Quantum Oblivious Transfer is Secure Against all Individual Measurements

D. Mayers*
DIRO
Université de Montréal
Montréal, H3C-3J7

L. Salvail†
DIRO
Université de Montréal
Montréal,H3C-3J7

Abstract

In this paper we show that the BBCS-protocol implementing one of the most important cryptographic primitives oblivious transfer, *is secure against any individual measurement allowed by quantum mechanics. We analyze the common situation where successive measurements on the same photon could be used to cheat in the protocol. We model this situation by using a single inner-product-preserving operator (IPP) followed by a complete composite outcome Von Neumann measurement. A lower bound on the residual collision entropy is then obtained under the assumption that only individual measurements can be performed. This bound is used to apply privacy amplification techniques in order to conclude the security of the BBCS-protocol.*

1 Introduction

With the advent of quantum cryptography, a practical application of quantum information theory has now appeared. Quantum cryptography, like computational complexity based cryptography, seeks to implement the few main primitives sufficient to build almost all complex cryptographic tasks. Working prototypes for some of these primitives have been built and practical applications are being considered [BBBSS, TRT1, TRT2]. However, the full proof of the security of some of these primitives against any attack allowed by quantum mechanics is still missing and this consitutes an interesting and practical challenge for quantum information theorists and cryptographers.

It is a well-known fact that *Oblivious Transfer* is a primitive sufficient for the realization of any cryptographic protocol involving two parties [Ki]. *Oblivious Tranfer* allows one party $\mathcal{A}$lice to send a string $\beta \in \{0,1\}^l$ in such a way that $\mathcal{B}$ob will receive it with probability $\frac{1}{2}$ and will know whether he received it or not. $\mathcal{A}$lice knows nothing about what happened to her string.

The BBCS-protocol [BBCS] implements this primitive in the quantum model. In the first part of this protocol, $\mathcal{A}$lice sends to $\mathcal{B}$ob photons polarized using either the rectilinear or the diagonal basis to encode some bits. A secure realisation of oblivious transfer in the continuation of the protocol relies on the fact that if $\mathcal{B}$ob measures these photons at this point he cannot obtain too much information about the bits because he does not know which of the two basis has been used. However, for the continuation $\mathcal{A}$lice must announce all the bases used to send the photons. The obvious problem with the security of this protocol is that, if $\mathcal{B}$ob does not measure the photons and stores them until he learns the bases, then he can obtain all the information about the bits. In that case the overall protocol becomes totally insecure. We refer to the case where $\mathcal{B}$ob does not measure the photons and store them as the photon-storing attack.

To protect $\mathcal{A}$lice against the photon-storing attack the original BBCS-protocol can be modified slightly ([Cr]). The modification is very simple. Before she announces the bases, $\mathcal{A}$lice simply ask $\mathcal{B}$ob to commit the outcome of his measurement as well as the basis that he used. Next, $\mathcal{A}$lice with probability one half requests $\mathcal{B}$ob to open this commitment. If $\mathcal{B}$ob does not read the photon, he will fail $\mathcal{A}$lice's test with probability one quarter, that is, each time he commits the correct basis, but the wrong bit.

To prove the security of this protocol, one needs to consider how much information can be obtained by $\mathcal{B}$ob about the bits. Usually, quantum information theorists use Shannon entropy to measure the amount of ignorance that remains about a quantum system af-

*Supported by Québec FCAR.
e-mail adress mayersd@iro.umontreal.ca.
†Supported by an NSERC scholarship.
e-mail address salvail@iro.umontreal.ca.

0-8186-6715-X/94 $4.00 © 1994 IEEE

ter a measurement. However, to prove the security of the BBCS-protocol and of other similar protocols, the work of [BBCM] have established that another measure of entropy, the collision entropy, turns out to be more adequate. The collision entropy of a distribution of probability f on a set X is simply given by the formula $H_c(f) = -\log \sum_{x \in X} f(x)^2$. Their work implies that a necessary condition to obtain the security of the BBCS-protocol is that $\mathcal{B}$ob must have some amount of collision entropy about the bits that he received. Thus far this condition has been obtained given the following assumption

Assumption 1 *Every measurement is complete.*

Obviously quantum mechanics allows measurements that do not respect this assumption. Assumption 1 means that $\mathcal{B}$ob either executes a complete measurement on the photon before he learns the basis or else executes the photon-storing attack.

If we remove assumption 1, $\mathcal{B}$ob may execute an incomplete measurement, obtain just enough information to pass $\mathcal{A}$lice's test and then store the residual state until he learns the basis. One can see that whereas it is clear that the new protection is sufficient to ensure the security of the protocol against the ordinary photon-storing attack, this is less obvious if we consider the storage of incompletely measured photons.

The difficulty in analysing this situation lies more at the formal level than at the intuitive level. Intuitively, for a given basis used by $\mathcal{A}$lice, if an outcome of the pre-basis measurement provides a lot of information about the initial state, then in the other basis it significantly "disturbs" this state and does not provide much information. Now, each time $\mathcal{B}$ob commits the same basis than $\mathcal{A}$lice uses, $\mathcal{B}$ob must obtain a lot of information about the bit from the pre-basis measurement. However, $\mathcal{B}$ob does not know which basis is chosen by $\mathcal{A}$lice, therefore, half of the time $\mathcal{B}$ob must disturb the initial state and, in these cases, both the pre-basis and the post-basis measurement do not provide much information. This allows us to obtain the desired lower bound for $\mathcal{B}$ob's total collision entropy. The most straightforward approach to formalize the above discussion, in particular the concept of disturbance, in the context of the most general attack allowed by quantum mechanics, is to use the model for generalised measurements that is described in [Ma]. Using this model and building on the work of [Cr], [BBCM] and [MC], our contribution is to show that with the protection against photon-storing the protocol is secure under the following assumption:

Assumption 2 *Every measurement is performed on individual photons.*

The case of coherent measurements (i.e., removing assumption 2), in a context where assumption 1 is removed, remains unsolved and is the missing piece in the full proof of the security of the scheme.

