E}\text{ve}}$ is a subset of $V_{\mathcal{B}\text{ob}}$ we obtain

$$I(S; V_{\mathcal{E}\text{ve}}) = 2 \times 2^{-\alpha_m n} + I(S; V_{\mathcal{E}\text{ve}} | Pass = 1) \Pr(Pass = 1).$$

We only have to take care of the last term. Partitioning the last term over $C = C_A \oplus C_B$, we obtain

$$\begin{aligned}
&I(S; V_{\mathcal{E}\text{ve}} | Pass = 1) \Pr(Pass = 1) \\
&= \frac{1}{2} I(S; V_{\mathcal{E}\text{ve}} | C = 0) \Pr(Pass = 1) \\
&\quad + \frac{1}{2} I(S; V_{\mathcal{E}\text{ve}} | C = 1) \Pr(Pass = 1)
\end{aligned}$$

We now use the two following propositions.

Proposition 3. *For every $\mathcal{E}$ve, for every $\mathcal{C}$hannel,* $(\forall n > n_0'')$,

$$I(S; V_{\mathcal{E}ve} | C = 1) \times \Pr(Pass = 1) \leq 2^{-\alpha'' n}.$$

Proposition 4. *For every $\mathcal{E}$ve, for every $\mathcal{C}$hannel,* $(\forall n > n_0'')$,

$$I(S; V_{\mathcal{E}ve} | C = 0) \times \Pr(Pass = 1) \leq 2^{-\alpha'' n}.$$

Using propositions 3 and 4 we obtain the security against $\mathcal{E}$ve. We shall prove these propositions in the remainder of this section.

Proof of Proposition 3. Let us consider any integer $n > n_0''$, any $\mathcal{C}$hannel and any $\mathcal{E}$ve. Let us consider a $\mathcal{B}$ob that executes $\mathcal{E}$ve's actions in addition to his honest actions. Because $V_{\mathcal{E}\text{ve}}$ is a subset of $V_{\mathcal{B}\text{ob}}$, it will be enough to show that

$$I(S; V_{\mathcal{B}\text{ob}} | C = 1) \times \Pr(Pass = 1) \leq 2^{-\alpha'' n}.$$

The basic idea of the proof is simply that, because tolerance against error implies that $\mathcal{B}$ob must receive S each time that $C = 0$ and security against $\mathcal{B}$ob implies that he cannot receive S more than half of the time, then $\mathcal{B}$ob cannot receive S when $C = 1$. The remainder of the proof expresses this idea more formally in a way that takes care of additional points related to the test. By contradiction, let us assume that

$$I(S; V_{\mathcal{B}\text{ob}} | C = 1) \times \Pr(Pass = 1) > 2^{-\alpha'' n} = 2^{-(\alpha_m/3)n}.$$

This implies

$$Pr(Pass = 1) > (1/r)2^{-(\alpha_m/3)n} \tag{8}$$

and

$$I(S; V_{\mathcal{B}\mathrm{ob}}|C = 1) > 2^{-(\alpha_m/3)n} \tag{9}$$

To obtain the contradiction, we show that

$$I(S; V_{\mathcal{B}\mathrm{ob}}|Pass = 1) \geq (r/2) + \frac{11}{24}2^{-(\alpha_m/3)n} \tag{10}$$

and

$$I(S; V_{\mathcal{B}\mathrm{ob}}|Pass = 1) < (r/2) + \frac{6}{24}2^{-(\alpha_m/3)n}. \tag{11}$$

First, we show 10. If we partition $I(S; V_{\mathcal{B}\mathrm{ob}}|Pass = 1)$ over C, we obtain

$$\begin{aligned} & I(S; V_{\mathcal{B}\mathrm{ob}}|Pass = 1) \\ & \geq \frac{I(S; V_{\mathcal{B}\mathrm{ob}}|C = 1)}{2} \\ & \quad + \frac{I(S; V_{\mathcal{B}\mathrm{ob}}|C = 0)}{2}. \end{aligned}$$

