Quantum Key Distribution and String Oblivious Transfer in Noisy Channels

Dominic Mayers[1]

DIRO,Université de Montréal
C.P. 6128, Succursale CENTRE-VILLE
Montréal (Québec)
Canada, H3C 3J7

Abstract. We prove the unconditional security of a quantum key distribution (QKD) protocol on a noisy channel against the most general attack allowed by quantum physics. We use the fact that in a previous paper we have reduced the proof of the unconditionally security of this QKD protocol to a proof that a corresponding Quantum String Oblivious Transfer (String-QOT) protocol would be unconditionally secure against Bob if implemented on top of an unconditionally secure bit commitment scheme. We prove a lemma that extends a security proof given by Yao for a (one bit) QOT protocol to this String-QOT protocol. This result and the reduction mentioned above implies the unconditional security of our QKD protocol despite our previous proof that unconditionally secure bit commitment schemes are impossible.

1 Introduction and Brief History

One of the most popular application of quantum physics to cryptography is quantum key distribution (QKD). In an ideal QKD, Alice and Bob who share no secret information initially, share a secret string s at the end. An eavesdropper, typically called Eve, should learn nothing about the secret string s, except perhaps for its length.

In this paper, we prove the security of a QKD protocol against the most general attack allowed by quantum physics. This QKD protocol works with a noisy quantum channel, an imperfect measuring apparatus, but requires a perfect source and a faithful classical channel. A channel is *faithful* if no one can modified a message sent in the channel without being detected. The need for a faithful classical channel is not a problem because a secret string s_0 initially shared between Alice and Bob can be used to simulate a faithful classical channel by use of an unconditionally secure classical authentification scheme [26]. We assume a perfect source to avoid the technical difficulty associated with many photons per pulse.

Our preliminary version of the protocol uses a random linear code for error correction. Random linear codes are very difficult to decode. However, this problem can be solved and a version of the protocol using an efficient error correcting code and with no requirement for a perfect source will be considered in the journal version of this paper.

N. Koblitz (Ed.): Advances in Cryptology - CRYPTO '96, LNCS 1109, pp. 343-357, 1996.

In addition to QKD, other applications of quantum physics to cryptography have been proposed. The most popular are quantum bit commitment (QBC) and quantum oblivious transfer (QOT). We briefly review these protocols since we shall refer to them in our results. In the bit commitment task from Alice to Bob, Alice commits a bit b. Later, if Bob asks Alice to *unveil* the commitment, he receives the bit b. The main point is that Alice cannot change the value of b and Bob learns nothing about b unless Alice unveils it. In the oblivious transfer task from Alice to Bob, Alice enters a bit b, Bob receives a perfectly random bit c and he learns the value of b if and only if $c = 0$. Alice learns nothing about c.

The first quantum bit commitment protocol ever proposed is due to Bennett and Brassard [2]. The authors themselves knew at the time that this protocol is insecure. Other quantum bit commitment protocol have been proposed, but none of them could be proven unconditionally secure. In fact, it has been shown recently that unconditional security for quantum bit commitment is impossible [18, 19, 20]. A proof of computational security for a quantum bit commitment protocol is still possible, but none is currently available. The absence of a provably secure bit commitment is unfortunate because all the known quantum oblivious transfers are built on top of bit commitment, that is, they use quantum bit commitment as a sub-protocol.

The first quantum oblivious transfer protocol which would be secure if implemented on top of a secure bit commitment protocol has been proposed by Crépeau [12]. Its security against most but not all reasonable attacks allowed by the current technology has been shown in [5]. The first proof that considered the most general attack allowed by quantum physics, including the so called *coherent* measurements on many photons at a time, has been obtained by Yao [27]. Yao's proof is an important step and provides useful techniques, but it provides no security because, as for all the previous proofs [5, 21], it requires a secure bit commitment and none has yet been proven secure.

Now, we are back to QKD. The security of a QKD protocol against most but not all reasonable attacks allowed by the current technology has been established in [3, 4]. In [17], we have reduced the unconditional security of any QKD protocol of a certain kind to a proof that a corresponding String-QOT protocol would be unconditionally secure if implemented on top of an unconditionally secure bit commitment scheme. The QKD protocols of the appropriate type are in one to one correspondence with corresponding String-QOT protocols. The standard QOT protocol in Yao's proof turns out to be associated with a QKD protocol of the appropriate type. Therefore, the unconditional security of this QKD protocol is obtained from the above reduction. However, there are two problems with this protocol. First, the QOT protocol in Yao's proof is a standard one bit QOT, therefore only one secret bit is returned in the QKD version. One can repeat the protocol n times to obtain a secret string of length n, but an initial secret key s_0 is required to simulate a faithful classical channel and, therefore, each execution of the protocol uses more secret bits than it returns back! Second, the QOT protocol in Yao's proof, and thus the corresponding QKD protocol, requires a noiseless quantum channel and a perfect source.

In this paper, we pursue the original idea of [17] and extend Yao's proof to a String-QOT protocol associated via the above reduction with a "strong" QKD protocol. Therefore, we have the unconditional security of this QKD protocol. This QKD protocol returns a secret string s that is longer than the required initial string s_0. Also, it works in a noisy quantum channel. Note that our proof for this QKD protocol considers any kind of errors in Bob's apparatus because we give full control over both the channel and the apparatus to a dishonest Bob in String-QOT.