2 The BBCS Oblivious Transfer Protocol

2.1 Preliminaries

In the following, $x \in_R X$ denotes a uniformly distributed random element of X. For $a, b \in \{0,1\}^n$, $a \oplus b$ for is the bit by bit exclusive-or of the strings a and b.

We denote by $+ = (|\leftrightarrow\rangle, |\updownarrow\rangle)$ respectively and $\times = (|\nearrow\rangle, |\nwarrow\rangle)$ the bases for the rectilinear ("+") and diagonal ("×") polarizations in the quantum space of a photon. The [BB84] coding scheme works as follows:

$$|0\rangle_\theta = \begin{cases} \leftrightarrow & \text{if } \theta = + \\ \nearrow & \text{if } \theta = \times \end{cases}$$

and similarly

$$|1\rangle_\theta = \begin{cases} \updownarrow & \text{if } \theta = + \\ \nwarrow & \text{if } \theta = \times. \end{cases}$$

For our purpose, an *n-bit commitment* is a black box primitive defined by

Definition 1 *An n*-bit commitment *allows the committer $\mathcal{B}$ob to commit to the value of a n-bit string in a way that prevents the receiver $\mathcal{A}$lice from learning it without his help. In addition, $\mathcal{B}$ob cannot change the values of these bits without being detected by $\mathcal{A}$lice.*

This primitive can be implemented securely in the quantum model against any measurements allowed by quantum mechanics [BCJL]. Thus we can use *n-bit commitment* as a "black box" exactly matching the properties given in definition 1. We use the particular case of *2-bit commitment* and we denote such a commitment by $c = (x, y)$ for $x, y \in \{0,1\}$.

2.2 The BBCS-protocol

In this section, we sketch the version of the BBCS-protocol which includes the protection against incomplete measurements. The first part uses the quantum channel. The second part is the additionnal protection (it may also require the quantum channel if quantum commitments are used). The third part consists of a classical exchange of information using a public channel. The three are executed sequentially one after the other.

The Quantum Part. First, $\mathcal{A}$lice sends $4n$ photons encoding $4n$ bits using the [BB84] encoding rules. For all $i \in \{1, \ldots, 4n\}$, let $|b_i\rangle_{\theta_i}$ be the quantum state that is sent to represent the bit b_i in the basis θ_i. $\mathcal{B}$ob then chooses a random basis $\widehat{\theta}_i$, measures the quantum state $|b_i\rangle_{\theta_i}$ for all $i \in \{1, \ldots, 4n\}$ and obtains $|\widehat{b}_i\rangle_{\widehat{\theta}_i}$.

The protection. The idea is very simple and consists of requiring for $\mathcal{B}$ob to produce, for each photon π_i sent by $\mathcal{A}$lice, a commitment $c_i = (\widehat{\theta}_i, \widehat{b}_i)$ containing the basis $\widehat{\theta}_i$ and the corresponding bit $\widehat{b}_i$ resulting from that measurement. Independantly for each of these positions i, $\mathcal{A}$lice flips a coins, if a head is obtained then she asks $\mathcal{B}$ob to open c_i. In that case she verifies that

$$\widehat{\theta}_i = \theta_i \Rightarrow \widehat{b}_i = b_i. \tag{1}$$

Finally, $\mathcal{A}$lice verifies that relation 1 has not been violated more than a fraction δ of the time. The value δ is a security parameter slightly above the maximum error rate a particular implementation of the protocol can support. If the verification is succesful, then $\mathcal{A}$lice announces all the θ_i's and the classical part of the BBCS-protocol is executed with the N bits b_i for which c_i has not been opened. Since the commitments are perfectly secure, $\mathcal{A}$lice has no clue whether of I_s or I_{1-s} is I_0.