Formula 7 and 8 give us $\Pr(Pass = 1) > 2^{-\alpha_m n}$ which is the required hypothesis in tolerance against errors. Formula 5 and 6 give us that

$$I(S; V_{\mathcal{B}\mathrm{ob}}|C = 0) \Pr(C = 0|Pass) > (r/2) - (r + \frac{1}{2})2^{-\alpha_m n}. \tag{12}$$

Using equation 9, we obtain

$$I(S; V_{\mathcal{B}\mathrm{ob}}|C = 1) \Pr(C = 0|Pass) \geq \frac{1}{2}2^{-(\alpha_m/3)n}. \tag{13}$$

Summing inequalities 12 and 13, one easily obtain 10. Now, we show 11. Let $\tilde{C}$ be the random bit whose existence is required by the security against $\mathcal{B}$ob. Partitioning $I(S; V_{\mathcal{B}\mathrm{ob}}|Pass = 1)$ over $\tilde{C}$ and using 2, we obtain

$$\begin{aligned} & I(S; V_{\mathcal{B}\mathrm{ob}}|Pass = 1) \\ & = \frac{I(S; V_{\mathcal{B}\mathrm{ob}}|\tilde{C} = 0 \wedge Pass = 1)}{2} \\ & \quad + \frac{I(S; V_{\mathcal{B}\mathrm{ob}}|\tilde{C} = 1 \wedge Pass = 1)}{2} \\ & \quad + I(S; \tilde{C}|Pass = 1) \end{aligned}$$

Clearly,

$$\frac{I(S; V_{\mathcal{B}\mathrm{ob}}|\tilde{C} = 0 \wedge Pass = 1)}{2} \leq \frac{r}{2}. \tag{14}$$

Also, using 1, we obtain

$$\frac{I(S; V_{\mathcal{B}\mathrm{ob}}|\tilde{C} = 1 \wedge Pass = 1)}{2} \Pr(Pass = 1) < \frac{1}{2}2^{-\alpha_m n}.$$

from which, using 8, we get

$$\frac{I(S;V_{\mathcal{B}\text{ob}}|\tilde{C}=1\wedge Pass=1)}{2} < \frac{r}{2}2^{-(2\alpha_m/3)n} \leq \frac{1}{12}2^{-(\alpha_m/3)n}. \qquad (15)$$

Now, partitioning $I(S;\tilde{C},Pass)$ over $Pass$, we obtain that

$$I(S;\tilde{C},Pass) \geq I(S;\tilde{C}|Pass=1)\Pr(Pass=1).$$

Therefore, using 8 and 4, we obtain

$$I(S;\tilde{C}|Pass=1)\frac{2^{-(\alpha_m/3)n}}{r} \leq 2^{-\alpha_m n}$$

which implies

$$I(S;\tilde{C}|Pass=1) \leq r2^{-(2\alpha_m/3)n} \leq \frac{1}{6}2^{-(\alpha_m/3)n}. \qquad (16)$$

Summing inequalities 14, 15 and 16, one easily obtains 11. This concludes the proof of proposition 3.

To prove proposition 4, the following lemma is useful.

Lemma 5. *Let $\mathcal{A}$, $\mathcal{B}$,$\mathcal{C}$ and $\mathcal{D}$ be any random variables such that $\mathcal{C}$ is a function of $\mathcal{D}$. For every d, we have*

$$I(\mathcal{A};\mathcal{B},\mathcal{C}|\mathcal{D}=d) = I(\mathcal{A};\mathcal{B}|\mathcal{D}=d).$$

The proof of this lemma is left to the reader.