It is shown in [6] that the security of any OT protocol implies the security of a String-OT protocol. In particular, the security of the QOT protocol in Yao's proof implies the security of a String-QOT protocol. However, the security of the resulting String-QOT protocol does not imply the security of a QKD protocol via the above reduction because it is not of the required type. Yao did not mention the possibility of generalizing his proof to a String-QOT case. It should be said that Yao was not aware of the above reduction (or did not believe it) at the time he wrote his paper [27]. Yao has announced in [27] that in the journal version of his paper the QOT protocol will work on a noisy channel but our String-QOT protocol has been design to work on a noisy channel without much additional effort.

2 Related results

The main problem that one must adress in the design of a QKD protocol is that Alice and Bob must exhange quantum systems, let say photons, and there is no way to distinguish interaction of these photons with the environment and interaction of these photons with Eve's measuring apparatus. Therefore, Eve can always succeed to *entangle* her measuring apparatus with the exchanged photons without being detected. Later, if these photons are used to define the shared key, Eve can obtain information about this key. However, using privacy amplification techniques, one can make this information arbitrarily small. For example, in the QKD protocol considered in this paper, a classical string $w' \in \{0,1\}^N$ is stored in N photons travelling from Alice to Bob. Because Eve can obtain information about w', privacy amplification is used to distil from w' a shorter but secret string $b = h(w')$. Privacy amplification is an essential part of any QKD protocol. Privacy amplification in the QOT protocol of Yao's proof corresponds to the fact that the secret bit is the exclusive or of all the bits of w'.

Much after the BB84 protocol of [2] have been proposed, Ekert suggested a scheme in which EPR pairs are created and the photons in each pair are split between Alice and Bob [15]. In this EPR scheme, no information is stored in the photons before they are sent, therefore one would hope that no information can be extracted by Eve. However, Eve can still entangle her apparatus with the photons and it has been shown that the kind of attacks that could work against the BB84 scheme correspond to attacks that would work against this EPR scheme [9]. This result highly suggested that EPR pairs might not be useful for quantum cryptography.

However, recently Deutsch, Ekert and al. proposed another EPR-based protocol with a new element, an *entanglement purification* procedure also called in this context a quantum privacy amplification procedure [14]. Entanglement purification [10] allows Alice and Bob to generate, from any supply of pairs of photons with non-zero entanglement, a smaller set of maximally entangled EPR pairs whose entanglement with any outside system, including Eve's apparatus, is arbitrarily low. Deutsch, Ekert and al. reasonnably argue that their protocol is unconditionally secure against the most general attack allowed by quantum physics. An interesting point is that privacy amplification is done at the quantum level, and one can hope that this kind of privacy amplification procedure is more efficient. On the other hand, working prototypes for protocol that use simple quantum coding schemes already exist [24, 25, 22, 23, 16], whereas the technology required for this EPR-based protocol is not yet available.

Let us emphasis that in a security proof for a QKD or a String-QOT protocol one must consider carefully the criteria to reject or accept an execution of the protocol. This criteria always exists for a given lower bound on the lenght of the shared key or string. In the case of our String-QOT protocol, Alice must detect less than δn errors. One must show that this criteria implies that the cheater cannot succeed. This analysis is difficult in the case of the most general attack allowed by quantum physics and to our knowledge, only Yao's paper [27] deals rigorously with this issue.

The purpose of quantum cryptography is not only to prove the security of protocols. We also want to design more efficient protocols and see how efficient are these protocols in theory and in practice. Biham and More have obtained the exact theoretical efficiency of the QKD protocol of [1] against a restricted but still reasonnable type of attacks [8]. Furthermore, it is reasonnable to believe that we could eventually prove that the security parameters required against this restricted type of attack is not too far from the security parameters required against the most general attack.

3 Some algebra

Typically, a quantum protocol involves many systems and each system is associated with its own Hilbert space $\mathcal{H}$ also called a state space. For example, the polarization of a photon is associated with a two dimensional Hilbert space. The inner product of $\mathcal{H}$ evaluated on $(|\phi\rangle, |\psi\rangle) \in \mathcal{H}^2$ is denoted $\langle\phi|\psi\rangle$. For every vector $|\phi\rangle \in \mathcal{H}$, let $|\phi\rangle^\dagger : \mathcal{H} \to \mathbb{C}$ be be the linear functional on $\mathcal{H}$ which, when evaluated on any vector $|\psi\rangle \in \mathcal{H}$, simply returns the inner product $\langle\phi|\psi\rangle$. For obvious reason, $|\phi\rangle^\dagger$ is more conveniently denoted $\langle\phi|$. In terms of matrices, one represents a vector $|\psi\rangle \in \mathcal{H}$ as a column matrix. The operation "$\dagger$" on a matrix is simply the transpose conjugate, therefore $\langle\psi|$ is represented by a row matrix.