The Classical Part. The θ_i allow $\mathcal{B}$ob to recognize which positions i are measured in the correct basis (i.e. $\widehat{\theta}_i = \theta_i$) and which bits $\widehat{b}_i$ match b_i with probability at least $1-\delta$ where δ is an upper bound for the error rate of the quantum channel. Using this information $\mathcal{B}$ob can determine two sets $I_0 = \{i|\theta_i = \widehat{\theta}_i\}$ and $I_1 = \{i|\theta_i \neq \widehat{\theta}_i\}$ from which some arbitrary elements can be added or removed in order to get $\#I_0 = \#I_1 = \lfloor \frac{N}{2} \rfloor = m$. Now, $\mathcal{B}$ob discloses to $\mathcal{A}$lice the sets I_s and I_{1-s} for a random bit s that he keeps secret. $\mathcal{A}$lice chooses $s' \in \{0,1\}$ at random and publicly announces s' together with $C(b^{(s')})$, where $C : \{0,1\}^m \to \{0,1\}^c$ is an error-correcting code that allows $\mathcal{B}$ob to correct the transmission errors in $I_{s'}$ for an error-rate up to δ. For every $x \in \{0,1\}^m$, the value $C(x)$ consists of extra bits that are always sent separately by an error-free channel such as a telephone. The code C is chosen such that if $s \neq s'$, then $\mathcal{B}$ob's uncertainty about the value of $b^{(s')} = \{b_i | i \in I_{s'}\}$ given $C(b^{(s')})$ remains high. At this point, if $s' = s$ then $\mathcal{B}$ob shares the string $b^{(s')}$ with $\mathcal{A}$lice otherwise he knows little about $b^{(s')}$. Adopting privacy amplification techniques [BBR, BBCM], $\mathcal{A}$lice chooses at random from a universal$_2$ class of hashing functions [CW] a function $h : \{0,1\}^m \to \{0,1\}^l$, where $l < n$. Then she chooses $\gamma \in \{0,1\}^l$ such that $h(b^{(s')}) \oplus \gamma = \beta$ is the string to be transmitted by oblivious transfer and announces both h and γ. Privacy amplification guarantees that, if $s \neq s'$ then knowing $h, \widehat{b}^{(s')}$ and a string γ is not sufficient to learn more than a negligeable amount of Shannon information about $h(b^{(s')}) \oplus \gamma = \beta$.

3 Known results

To obtain the security of the BBCS-protocol we must consider the possibility of a dishonest $\mathcal{A}$lice and a dishonest $\mathcal{B}$ob separately.

Given the perfect bit commitment scheme [BCJL], $\mathcal{A}$lice has no clue on which I_s or I_{1-s} is the set of reliable photons. Thus, she has no way to cheat the protocol i.e. she does not know whether β is received or not.

The security against $\mathcal{B}$ob's possible behaviour can be obtained by privacy amplification technique. This tool is used in the classical part and requires that after the quantum part $\mathcal{B}$ob has a significant amount of collision entropy about the N bits.

Definition 2 *The* collision entropy *of a distribution of probability f on a set X is*

$$H_c(f) = -\log P_c(f)$$

where $P_c(f)$ is the collision probability defined by

$$P_c(f) = \sum_{x \in X} f(x)^2.$$

In the case, where f is a distribution of Bernoulli, we write $H_c(f) = H_c(p)$, where p is the probability of sucess.

Let f be the distribution of probability that corresponds to $\mathcal{B}$ob's knowledge about $b^{(s)}, b^{(1-s)}$ after the measurements. The main theorem of [BBCM] stipulates that if $H_c(f) \geq 2t$ then for $h : \{0,1\}^N \to \{0,1\}^{t-r}$(and $t > r$) chosen at random from a universal$_2$ class of hashing functions [CW], $\mathcal{B}$ob has no more than $2^{-r}/\ln 2$ bits of Shannon information except with negligible probability on one of $h(b^{(s)})$ or $h(b^{(1-s)})$. Furthermore, $\mathcal{A}$lice has probability exactly

$\frac{1}{2}$ of choosing that one and in that case $\mathcal{B}$ob learns almost nothing about $\beta \in \{0,1\}^{t-r}$ (except with negligible probability).

If the quantum channel is a noisy channel, then the code C gives extra knowledge about $b^{(s)}, b^{(1-s)}$. The functions h must remove this information in addition to the information that is obtained by $\mathcal{B}$ob's measurements. Recent work ([MC]) has determined the extra "shrinking" parameter needed to remove this information as well. If the code C gives c bits of information in order to correct an error-rate δ and if $H_c(f) \geq 2t$ then a universal$_2$ class of hashing functions $h : \{0,1\}^N \to \{0,1\}^{t-r-2c}$ removes almost all information about one of $b^{(s)}$ or $b^{(1-s)}$ except with negligeable probability. As a consequence, Crépeau's proof can be extended to the case where the quantum channel is noisy.

In section 4 we show that,under the assumption 2, for almost all execution of the BBCS-protocol protected against photon-storing, there exists $t' > 0$ (where t' is function of δ) such that, for every value of n, $\mathcal{B}$ob's collision entropy on the N bits is larger than $2t'n$ excepted with a negligeable probability. Therefore, in the above results, we may replace t by $t'n$ and r by $r'n$, where $r' < t'$.

4 A lower bound for $\mathcal{B}$ob's total collision entropy

In this section, we prove the following theorem.

Theorem 1 *Let f be the distribution of probability that corresponds to $\mathcal{B}$ob's knowledge, about the bits b_i, where $open_i = 0$, after step 5 of the protocol* **Game**(δ, n)*. Given that the measurements act on individual photons, if $\mathcal{B}$ob has not been rejected at step 4, then excepted with a probability smaller than $2^{-\alpha n}$, where $\alpha > 0$, $\mathcal{B}$ob's total collision entropy $H_c(f)$ is bounded below by $2t'n$, where $2t' = p_H H_c(p_I)(4 - \frac{\delta}{p_F})$, in which $p_F = \frac{1}{9}(1 - \frac{\sqrt{3}}{2})$, $p_H = \frac{1}{36}$ and $p_I = \frac{1}{4}$.*

Regarding notation, we use the general rule that every random value that is represented by a lowercase letter in the protocol, corresponds to a random variable which we denote by the matching uppercase letter. For example, the bits b_i and the basis θ_i for the ith photon, become respectively the random variables B_i and Θ_i.