Proof of Proposition 4. Let us consider any $n > n_0''$, any eavesdropper $\mathcal{E}\text{ve}_0$ and any channel $\mathcal{C}$hannel. Our proof consists of finding an eavesdropper $\mathcal{E}\text{ve}_1$ such that

$$I(S^{(1)};V_{\mathcal{E}\text{ve}}^{(1)}|C^{(1)}=1) = I(S^{(0)};V_{\mathcal{E}\text{ve}}^{(0)}|C^{(0)}=0),$$

where the upper index (i) on a random variable means that it is associated with the eavesdropper $\mathcal{E}\text{ve}_i$. Let

$$X = (Open,\hat{\Theta},C_B),$$

$$U = (B,\Theta,E_0,E_1,C_A,G,S),$$

$$Y = (Error,J_{\mathcal{E}\text{ve}})$$

and

$$Z = (\Theta,Error,C_A,G,Syn(W_{C_A}),A,J_{\mathcal{E}\text{ve}}).$$

Note that $\mathcal{E}$ve's view on the execution is $V_{\mathcal{E}\text{ve}} = (X,Z)$. Let F be the transformation that maps $x = (open,\hat{\theta},c_B)$ into $x' = (open,\hat{\theta}',\bar{c}_B)$ where

$$\hat{\theta}_i' = \begin{cases} \hat{\theta}_i & \text{if } open_i = 1 \\ \hat{\theta}_i \oplus 1 & \text{if } open_i = 0 \end{cases}.$$

Let $p_n = \Pr(X = x) = \frac{1}{2\times 4^{4n}}$. For every $\mathcal{E}\mathrm{ve}_1$, using a partition over X and the relation $I(S, X|C = c) = 0$ to obtain the first equality, lemma 5 to obtain the second equality and the bijectivity of F on X to obtain the third equality, we have:

$$\begin{aligned}
&I(S^{(1)}; V^{(1)}_{\mathcal{E}\mathrm{ve}}|C^{(1)} = 1)\\
&= \sum_x I(S^{(1)}; V^{(1)}_{\mathcal{E}\mathrm{ve}}|X^{(1)} = x \wedge C^{(1)} = 1) \times p_n\\
&= \sum_x I(S^{(1)}; Z^{(1)}|X^{(1)} = x \wedge C^{(1)} = 1) \times p_n\\
&= \sum_x I(S^{(1)}; Z^{(1)}|X^{(1)} = F(x) \wedge C^{(1)} = 1) \times p_n
\end{aligned}$$

Similarly, we have

$$\begin{aligned}
&I(S^{(0)}; V^{(0)}_{\mathcal{E}\mathrm{ve}}|C^{(0)} = 0)\\
&= \sum_x I(S^{(0)}; Z^{(0)}|X^{(0)} = x \wedge C^{(0)} = 0) \times p_n
\end{aligned}$$

Note that (S, Z) is a function of (U, Y). Therefore, we are done if we may define $\mathcal{E}\mathrm{ve}_1$'s strategy at steps 2 and 8 such that the distribution of $(U^{(0)}, Y^{(0)})$ given $(X, C)^{(0)} = (x, 0)$ is identical to the distribution of $(U^{(1)}, Y^{(1)})$ given $(X, C)^{(1)} = (F(x), 1)$. Let us consider an execution under $\mathcal{E}\mathrm{ve}_0$ where $(X, C)^{(0)} = (x, c)$ and an execution under $\mathcal{E}\mathrm{ve}_1$ where $(X, C)^{(1)} = (F(x), \bar{c}) = F(x, c)$. For every $\mathcal{E}\mathrm{ve}_1$'s strategy, because $\mathcal{A}$lice acts exactly in the same way in both executions and U is invariant under F, we have that $U^{(0)}$ in $\mathcal{E}\mathrm{ve}_0$ execution is identical to $U^{(1)}$ in $\mathcal{E}\mathrm{ve}_1$ execution. Now, we fix the value of U and consider the random variable Y. We must construct $\mathcal{E}\mathrm{ve}_1$'s strategy such that the distribution of $Y^{(0)}$ given $(U, X, C)^{(0)} = (u, x, c)$ is the same as the distribution of $Y^{(1)}$ given $F(U, X, C)^{(1)} = (u, x, c)$. At step 2, we define $\mathcal{E}\mathrm{ve}_1$ such that she executes the same transfer of information as $\mathcal{E}\mathrm{ve}_0$. This is a natural choice because, at this step, (Y, C) is unknown and $\mathcal{E}\mathrm{ve}_1$ cannot make use of the difference between the above conditions. We obtain that the random variable *Error* behaves in the same way in both executions because

- $\mathcal{B}$ob's outcomes at positions that are used for the test are independent of $\mathcal{B}$ob's choice of bases at positions that are not used for the test and
- $\mathcal{E}\mathrm{ve}_1$ has tampered the photons in the same way as $\mathcal{E}\mathrm{ve}_0$.