The space of linear functionals on $\mathcal{H}$ is denoted $\mathcal{H}^\dagger$. It is called the dual of $\mathcal{H}$. The inner product of $\mathcal{H}$ is also an operation on the cartesian product $\mathcal{H}^\dagger \times \mathcal{H}$. This operation can be generalized to any cartesian product of the form $\mathcal{G}_1 \times \ldots \times \mathcal{G}_n$ where each space $\mathcal{G}_i$ occurs only once and is either a state space

state $|\psi\rangle$ is $\|M_v|\psi\rangle\|^2$, the square of the norm of $M_v|\psi\rangle$. The final state $|v\rangle$ can be anything because just at the end of the measurement one is free to store the residual quantum information into the final state $|v\rangle$ of his choice. If $\Omega = \{|\phi_v\rangle\}$ is a basis of $\mathcal{H}$, a measurement in the basis Ω is simply the measurement that associate v to $|\phi_v\rangle$. Such a measurement is called an orthogonal measurement.

Now, let us generalize to incomplete measurement the above definition. The most general measurement on $\mathcal{H}$ is a set of outcome k where every outcome k is associated with an operator M_k on $\mathcal{H}$. The difference with a complete measurement is that M_k is in general a sum $M_k = \sum_v |v\rangle\langle\phi_v|$ rather than only a rank one operator $M_k = |k\rangle\langle\phi_k|$. The only requirement on the operators M_k is that $\sum_k M_k^\dagger M_k = \mathbf{I}$. The image of M_k can be any sufficiently large state space $\mathcal{H}_k$, because just at the end of the measurement one is free to store the residual quantum information into the system of his choice. For example, the quantum information can be send from the state space of a photon into the state space of an atom. The probability of k given an initial state $|\psi\rangle$ is $\|M_k|\psi\rangle\|^2$.

Every measurement $\mathbf{M}$ on a state space $\mathcal{H}$ that returns an outcome k can be refined by executing another measurement $\mathbf{M}'$ on $\mathcal{H}_k$. The new measurement $\mathbf{M}'$ may depend upon k. Let M'_v be the operation on $\mathcal{H}_k$ associated with the outcome v of $\mathbf{M}'$. The operation on the original space $\mathcal{H}$ associated with the overall outcome (v,k) is simply $M_{v,k} = M'_v M_k$.

If a quantum preparation contains a pure state $|\psi_\alpha\rangle$ with probability p_α, then one may conveniently represent this preparation by the operator $\rho = \sum_\alpha p_\alpha\ |\psi_\alpha\rangle\langle\psi_\alpha|$. The idea is that the probability of v given the preparation represented by ρ is simply $\langle\phi_v|\rho|\phi_v\rangle$. This works even if the initial states $|\psi_\alpha\rangle$ are not orthogonal. Note the important fact that two distinct preparations may correspond to a same density operator. Even for an incomplete measurement on a given preparation, one may use the density operator ρ of this preparation to compute the probability of an outcome k. We have that $\Pr(K = k|\rho) = \mathrm{Tr}(\Pi_k\rho)$, where $\Pi_k = M_k^\dagger M_k$. This trace is linear on Π_k and linear on ρ. Therefore, it is often advantageous to work with Π_k and ρ rather than with M_k and $|\psi_\alpha\rangle$. The matrix representation of the operator ρ in the basis $\{|\psi_\alpha\rangle\}$ is defined by $(\rho)_{\alpha,\alpha'} = \langle\psi_\alpha|\rho|\psi_{\alpha'}\rangle$.

In accordance with the BB84 coding scheme, the states $|0\rangle_+$, $|0\rangle_\times$, $|1\rangle_+$ and $|1\rangle_\times$ corresponds to one photon polarized at 0°, 45°, 90° and −45° degrees respectively. Note that + and × corresponds to the bases $\{|0\rangle_+, |1\rangle_+\}$ and $\{|0\rangle_\times, |1\rangle_\times\}$ respectively. For every $\theta \in \{+,\times\}^n$ and every $w \in \{0,1\}^n$, $|\psi_{w,\theta}\rangle$ denotes the product state $|w_1\rangle_{\theta_1} \ldots |w_n\rangle_{\theta_n}$. For any set of positions $E = \{\gamma_1, \ldots, \gamma_N\}$, let $w[E]$ be the string given by $w[E]_i = w_{\gamma_i}$, $1 \le i \le N$, and let $|\psi_{w,\theta}[E]\rangle$ be the product state $|w_{i_1}\rangle_{\theta_{i_1}} \ldots |w_{i_N}\rangle_{\theta_{i_N}}$ for the photons with position in E.

5 The String-QOT protocol and its security

The QOT protocol considered by Yao in [27] is a variant of the QOT protocol which has been first proposed by Crépeau [11, 12] and improved later in [5, 13]. We consider the natural generalization of this single bit QOT protocol to a

string QOT. In this String-QOT protocol, n is the number of photons sent in the protocol, b is the string sent by Alice, m is the lenght of b, r is the number of redundant bits needed for error correction, and $N = \lfloor .24n \rfloor$ is the lenght of the string shared between Alice and Bob *before* privacy amplification.