4.1 Bob's strategies

The following protocol describes the most general $\mathcal{B}$ob's strategy. In this protocol, $\mathcal{B}$ob is entirely free of using any useful knowledge that he learned prior to the current instruction.

SubProtocol 4.1 (Game(δ, n))

1: $\mathcal{A}$lice sets $fail \leftarrow 0, N \leftarrow 0$

2: $\overset{4n}{\underset{i=1}{\textbf{DO}}}$

$\mathcal{A}$lice picks $b_i \in_R \{0,1\}$ and $\theta_i \in_R \{+, \times\}$

$\mathcal{A}$lice sends to $\mathcal{B}$ob a photon π_i in the quantum state $|b_i\rangle_{\theta_i}$

$\mathcal{B}$ob chooses a measurement $\mathcal{M}_i$, measures π_i in order to obtain $\widehat{\theta}_i \in \{+, \times\}$ and $\widehat{b}_i \in \{0,1\}$

$\mathcal{B}$ob sends the 2-bit commitment c_i for $(\widehat{b}_i, \widehat{\theta}_i)$ to $\mathcal{A}$lice

3: $\overset{4n}{\underset{i=1}{\textbf{DO}}}$

$\mathcal{A}$lice picks $open_i \in_R \{0,1\}$, if $open_i = 1$ then she asks $\mathcal{B}$ob to unveil the commitment c_i

If $open_i = 0$ then $\mathcal{A}$lice and $\mathcal{B}$ob set $N \leftarrow N + 1$

Else if $c_i = (\theta_i, 1 - b_i)$ then $\mathcal{A}$lice sets $fail \leftarrow fail + 1$

4: If $fail \leq \delta n$ then $\mathcal{A}$lice announces her choices $\theta_1, \theta_2, \ldots, \theta_{4n}$ to $\mathcal{B}$ob otherwise she refuses to continue

5: $\overset{4n}{\underset{i=1}{\textbf{DO}}}$ $\mathcal{B}$ob chooses $\mathcal{M}'_i$ to refine the measurement on π_i and obtains the result j_i.

In this subsection, without loss of generality, we discard from the analysis measurements that results from strategies that are useless to $\mathcal{B}$ob and discuss the connection between the useful measurements (i.e., the undiscarded measurements), their classical outcomes and variables such as $\widehat{\theta}_i, \widehat{b}_i$ that are used in the protocol.

In the protocol **Game**(δ, n), $\mathcal{B}$ob executes two measurements on each photon: the pre-basis measurement $\mathcal{M}_i$ and the post-basis measurement $\mathcal{M}'_i$. However, the effect of these two measurements on the ith photon as well as their classical outcomes can be seen as coming from a single measurement, which we call the ith measurement. We must keep in mind that, in accordance with $\mathcal{B}$ob's strategy, this measurement is a random variable that depends upon other random variables, including the basis Θ_i.

It is shown in [Ma] that any possible choice of $\mathcal{B}$ob for the ith measurement can be represented by a single IPP transformation from the initial space of states to a larger space of states followed by an ordinary von Neumann measurement on the latter. Let U_i be the IPP transformation that is associated with the ith measurement. We may assume that this measurement is complete because it is not advantageous for $\mathcal{B}$ob to leave any residual information out in the final state of the photon. Therefore, this measurement can be represented by an orthonormal basis in the final space of states for the transformation U_i. The vectors in this basis are denoted $|r_i\rangle$, where r_i represents the outcome of the ith measurement; it includes both, the classical outcome of the pre-basis measurement and the classical outcome of the post-basis measurement.

Using the pre-basis measurement outcome (that is included in r_i), $\mathcal{B}$ob determines a pair $c_i = (\widehat{\theta}_i, \widehat{b}_i) = f(r_i)$ that he commits to $\mathcal{A}$lice. Bob has no advantage in using a randomized function f, because he wants to obtain c_i that minimize the possibility that $fail$ increases (the outcome r_i is random, but not f). Also, because $\mathcal{B}$ob wants to make the most incomplete pre-basis measurement as possible, it is best for him to make a pre-basis measurement in which there is not more than one outcome for each non zero probability value of C_i, i.e., f is injective. Taking advantage of this, we identify the outcome r_i of the ith measurement with the triplet $(j_i, \widehat{\theta}_i, \widehat{b}_i)$, where j_i is the post-measurement outcome and $(\widehat{\theta}_i, \widehat{b}_i)$ is the pair c_i that is committed, which pair may now be considered as the pre-basis measurement outcome.

Now, let us consider the dependencies or independencies that exists among the variables of the protocol. Because it includes the post-basis measurement, the ith measurement may depend upon the basis Θ_i that is announced by Alice, however, the outcome C_i of the pre-basis measurement is independent of the basis Θ_i, because the density matrices associated with the two values of Θ_i are identical. After the pre-basis measurement, since $\mathcal{B}$ob has already commited the pair c_i, he has no way to reduce its chance of being caught and, therefore, having the post-basis measurement depends upon previous outcomes is totally useless. From this one obtains that the distribution on the quadruplets $(\Theta_i, B_i, Open_i, J_i)$,$i = 1, \ldots, 4n$, given fixed values for $C_1, \ldots, C_{4n}$ is a distribution of independent quadruplets. In other words, once we have fixed the values of $C_1, \ldots, C_{4n}$, the measurements are fixed and, in that case, variables that are associated with distinct measurements become completely independents.