We now fix the value of *Error*. At step 8, $\mathcal{E}\mathrm{ve}_1$ with the view $V^{(1)}_{\mathcal{E}\mathrm{ve}}$ executes what $\mathcal{E}\mathrm{ve}_0$ executes with the view $F(V^{(1)}_{\mathcal{E}\mathrm{ve}}) = V^{(0)}_{\mathcal{E}\mathrm{ve}}$. In other words, in these two distinct executions, $\mathcal{E}\mathrm{ve}_0$ and $\mathcal{E}\mathrm{ve}_1$ act in exactly the same way. The distribution of the random variable $J_{\mathcal{E}\mathrm{ve}}$ must be the same in both case, because they have executed the same transfer of information and the same measurement, and $\mathcal{A}$lice has sent the same state. This concludes the proof of proposition 4 and theorem 1.

4 Security of QKD

The QKD protocol is exactly the QOT protocol, where $\mathcal{B}$ob announces $\hat{\Theta}$ and C_B, and $\mathcal{A}$lice always chooses $C = 0$ ($C_A = C_B$). The security of this QKD protocol is a direct consequence of proposition 4.

5 Conclusion

In this paper, we have shown that the security of an *ordinary* QOT protocol and its tolerance against error implies its security against eavesdropping and, as a corollary, the security of a QKD protocol. In the $\binom{1}{2}$-OT case, security against an eavesdropper means that, if $\mathcal{A}$lice and $\mathcal{B}$ob are honest, $\mathcal{E}$ve cannot find out anything new about (s_1, s_2). A $\binom{1}{2}$-QOT protocol is similar to an ordinary OT protocol, except that $\mathcal{A}$lice transfers two random strings w_0 and w_1 using the sets e_0 and e_1 respectively. One may wonder, if we could obtain the security against eavesdropping of a $\binom{1}{2}$-QOT protocol via a similar approach. This would be interesting because, if efficiency is a concern, the $\binom{1}{2}$-OT task is more powerful than the ordinary OT task: one execution of a $\binom{1}{2}$-OT protocol is enough to construct an ordinary OT protocol, but Kn executions of an ordinary OT protocol, for some $K > 0$, is required to construct a $\binom{1}{2}$-OT protocol [Cr87].

Unfortunately, there is an additional problem in the $\binom{1}{2}$-OT case which is related to the fact that $\mathcal{E}$ve may be aware of some correlation between s_1 and s_2 before the protocol begins. This correlation becomes a correlation between w_0 and w_1 at the time $\mathcal{E}$ve measures her system and, in principle, this may help her to execute a better measurement. In a more elaborate version of this paper, we shall provide a proof for the $\binom{1}{2}$ case where s_1 and s_2 are independent in $\mathcal{E}$ve's initial information.

It would have been reasonnable to better explain our formal definitions of security that appear in section 2. Ideally, we should have explained the connection between these definitions and previous definitions found in the literature such as those found in [Cr90]. As mentioned before, an analysis of these definitions will be presented in a subsequent paper.

Finally, now that we know that security may be obtained, it will be useful to determine the maximal error rate that can be tolerated and, for a given error rate, how much resource is required to guarantee a desired level of security. We need this information to find out what kind of technology is required to realize quantum protocols that are efficient and secure. To our knowledge, some theoretical work remains yet to be done at this level, at the least for QOT and QKD.