STRING-QOT(b)

1. Alice picks a random uniformly chosen $(r+m) \times N$ boolean matrix f where $N = \lfloor .24n \rfloor$. The r first rows define a matrix g used for error correction and the m following rows define a matrix h used for privacy amplification (see step 7).
2. Bob picks a random uniformly chosen $\hat{\theta} = \hat{\theta}_1 \ldots \hat{\theta}_n \in \{+, \times\}^n$ and makes a quantum commit of all $\hat{\theta}_i$ to Alice.
3. Alice picks a random uniformly chosen $w \in \{0,1\}^n$, a random uniformly chosen $\theta \in \{+, \times\}^n$, and sends to Bob n photons in the state $|\psi_{w,\theta}\rangle$.
4. Bob measures every photon i in basis $\hat{\theta}_i$, record the results $\hat{w}_i$ and makes a quantum commit of all n bases $\hat{w}_i$ to Alice.
5. Alice picks a random uniformly chosen subset $R \subseteq \{1, \ldots, n\}$ and tests the commitment made by Bob at positions $i \in R$. If more than δn positions $i \in R$ reveal $\theta_i = \hat{\theta}_i$ and $w_i \neq \hat{w}_i$, then Alice stops the protocol; otherwise, the test result is accepted.
6. Alice announces the string θ. Let T_0 be the set of all i with $\theta_i = \hat{\theta}_i$, and let T_1 be the set of all i with $\theta_i \neq \hat{\theta}_i$. Bob chooses a set $E_0 \subseteq T_0 - R$, a set $E_1 \subseteq T_1 - R$, where $|E_0| = |E_1| = N$, and announces $\{E_0, E_1\}$ in random order to Alice.
7. Alice chooses at random a set $E_c \in \{E_0, E_1\}$. For error correction, she announces the matrix g and the string $s = g\, w[E_c]$. For the computation of b, she announces the matrix h and the string $a = b \oplus (h\, w[E_c])$.
8. If $c = 0$, Bob obtains $w[E_c]$ by correcting the errors in $\hat{w}[E_c]$, then he computes the intermediary string $t = h\, w[E_c]$ and obtains the string b via $b = a \oplus t$. If $c = 1$, Bob obtains no information about t and, thus, no information about b.

Yao's QOT protocol is exactly as above, except that $r = 0$, $m = 1$ and $e_1 = (1, 1, \ldots, 1) \in GF(2)^N$ are fixed, that is, there is no error correction and there is only one secret bit $t = t_1$ which is the exclusive or of all the bits in $w[E_0]$.

The QKD version is identical to the String-QOT protocol, except that Bob announces E_0 to Alice rather than $\{E_0, E_1\}$ and Alice always chooses $c = 0$. In this paper, we shall only consider attacks that correspond to attacks that may be executed by Eve in the QKD version. Clearly, Eve has no control over the set E_0 (and E_1), so we shall assume that Bob constructs E_0 and E_1 as specified in the protocol. The case in which there is no restriction on E_0 and E_1 is not more difficult, but we don't need it to obtain the security of the QKD protocol.

As usual in statistic, a random variable is represented by an upper case letter, whereas the value taken by such a variable is represented by a lower case letter, for instance, the bit c is the value taken by a random variable C.

Let V be Bob's view at the end of the protocol. Let $Pass$ be the binary random variable that takes the value 1 if and only if the test result is accepted. To obtain the security of the above protocol against Bob, for any attack where E_0 and E_1 are honestly choosen, we show that there exists a factor of security $\xi > 0$ such that $I(B; V|Pass = 1 \wedge C = 1) \times \Pr(Pass = 1) \leq 2^{-\xi n}$.

6 Bob's view

We must determine what kind of information Bob can obtain about b. Let us assume that the possible values (b, w, θ) of (B, W, Θ) are stored in orthonormal states $|b, w, \theta\rangle_C$. The entire view of Bob can be seen as the outcome of a measurement executed on $|b, w, \theta\rangle_C|\psi_{w,\theta}\rangle$. This measurement is not executed by Bob alone. For instance, the announcement of θ by Alice is part of this measurement: it corresponds to the extraction of the information θ from the state $|b, w, \theta\rangle_C$. Furthermore, we shall generously assume that at the end, after that Bob has finished his attack, Alice announces $w[\bar{E}_c]$ to Bob.

Let us analyse the operation M_v associated with a view v. At step 4 the measurement operates only on $|\psi_{w,\theta}\rangle$ and returns $\hat{w}$: we consider the classical computation of $\hat{w}$ as part of the measurement executed by a dishonest Bob. The corresponding operation on the photons is denoted $M_{\hat{w}}$. At step 5, R is chosen by Alice and announced to Bob, but this has no effect on the initial state. At step 6 Alice announces θ. The corresponding operation on the initial state is of the form $M_{\theta,\hat{w}} = P_\theta M_{\hat{w}}$ where P_θ is the projection $|\theta\rangle\langle\theta|_C$ which corresponds to the announcement of θ.

Let P_s and P_a be respectively the projection that corresponds to the announcement of s and a, that is, P_s projects on the span of the states $|w[E_c]\rangle_C$ such that $S = s$ and P_a projects on the span of the states $|b, w[E_c]\rangle_C$ such that $A = T(w[E_c]) \oplus b = a$. Note that, because Bob could have some initial information about b, the condition $A = a$ may actually provide information about $t = b \oplus a$. Finally, let P_w be the projection $|w[\bar{E}_c]\rangle\langle w[\bar{E}_c]|_C$ which corresponds to the announcement of $w[\bar{E}_c]$.