4.2 The main idea

This subsection analyses the mecanism that is used in the protocol to guaranty that $\mathcal{B}$ob's total collision entropy H_c is bounded. This analysis is developped in a context, where $\mathcal{B}$ob has made all of his $4n$ commitments and he is waiting for Alice to ask the openning of about half of the commitments. Therefore, we fix the sequence of pairs $c_i = (\widehat{\theta}_i, \widehat{b}_i)$, $i = 1, \ldots, 4n$, that are commited.

With regard to this analysis, the most important aspect of the protocol is that if $\mathcal{B}$ob is not rejected then the variable $fail$ must be smaller than δn and therefore whenever $\mathcal{B}$ob has committed to the correct basis $(\widehat{\theta}_i = \theta_i)$. he must have committed to the correct bit $(\widehat{b}_i = b_i)$. This means that, whenever $\mathcal{B}$ob is not rejected, he has a lot of information about most bits b_i, where $\theta_i = \widehat{\theta}_i$. Therefore, most contributions to $\mathcal{B}$ob's total collision entropy H_c must occur when $\theta_i \neq \widehat{\theta}_i$. Furthermore, even if $\theta_i \neq \widehat{\theta}_i$, we cannot assume that, for every outcome j_i, $\mathcal{B}$ob obtains only a small amount of collision information. In particular, $\mathcal{B}$ob could learn a lot about B_i for some outcome j_i that is unlikely to happen. This suggests that we define a random event ΔH_i that will be used to count the random number of bits B_i that significatively contribute to $\mathcal{B}$ob's total collision entropy. The definition of ΔH_i, must also take care of the fact that only the N bits B_i, where $Open_i = 0$, must contribute to this measure of $\mathcal{B}$ob's ignorance.

Definition 3 *The event ΔH_i for the triplets of random variables $(\Theta_i, Open_i, J_i)$ is defined as the set of triplets $(\widehat{\theta}_i^c, 0, j_i)$, where*

$$(\forall b)\ Pr(B_i = b | \Theta_i = \widehat{\theta}_i^c \wedge R_i = (\widehat{\theta}_i, \widehat{b}_i, j_i)) > p_I, \quad (2)$$

where $p_I = 1/4$

Equation 2 means that

$$H_c(B_i | \Theta_i = \theta_i \wedge R_i = (\widehat{\theta}_i, \widehat{b}_i, j_i)) > -lg(p_I^2 + (1-p_I)^2) = lg(8/5),$$

where the left side of the inequality is $\mathcal{B}$ob's collision entropy on the bit B_i. The purpose of this definition is to find a lower bound on $\mathcal{B}$ob's total collision entropy, however we are not going to find the best bound. In computing this bound we will ignore the photons π_i for which the event ΔH_i has a low probability, even though some of these other photons may also contribute to $\mathcal{B}$ob's collision entropy. Furthermore, the value $p_I = 1/4$ that is used in the definition of ΔH_i has been chosen without much consideration for optimization.

Now, the main idea is to show that if the probability of the event ΔH_i is small then the probability that the variable $Fail$ increases is large. To go ahead with this idea we define two sets Γ_H and Γ_F.

Definition 4 *The set Γ_H is the set of photons π_i, for which*

$$Pr(\Delta H_i | C_i = (\widehat{\theta}_i, \widehat{b}_i)) \geq p_H,$$

where $p_H = \frac{1}{36}$.

For every $i \in \Gamma_H$, the variable H_c has a probability at least p_H of being incremented by $lg(8/5)$ bits. As for the parameter $p_I = 1/4$ in ΔH_i, the parameter $p_H = 1/36$ has been chosen without much consideration for optimization.

Definition 5 *The set Γ_F is the set of photons π_i, for which*

$$Pr(\mathcal{B}_i = \widehat{b}_i^c \wedge \Theta_i = \widehat{\theta}_i \wedge Open_i | C_i = (\widehat{\theta}_i, \widehat{b}_i)) \geq p_F(p_I, p_H)$$

where

$$p_F(p_I, p_H) = \frac{1}{8}(1 - 2\sqrt{p_I(1-p_I)})(1 - 4p_H)$$

For every $i \in \Gamma_F$, the variable $Fail$ has a probability at the least p_F of being incremented.

4.3 The main lemma

Now, we are ready to state a lemma that expresses the main idea that has been introduced in the preceding section. Subsequently, this lemma is used to prove the theorem.

Lemma 1 (Main lemma) *For every execution of the protocol* **Game**(δ, n), *if Γ_H and Γ_F are defined as above, then $\Gamma_H^c \subseteq \Gamma_F$, where Γ_H^c is the complement of Γ_H with respect to the $4n$ photons.*