Acknowledgement

The author gratefully acknowledge fruitful discussions with Charles Bennett, Gilles Brassard, Claude Crépeau and Louis Salvail, and the support of the Institute for Scientific Interchange at Torino under whose auspice much of this work was done. This research was partially supported by Québec's FCAR.

References

[BB84] C.H. Bennett, G. Brassard, Quantum Cryptography: Public key distribution and coin tossing, *Proc. of IEEE International Conference on Computers, Systems, and Signal Processing*, Banglore, India, December 1984, pp. 175 – 179.

[BBBSS] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Experimental quantum cryptography, *Journal of Cryptology*, vol. 5, no. 1, 1992, pp. 3 – 28. Previous version in *Advances in Cryptology* — Eurocrypt '90 Proceeding, May 1990, Springer – Verlag, pp. 253 – 265.

[BBBW] C.H. Bennett, G. Brassard, S. Breidbart and S. Wiesner, Quantum cryptography, or unforgeable subway tokens, *Advances in Cryptology*: Crypto '82 Proceeding, August 1982, Plenum Press pp. 267 – 275.

[BBCS] C.H. Bennett, G. Brassard, C. Crépeau, M.-H. Skubiszewska, Practical Quantum Oblivious Transfer, In *proceedings of CRYPTO'91*, Lecture Notes in Computer Science, vol. 576, Springer – Verlag, Berlin, 1992, pp. 351 – 366.

[BC] G. Brassard and C. Crépeau, Quantum bit commitmemt and coin tossing protocols, in *Advances in Cryptology: Proceeding of CRYPTO'90*, Lecture Notes in Computer Science, vol. 537, Springer – Verlag, Berlin, 1991, pp. 49 – 61.

[BCJL] G. Brassard, C. Crépeau, R. Jozsa, D. Langlois, A quantum bit commitment scheme provably unbreakable by both parties, in *Proceeding of the 34th annual IEEE Symposium on Foundations of Computer Science*, November 1993, pp. 362 – 371.

[Cr87] C. Crépeau, Equivalence Between Two Flavors of Oblivious Transfers, *Advances in Cryptology* — Crypto '87 Proceeding, August 1987, Springer – Verlag, pp. 350 – 354.

[Cr90] C. Crépeau, Correct and Private Reductions among Oblivious Transfers, Ph.D. Thesis, Massachusetts Institute of Technology, 1990.

[Cr94] C. Crépeau, Quantum oblivious transfer, *Journal of Modern Optics*, vol. 41, no. 12, December 1994, pp. 2445 – 2454.

[CS] C. Crépeau, and L. Salvail, Quantum Oblivious Mutual Identification, *Advances in Cryptology: Proceedings of Eurocrypt'95*, May 1995, Springer – Verlag, to appear.

[MS] D. Mayers and L. Salvail, Quantum Oblivious Transfer is Secure Against All Individual Measurements, *Proceedings of the workshop on Physics and Computation*, PhysComp '94, Dallas, Nov 1994, pp. 69 – 77.

[MT] Marand, C. and P. Townsend, Quantum key distribution over distances up to 30km, *Optics Letters*, to appear.

[To94] P.D. Townsend, Secure key distribution system based on quantum cryptography, *Electronics Letters*, Vol. 30, no. 10, 12 May 1994.

[TRT1] P.D. Townsend, J.G. Rarity and P.R. Tapster, Single pulse interference in a 10 km long optical fibre interferometer, *Electronics Letters*, vol. 29, no. 7, 1 April 1993, pp. 634 – 635.

[TRT2] P.D. Townsend, J.G. Rarity and P.R. Tapster, Enhanced single photon fringe visibility in a 10 km-long prototype quantum cryptography channel, *Electronics Letters*, vol. 29, no. 14, 8 July 1993, pp. 1291 – 1293.

[Yao] A. Yao, Security of Quantum Protocols Against Coherent Measurements, in *Proceedings of the 26th Symposium on the Theory of Computing*, June 1995, to appear.

This article was processed using the LaTeX macro package with LLNCS style