Note that Bob has no advantage in measuring the photons at step 6 (because he creates E_0 and E_1 honestly). So the operation $M_{\hat{w}}$ on the photons at step 5 remains the same at step 6. At step 7, Alice announces the information for privacy amplification and error correction, but this is under Alice's control and operates only on the classical part of the initial state. Certainly, at step 8, Bob is free to execute on the residual state of the photons the complete measurement of his choice. The final operation on the initial state $|b, w, \theta\rangle_C|\psi_{w,\theta}\rangle$ is of the form $M_v = P_C|v\rangle\langle\phi_v|$ where $|v\rangle\langle\phi_v|$ operates on $|\psi_{w,\theta}\rangle$ and P_C is the projection $P_w P_a P_s P_\theta$ on the classical part $|b, w, \theta\rangle_C$.

7 The small distance property

In this section, we want to find a property on M_v that can be proven using the fact that Bob must pass the test. Of course, we also want a property that

implies that Bob has no information when $c = 1$. We recall that no more than δn positions i for which $\theta_i = \hat{\theta}_i$ and $w_i \neq \hat{w}_i$ are tolerated in the test.

Let us consider an example in which Bob stores some photons and measures them only after that the bases have been announced by Alice. Let $\epsilon = 8\delta$. Bob cannot store much more than ϵn photons, because otherwise he will not pass the test: half of the photons are used for the test, half of these tested photons will be in the correct basis and half of these will create an error. Consider the case where Bob stores exactly ϵn photons. Let F be the set of stored photons and $\bar{F}$ the set of non stored photons. To pass the test, Bob measures the non stored photons using the commited string of bases $\hat{\theta}[\bar{F}]$ and obtains $\hat{w}[\bar{F}]$. After that he has learned all the classical information that Alice announces, Bob measures the stored photons in the correct bases $\theta[F]$ and obtains $w[F]$. The value $(\hat{w}, \hat{\theta}, \theta)$ is fixed in the final view v and the corresponding final operation $|v\rangle\langle\phi_v|$ on the photons is such that $|\phi_v\rangle = |\psi_{\hat{w},\hat{\theta}}[\bar{F}]\rangle|\psi_{w,\theta}[F]\rangle$. We don't care about the final state $|v\rangle$.

In which way the dishonest vector $|\phi_v\rangle = |\psi_{\hat{w},\hat{\theta}}[\bar{F}]\rangle|\psi_{w,\theta}[F]\rangle$ is close from the honest vector $|\phi_v\rangle = |\psi_{\hat{w},\hat{\theta}}\rangle$? If we expand the state $|\psi_{\hat{w},\hat{\theta}}[\bar{F}]\rangle|\psi_{w,\theta}[F]\rangle$ in the basis $\{|\psi_{\hat{w},\hat{\theta}}\rangle\}$, we obtain $|\psi_{\hat{w},\hat{\theta}}[\bar{F}]\rangle|\psi_{w,\theta}[F]\rangle = \sum_\alpha \lambda_\alpha |\psi_{\alpha,\hat{\theta}}\rangle$ where $\lambda_\alpha \neq 0$ only if we have $\alpha[\bar{F}] = \hat{w}[\bar{F}]$. In particular, we must have $d(\alpha, \hat{w}) \leq \epsilon n$. Of course, Bob could choose the photons that he stores at random and in view of the previous outcomes. In this case, we cannot expect that, for some fixed set F, $\alpha[\bar{F}] = \hat{w}[\bar{F}]$ implies $\lambda_\alpha = 0$. However, it is reasonnable to expect that $\lambda_\alpha \neq 0$ implies $d(\alpha, \hat{w}) \leq \epsilon n$. That is, the state $|\phi_v\rangle$ must be in the span of the states $|\psi_{\alpha,\hat{\theta}}\rangle$ with $d(\alpha, \hat{w}) \leq \epsilon n$. This is exactly the property that is called the low weight property by Yao [27]. In Yao's proof, $\epsilon = 1/40$. The test of the QOT protocol in Yao's proof tolerates no error at all: $\delta = 0$. However, Yao's proof works exactly in the same way even when $\delta > 0$ in the QOT protocol. In section 10 we shall briefly scketch an alternative proof that shows that, for all practical purposes, this property holds.

Let us formulate the low-weight property in terms of M_v and the set E_c. We consider E_c because it contains the relevant positions. Let $E \subseteq \{1, \ldots, n\}$ be any set of positions and ϵ be some small positive number. Let $d_E(\alpha, \alpha') = \#\{i \in E \mid \alpha_i \neq \alpha'_i\}$. If $E = \{1, \ldots, n\}$, then $d_E(\alpha, \alpha')$ is the usual Hamming distance. We denote $W_1[E, \epsilon n]$ the space generated by the states $|\psi_{\alpha,\hat{\theta}}\rangle$ where $d_E(\alpha, \hat{w}) \leq \epsilon n$. We denote $W_0[E, \epsilon n]$ the space generated by the states $|\psi_{\alpha,\hat{\theta}}\rangle$ where $d_E(\alpha, z) > \epsilon n$. We denote $P_j[E, \epsilon n]$ the projection on $W_j[E, \epsilon n]$.