To introduce the proof of this lemma we begin by considering a simpler situation where, $\mathcal{B}$ob does not use Θ_i to choose the ith measurement. Let $\Phi(j_i\theta_i b_i)$ represents the transition amplitude from the initial state $|b_i\rangle_{\theta_i}$ to the final state $|j_i\widehat{\theta}_i\widehat{b}_i\rangle$. If $\mathcal{B}$ob obtains a lot of information from the result $(j_i\widehat{\theta}_i, \widehat{b}_i)$ (when $\theta_i = \widehat{\theta}_i^c$) then, one can easily show, using Baye's rule to compute the aposteriori probability, that one of the two amplitudes $\Phi(j_i\widehat{\theta}_i^c 0)$ and $\Phi(j_i\widehat{\theta}_i^c 1)$ must be small with respect to the other one. To show that in this case the variable $Fail$ is likely to be incremented, we must make use of the fact that if, for *this measurement*, Alice had used the other basis, then the two corresponding amplitudes would have about the same magnitude. To see this, we simply use

$$(\forall b_i) \;\; \Phi(j_i\widehat{\theta}_i b_i) = (1/\sqrt{2})(\Phi(j_i\widehat{\theta}_i^c 0) \pm \Phi(j_i\widehat{\theta}_i^c 1))$$

which implies that the magnitude of these two transition amplitudes is between $\frac{1}{\sqrt{2}} |\; |\Phi(j_i\widehat{\theta}_i^c b_i^c)| - |\Phi(j_i\widehat{\theta}_i^c b_i)| \;|$ and $\frac{1}{\sqrt{2}} |\; |\Phi(j_i\widehat{\theta}_i^c b_i^c)| + |\Phi(j_i\widehat{\theta}_i^c b_i)| \;|$. This means that the wrong bit $\widehat{b}_i^c$ must have occurred with some probability that cannot be very far away from 1/2. Now, in this situation, $fail$ increases if $Open_i = 1$ and $\Theta_i = \widehat{\theta}_i$, therefore it increases with a probability that is not far from 1/8.

Now let us return to the real protocol, where $\mathcal{B}$ob is allowed to change the post-basis measurement in accordance with the value of Θ_i. In this situation, the preceding discussion does not directly apply. In particular, it is a loss of generality to conclude that a large difference in the amplitude $\Phi(j_i\widehat{\theta}_i^c 0)$ and $\Phi(j_i\widehat{\theta}_i^c 1)$ implies that the physical amplitudes $\Phi(j_i\widehat{\theta}_i 0)$ and $\Phi(j_i\widehat{\theta}_i 1)$ have similar magnitude. One must rather consider fictitious amplitudes defined in the following way,

$$\Phi^f(j_i\theta_i^c b_i) = \frac{1}{\sqrt{2}}(\Phi(j_i\theta_i 0) \pm \Phi(j_i\theta_i 1)).$$

For each individual result $r_i = (j_i\widehat{\theta}_i\widehat{b}_i)$, these fictitious amplitudes do not have a direct physical interpretation in the protocol. To physically interpret the squares of their magnitudes as a probability one must consider a fictitious $\mathcal{B}$ob who does not use the basis θ_i to determine the post-basis measurement. However, we do not have to physically interpret them at all. They are simply, in a basis of our choice, the components of a matrix that represents the measurement that is made by $\mathcal{B}$ob. However, because the pre-basis measurement is independent of Θ_i, the following vectors,

$$|\Phi(\theta_i^c b_i)\rangle = \sum_{j_i} \Phi^f(j_i\theta_i^c b_i) \; |j_i\widehat{\theta}_i\widehat{b}_i\rangle, \qquad (3)$$

are not fictitious, they are more than columns in a matrix, they correspond, up to an IPP transformation, to the projected states that result from the pre-basis measurement when the initial state is $|b_i\rangle_{\theta_i^c}$ and the outcome is $(\widehat{\theta}_i, \widehat{b}_i)$.

Now, as in the simpler case that we have dicussed above, one can see that if the genuine amplitudes in the basis $\Theta_i = \widehat{\theta}_i^c$ have very different magnitudes, then their corresponding fictitious amplitudes in the other basis $\Theta_i = \widehat{\theta}_i$ must have similar magnitudes. The point is that, if this is true for a set of outcomes I_i

with significant probability, then the corresponding vectors defined by formula 3 will have about the same norm. Because the square of these vectors correspond to the probabilities of the corresponding transitions, this means that with significant probability $\mathcal{B}$ob has chosen the wrong bit B_i and this is enough to bound the collision entropy. The proof of the lemma is a formalization of the above discussion.

Proof of the lemma. The proof consists in using $i \in \Gamma_H^c$ to obtain $i \in \Gamma_F$. We first consider the set Γ_H^c. The event ΔH_i that is used in the definition of Γ_H is the conjonction of three events: $\Theta_i = \widehat{\theta}_i^c$, $Open_i = 0$ and $\neg I_i$, where the event I_i, for the random variable Θ_i and J_i is defined as the set of pairs (θ_i, j_i) such that

$$(\exists b)\ Pr(B_i = b | \Theta_i = \theta_i \wedge R_i = (j_i \widehat{\theta}_i, \widehat{b}_i)) \leq p_I. \quad (4)$$

Using definition 4 and the fact that $Pr(Open_i = 0 \wedge \Theta_i = \widehat{\theta}_i^c | C_i = (\widehat{\theta}_i, \widehat{b}_i)) = 1/4$, we obtain that Γ_H^c is the set of photons π_i such that

$$\Pr(I_i | \Theta_i = \widehat{\theta}_i^c \wedge C_i = (\widehat{\theta}_i, \widehat{b}_i)) \geq 1 - 4p_H = 8/9. \quad (5)$$

Let us expand the formula 5.