Let $P_0 = P_0[E_c, \epsilon n]$ and $P_1 = P_1[E_c, \epsilon n]$. A vector $|\phi\rangle$ in the state space of the photons has the ϵn-small distance property if and only if $P_0|\phi\rangle = 0$. In other words, it must be in $W_1[E_c, \epsilon n]$. The operation M_v has the ϵn-small-distance property if and only if, for every (b, w, θ), $M_v P_0 \, |b, w, \theta\rangle_C |\psi_{w,\theta}\rangle = 0$. The small-distance property corresponds to what Yao calls the low-weight property in [27]. Note that the small distance property concerns only the positions in E_c whereas Yao defines the low weight property in terms of all the positions. This difference is not so important: it is clear that $W_1[\{1, \ldots, n\}, \epsilon n]$ is a subspace of $W_1[E_c, \epsilon n]$, so Yao's low-weight property implies the small distance property.

8 Using the small distance property

We now show that if the small distance property holds and $c = 1$, then v provides no information at all on b. This corresponds to a generalization of lemma 1 in Yao's paper [27].

Lemma 1. *Let $C_0^{\perp}$ be the span of the rows of the matrix f seen as vectors in $GF(2)^N$. Let $d \times N$ be the minimal distance of $C_0^{\perp}$. If $\epsilon n < \frac{d \times N}{2}$, $c = 1$ and M_v has the ϵn-small distance property, then the outcome v provides no information at all on the string b.*

Proof. The basic idea is to show that, for a fixed v such that $c = 1$, the probability of $V = v$ given $B = b$, denoted $p(v|b)$, is the same for all b. For every (w', θ'), let $p(v|b, w', \theta') = \Pr(V = v | B = b \wedge W = w \wedge \Theta = \theta')$. We have that $p(v|b) = 4^{-n} \sum_{w',\theta'} p(v|b, w', \theta')$. Let $\mathcal{P}_{v,b}$ be the set of pair (w', θ') such that

$$P_C |b, w', \theta'\rangle_C \neq 0. \tag{1}$$

Equation (1) must hold if we want to have $p(v|b, w', \theta') \neq 0$. Since, we are only interested in (w', θ') that contributes to $p(v|b)$, in what follows we may assume that (1) always hold, that is, we only consider the pair (w', θ') in $\mathcal{P}_{v,b}$.

We obtain that P_C operates as the identity operator on $|b, w', \theta'\rangle_C$. Furthermore, one may easily check that (1) implies that we can express the ϵn-small distance property on M_v via the following equation.

$$\langle \phi_v | P_0 | \psi_{w',\theta'} \rangle = 0. \tag{2}$$

Because of these two facts, from hereafter we can ignore the classical part of the initial state in our computation.

Equation (1) implies $w'[\bar{E}_c] = w[\bar{E}_c]$, $\theta' = \theta$, $gw[E_c] = s$ and $hw[E_c] = t = b \oplus a$. The two last constraints can be written in one equation $fw[E_c] = x$ where x is the concatenation of s and t. The only degree of freedom is $\beta = w'[E_c]$ restricted by $f\beta = x$. Let $C_x = \{\beta \in \{0,1\}^N \mid f\beta = x\}$. There is a one-to-one correspondence between $\beta \in C_x$ and $(w', \theta') \in \mathcal{P}_{v,b}$. Let $p(v|\beta) = p(v|b, w', \theta')$ and $|\psi_{\beta,\theta}\rangle = |\psi_{w',\theta'}\rangle$. Ignoring the classical part of the initial state, using (2) we obtain $p(v|\beta) = |\langle \phi_v | \psi_\beta \rangle|^2 = |\langle \phi_v | P_0 + P_1 | \psi_\beta \rangle|^2 = |\langle \phi_v | P_1 | \psi_\beta \rangle|^2$.

Now, we would like to restrict our analysis to the photons with position in E_c. One may insert the projection $P = |\psi_{w,\theta}[E_c]\rangle\langle\psi_{w,\theta}[E_c]|$ in front of the state $|\psi_{\beta,\theta}\rangle$ because this projection is implicit in the definition of this state. One obtains $p(v|\beta) = |\langle \phi_v | P_1 P | \psi_{\beta,\theta} \rangle|^2$. These two projections commute, so we obtain $p(v|\beta) = |\langle \phi'_v | P_1 | \psi_{\beta,\theta} \rangle|^2$ where $|\phi'_v\rangle = P|\phi_v\rangle$. Note that $|\phi'_v\rangle = |\psi_{w,\theta}[\bar{E}_c]\rangle|\phi''_v\rangle$ and $|\psi_{\beta,\theta}\rangle = |\psi_{w,\theta}[\bar{E}_c]\rangle|\tilde{\psi}_{\beta,\theta}\rangle$ where both $|\phi''_v\rangle$ and $|\tilde{\psi}_{\beta,\theta}\rangle$ are states for the photons with position in E_c. Finally, we obtain that $p(v|\beta) = |\langle \phi''_v | P_1 | \tilde{\psi}_{\beta,\theta} \rangle|^2 = |\langle \tilde{\phi}_v | \tilde{\psi}_{\beta,\theta} \rangle|^2$ where $|\tilde{\phi}_v\rangle = P_1|\phi''_v\rangle$ has the ϵn-small-distance property. Now, let us consider the density operators

$$\rho_x = 2^{-k} \sum_{\beta \in C_x} |\tilde{\psi}_{\beta,\theta}\rangle\langle\tilde{\psi}_{\beta,\theta}|$$

where $k = N - r - m$. We shall show that these density operators cannot be distinguished by any state $|\tilde{\phi}\rangle$ that has the ϵn-small distance property. In section 9, it is shown that, in the context $E_c = E_1$, for every $\beta \in C_x$, the matrix representation of ρ_x in Bob's basis $\{|\tilde{\psi}_{\alpha,\hat{\theta}}\rangle \mid \alpha \in \{0,1\}^N\}$ is given by

$$(\rho_x)_{\alpha,\alpha'} = 2^{-N} \times \begin{cases} 0 & \text{if } (\alpha \oplus \alpha') \notin C_0^{\perp} \\ (-1)^{(\alpha \oplus \alpha') \otimes \beta} & \text{otherwise} \end{cases}$$

For every pair of distinct strings $x, x' \in \{0,1\}^{m+r}$, we have that $(\Delta\rho)_{\alpha,\alpha'} = (\rho_x)_{\alpha,\alpha'} - (\rho_{x'})_{\alpha,\alpha'} \neq 0$ if and only if $(\alpha \oplus \alpha') \in C_0^{\perp}$ and, for every $\Delta\beta \in C_{x \oplus x'}$, $\Delta\beta \odot (\alpha \oplus \alpha') = 1$. We only need to use the fact that a neccessary condition for $(\Delta\rho)_{\alpha,\alpha'} \neq 0$ is that $(\alpha \oplus \alpha')$ belongs to the dual $C_0^{\perp}$ and is different from 0. Therefore, a necessary condition for $(\Delta\rho)_{\alpha,\alpha'} \neq 0$ is that $d(\alpha, \alpha') > dn$. Therefore, for every (α, α') such that $(\Delta\rho)_{\alpha,\alpha'} \neq 0$, one of $|\psi_{\alpha,\hat{\theta}}\rangle$ or $|\psi_{\alpha',\hat{\theta}}\rangle$ belongs to $W_0[E, \epsilon n]$. We obtain

$$\langle\phi|\Delta\rho|\phi\rangle = \sum_{\alpha,\alpha'} (\Delta\rho)_{\alpha,\alpha'} \langle\phi|\tilde{\psi}_{\alpha,\hat{\theta}}\rangle\langle\tilde{\psi}_{\alpha',\hat{\theta}}|\phi\rangle = 0$$

This concludes the proof. □

9 The density matrices

In this section, we consider only the photons with positions in $E_1 = E_c$. Therefore $\hat{\theta}$ is the *opposite* of θ, that is, $(\forall i)\, \hat{\theta}_i \neq \theta_i$. We temporarily remove the tilde over the symbol ψ. It is as if we considered the general situation where N photons are sent from Alice to Bob in a string of bases $\theta \in \{+, \times\}^N$ and we want to find the matrix representation of the density operators

$$\rho_x = \sum_{\beta \in C_x} |\psi_{\beta,\theta}\rangle\langle\psi_{\beta,\theta}|$$

in the opposite basis $\{|\psi_{\alpha,\hat{\theta}}\rangle\}$. This computation in the easy case $r = 0$ and $m = 1$ has been done independently by Mor [7] and the author of this paper. Actually, Mor considered the case in which the states $|0\rangle_{\theta_i}$ and $|1\rangle_{\theta_i}$ are not necessarily orthogonal. The case with no restriction on r and m has been done after we saw [7] for the case $r = 0$ and $m = 1$ and get some additional insight from it. In this paper, we are only interested in the orthogonal case. Sometime after we finished our work, Mor did in a different context, independently and using another approach an analysis of the non orthogonal case [8].

Before we begin with the computation, we need some basic tool. For every vector $\beta \in GF(2)^N$, the mapping $\beta' \mapsto \beta' \oplus \beta$ on $GF(2)^n$ corresponds to a unitary transformation U_β on the state space of the photons defined via $U_\beta|\psi_{\beta',\theta}\rangle = |\psi_{\beta \oplus \beta',\theta}\rangle$. One may easily check that, for every position i where $\beta_i = 1$, the transformation U_β maps $|0\rangle_{\hat{\theta}_i}$ into itself and $|1\rangle_{\hat{\theta}_i}$ into $-|1\rangle_{\hat{\theta}_i}$. So, if there is an even number of positions i where $\alpha_i = \beta_i = 1$, we have

$U_\beta|\psi_{\alpha,\hat{\theta}}\rangle = |\psi_{\alpha,\hat{\theta}}\rangle$, otherwise, we have $U_\beta|\psi_{\alpha,\hat{\theta}}\rangle = -|\psi_{\alpha,\hat{\theta}}\rangle$. In terms of the operation $\odot$ on the vector space $GF(2)^n$, we have

$$U_\beta|\phi_{\alpha,\hat{\theta}}\rangle = \begin{cases} |\psi_{\alpha,\hat{\theta}}\rangle & \text{if } \beta \odot \alpha = 0 \\ -|\psi_{\alpha,\hat{\theta}}\rangle & \text{if } \beta \odot \alpha = 1 \end{cases}$$