$$\begin{aligned} &\Pr(I_i | \Theta_i = \widehat{\theta}_i^c \wedge C_i = (\widehat{\theta}_i, \widehat{b}_i)) \\ &= \frac{\sum_{(\widehat{\theta}_i^c, j_i) \in I_i} Pr(J_i = j_i \wedge \Theta_i = \widehat{\theta}_i^c \wedge C_i = (\widehat{\theta}_i \widehat{b}_i))}{Pr(\Theta_i = \widehat{\theta}_i^c \wedge C_i = (\widehat{\theta}_i \widehat{b}_i))} \\ &= \frac{\sum_{(\widehat{\theta}_i^c, j_i) \in I_i} Pr(R_i = (j_i \widehat{\theta}_i \widehat{b}_i) \wedge \Theta_i = \widehat{\theta}_i^c)}{Pr(\Theta_i = \widehat{\theta}_i^c \wedge C_i = (\widehat{\theta}_i \widehat{b}_i))} \\ &= \frac{\sum_{(\widehat{\theta}_i^c, j_i) \in I_i} Pr(R_i = (j_i \widehat{\theta}_i \widehat{b}_i))}{Pr(C_i = (\widehat{\theta}_i \widehat{b}_i))} \end{aligned}$$

We obtain that, for $i \in \Gamma_H^c$,

$$\sum_{(\widehat{\theta}_i^c, j_i) \in I_i} Pr(R_i = (j_i \widehat{\theta}_i^c \widehat{b}_i)) \geq (1 - 4p_H) Pr(C_i = (\widehat{\theta}_i \widehat{b}_i)) \quad (6)$$

Now, we reexpress in terms of the amplitudes Φ the condition $(\widehat{\theta}_i^c, j_i) \in I_i$. According to formula 4, this condition means

$$(\exists b_i)\ Pr(B_i = b_i | \Theta_i = \widehat{\theta}_i^c \wedge R_i = (j_i \widehat{\theta}_i, \widehat{b}_i)) \leq p_I$$

$$(\exists b_i)\ \frac{Pr(B_i = b_i \wedge \Theta_i = \widehat{\theta}_i^c \wedge R_i = (j_i \widehat{\theta}_i, \widehat{b}_i))}{Pr(\Theta_i = \widehat{\theta}_i^c \wedge R_i = (j_i \widehat{\theta}_i, \widehat{b}_i))} \leq p_I$$

$$\begin{aligned} (\exists b_i) Pr(R_i = j_i \widehat{\theta}_i \widehat{b}_i | \Theta_i = \widehat{\theta}_i^c \wedge B_i = b_i) \leq \\ 2 p_I Pr(R_i = j_i \widehat{\theta}_i \widehat{b}_i) \end{aligned} \quad (7)$$

For the L.H.S we have

$$Pr(R_i = j_i \widehat{\theta}_i \widehat{b}_i | \Theta_i = \widehat{\theta}_i^c \wedge B_i = b_i) = |\Phi(j_i \widehat{\theta}_i^c b_i)|^2$$

For the R.H.S we have

$$(\forall \theta_i) 2 Pr(R_i = j_i \widehat{\theta}_i \widehat{b}_i) = |\Phi(j_i \theta_i 0)|^2 + |\Phi(j_i \theta_i 1)|^2 \quad (8)$$

We obtain that $(\widehat{\theta}_i^c, j_i) \in I_i$ is equivalent to

$$(\exists b_i)\ |\Phi(j_i \widehat{\theta}_i^c b_i)|^2 \leq p_I (|\Phi(j_i \widehat{\theta}_i^c 0)|^2 + |\Phi(j_i \widehat{\theta}_i^c 1)|^2) \quad (9)$$

Now, to show that $\pi_i \in \Gamma_F$, we want to use the inequalities 9 and 6 (given by $i \in \Gamma_H^c$) to obtain

$$\begin{aligned} \|\, |\Phi(\widehat{\theta}_i, \widehat{b}_i^c)\rangle \|^2 &= \sum_{j_i} |\Phi^f(j_i, \widehat{\theta}_i, \widehat{b}_i^c)|^2 \\ &= Pr(C_i = (\widehat{\theta}_i, \widehat{b}_i) | \Theta_i = \widehat{\theta}_i \wedge B_i = \widehat{b}_i^c) \\ &\geq p_F, \end{aligned}$$

where p_F is given in definition 5. We make use of the constraint 9 on the amplitudes $\Phi(\cdot)$ to obtain a lower bound on each of the ficticious amplitude $\Phi^f(\cdot)$. The magnitude of the fictitious amplitudes $\Phi^f(j_i \widehat{\theta}_i \widehat{b}_i^c)$ is given by

$$|\Phi^f(j_i \widehat{\theta}_i \widehat{b}_i^c)| = \frac{1}{\sqrt{2}} |\Phi(j_i \widehat{\theta}_i^c 0) \pm \Phi(j_i \widehat{\theta}_i^c 1)|$$

Now, if the magnitude square of the smallest Φ is smaller than $p_I(|\Phi(\cdot)|^2 + |\Phi(\cdot)|^2)$ then the biggest is bigger than $(1-p_I)(|\Phi(\cdot)|^2 + |\Phi(\cdot)|^2)$. The lower bound is obtained by taking the extreme case. We obtain

$$\begin{aligned} (\forall b_i) |\Phi^f(j_i \widehat{\theta}_i^c b_i)|^2 \geq\ & f(p_I)(|\Phi(j_i \widehat{\theta}_i^c 0)|^2 \\ & + |\Phi(j_i \widehat{\theta}_i^c 1)|^2) \end{aligned} \quad (10)$$

where

$$f(p_I) = \frac{1}{2}(1 - 2\sqrt{p_I(1 - p_I)})$$

After summing the inequality 10, with $b_i = \widehat{b}_i^c$, using formula 8 and 6, we obtain

$$\begin{aligned} & Pr(C_i = (\widehat{\theta}_i \widehat{b}_i) | \Theta_i = \widehat{\theta}_i \wedge B_i = \widehat{b}_i^c) \\ & \geq 2 f(p_I)(1 - 4p_H) Pr(C_i = (\widehat{\theta}_i \widehat{b}_i)) \end{aligned}$$

From which we have

$$\begin{aligned} & Pr(B_i = \widehat{b}_i^c \wedge \Theta_i = \widehat{\theta}_i \wedge C_i = (\widehat{\theta}_i \widehat{b}_i)) \geq \\ & \frac{1}{2} f(p_I)(1 - 4p_H) Pr(C_i = (\widehat{\theta}_i, \widehat{b}_i)) \end{aligned}$$

$$Pr(B_i = \widehat{b}_i^c \wedge \Theta_i = \widehat{\theta}_i \wedge Open_i = 1 | C_i = (\widehat{\theta}_i \widehat{b}_i)) \geq \frac{1}{4} f(p_I)(1 - 4p_H).$$

Therefore, we have that $i \in \Gamma_F$, with

$$p_F = \frac{1}{4} f(p_I)(1 - 4p_H) = \frac{1}{8}(1 - 2\sqrt{p_I(1-p_I)})(1 - 4p_H)$$

and this concludes the proof of the lemma. □

Proof of the theorem. We want to prove that for every sequence $c_1, \ldots, c_{4n}$, $\mathcal{B}$ob's total collision entropy is bounded below (by the same bound). Let n_H and n_F be the sizes of Γ_H and Γ_F respectively. For $c_1, \ldots, c_{4n}$ fixed, n_H and n_F are also fixed. Basically, the lemma says that $n_F \geq 4n - n_H$ or equivalently $n_H \geq 4n - n_F$. Using the aposteriori independence of the bits B_i, we have that at the end of the protocol $\mathcal{B}$ob's total collision entropy is the sum of the collision entropy of each bit B_i, where $Open_i = 0$. Now, let $\Gamma_{\Delta H}$ be the set of photons $i \in \Gamma_H$, where $(\theta_i, open_i, j_i) \in \Delta H_i$. Let $H_c(p_I) = -lg(p_I^2 + (1 - p_I)^2) = lg(8/5)$. From what we said above, we obtain that $\mathcal{B}$ob's collision entropy is greather than $n_{\Delta H} \times H_c(p_I)$, where $n_{\Delta H}$ is the size of $\Gamma_{\Delta H}$. Now, using the independence between variables that are associated with distinct measurements, we have that $n_{\Delta H}$ is a binomial with parameters $p_H = 1/8$ and n_H. Similarly, the distribution of $Fail$ is a binomial with parameter p_F and n_F. Now, let us assume that $\mathcal{B}$ob's strategy is such that there is a non negligeable probability that Alice does not refuse to continue with the protocol. This implies that $n_F \times p_F \leq (\delta + \epsilon)n$ for any $\epsilon > 0$ except with negligeable probability. Therefore, we have $n_H \geq (4 - \frac{(\delta+\epsilon)}{p_F})n$. This gives us that $\mathcal{B}$ob's total collision entropy is greater that $[H_c(p_I)p_H(4 - \delta/p_F) - \epsilon']n$ for any $\epsilon' > 0$ excepted with an exponentially small probability. □

5 Conclusion

We have shown that the BBCS-protocol is secure if all measurements are performed individually on the received photons. Individual measurements are interesting because they are easier to effect than coherent measurements. The main open question is to enhance the proof to the case of coherent measurements. It would be interesting to find a better bound for the collision entropy in order to minimize the shrinking parameter for the hashing function used in the privacy amplification stage.

Acknowledgements

The authors are grateful to Gilles Brassard, Claude Crépeau, Dan Simon and Bill Wootters for fruitful and helpful discussions.

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

[BBCM] C.H. Bennett, G. Brassard, C. Crépeau, U. Maurer, *Privacy Amplification Against Probabilistic Information*, to be published.

[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.

[BBR] C.H. Bennett, G. Brassard, J.-M. Robert, *Privacy Amplification by Public Discussion*, SIAM Journal on Computing, Vol. 17, No.2, 1988, pp. 210-229.

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

[Cr] C. Crépeau, *Quantum Oblivious Transfer*, submitted to the Journal of Modern Optics'special issue on Quantum Cryptography,1994.

[CW] J. L. Carter, M. N. Wegman, *Universal Classes of Hash Functions*, Journal of Computer and System Science, Vol. 18, 1979, pp.143–154.

[Ma] D. Mayers, *Quantum Transformation and Generalized Measurements*, to appears.

[MC] C. Cachin, U. Maurer, *Linking Reconciliation and Privacy Amplification*, to appear in the proceeding of Eurocrypt'94.

[Ki] J. Kilian. *Founding cryptography on oblivious transfer*. In Proc. 20th ACM Symposium on Theory of Computing, pp. 20–31, Chicago, 1988. ACM.

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

[TRT2] Townsend, P. D., Rarity, J. G. and Tapster, P. R., "Enhanced single photon visibility in a 10km long prototype quantum cryptography channel",*Electronics Letters*, to appear.