For every $\beta \in C_x$, we have $C_x = C_0 \oplus \beta$. Therefore, for every $\beta \in C_x$,

$$\rho_x = U_\beta \rho_0 U_\beta, \tag{3}$$

where we have used $U_\beta^\dagger = U_\beta$. For any operator ρ and any β, one may easily check that, in Bob's basis,

$$(U_\beta \rho U_\beta)_{\alpha,\alpha'} = (-1)^{(\alpha \oplus \alpha') \odot \beta} \times (\rho)_{\alpha,\alpha'}. \tag{4}$$

Therefore, the main task to accomplish is the computation of the matrix representation of the density operator ρ_0 in Bob's basis.

Let $k = N-m-r$ and $\{\beta_1, \ldots, \beta_k\}$ be a basis of C_0. For every $j = 1, \ldots, k$, let $C^{(j)}$ be the span of $\{\beta_1, \ldots, \beta_j\}$ and $\rho^{(j)} = 2^{-j} \sum_{\beta \in C^{(j)}} |\psi_{\beta,\theta}\rangle\langle\psi_{\beta,\theta}|$. Note that $\rho_0 = \rho^{(k)}$ and $C_0 = C^{(k)}$. We shall show by induction on j, that for $j = 0, \ldots, k$,

$$(\rho^{(j)})_{\alpha,\alpha'} = 2^{-N} \times \begin{cases} 0 & \text{if } (\alpha \oplus \alpha') \notin C^{(j)\perp} \\ 1 & \text{otherwise} \end{cases} \tag{5}$$

The case $j = 0$ can be easily computed: $C^{(0)} = \{0\}$ and $C^{(0)\perp} = GF(2)^n$. We assume that it holds for j and obtain it for $j+1$. Because $C^{(j+1)} = C^{(j)} \cup (C^{(j)} \oplus \beta_{j+1})$, we have that

$$\rho_0^{(j+1)} = 1/2(\rho_0^{(j)} + U_{\beta_{j+1}} \rho_0^{(j)} U_{\beta_{j+1}}). \tag{6}$$

Therefore, using formula 4, we obtain

$$(\rho^{(j+1)})_{\alpha,\alpha'} = 1/2(\rho^{(j)})_{\alpha,\alpha'}(1 - (-1)^{(\alpha \oplus \alpha') \odot \beta_{j+1}}).$$

Note that $(\rho^{(j+1)})_{\alpha,\alpha'}$ is either 0 or 2^{-N}. We obtain that $(\rho^{(j+1)})_{\alpha,\alpha'} = 2^{-N}$ if and only if $(\rho^{(j)})_{\alpha,\alpha'} \neq 0$ and $(\alpha \oplus \alpha') \odot \beta_{j+1} = 0$. So, $(\rho^{(j+1)})_{\alpha,\alpha'} = 2^{-N}$ if and only if, for every $\beta \in C^{(j+1)}$, $(\alpha \oplus \alpha') \odot \beta = 0$. This last condition is equivalent to $(\alpha \oplus \alpha') \in C^{(j+1)\perp}$. This concludes the induction. Using our computation of $\rho_0 = \rho^{(k)}$, together with formula 3 and 4, we finally obtain that, for every $\beta \in C_x$,

$$(\rho_x)_{\alpha,\alpha'} = 2^{-N} \times \begin{cases} 0 & \text{if } (\alpha \oplus \alpha') \notin C_0^\perp \\ (-1)^{(\alpha \oplus \alpha') \otimes \beta} & \text{otherwise} \end{cases}$$

10 Proving the small distance property

Here we briefly explain why, for all practical purposes, the small distance property must hold. A complete proof is found in [27].

Let us consider an example where Bob chooses a random bit OK and stores all the photons when only when $OK = 1$. In this case, Bob passes the test with a probability a little bit greater than $1/2$ and the small distance property holds with probability $1/2$. The point is that we should not expect that, if Bob has a significant probability to pass the test, then the small distance property always holds. In this example, except with negligible probability, the small distance property holds when Bob passes the test.

Consider another example where Bob commits $\hat{\theta} = +^n$, measures every photon in a fixed basis θ' and commits the outcome $\hat{w}$ of this measurement. The fixed basis θ' cannot be too far away from $+$ because otherwise Bob will not pass the test. Without loss of generality, assume that the magnitude of ${}_+\langle 0|0\rangle_{\theta'} = {}_+\langle 1|1\rangle_{\theta'} = c_{\theta'}$ is close to 1 and the magnitude of ${}_+\langle 0|1\rangle_{\theta'} = {}_+\langle 1|0\rangle_{\theta'} = s_{\theta'}$ is close to 0. The value $\hat{w}$ is included in v and $|\phi_v\rangle = |\psi_{\hat{w},\theta'}\rangle$. If we expand $|\phi_v\rangle$ in Bob's basis $+^n$ we obtain $|\phi_v\rangle = \sum_\alpha \langle \psi_{\alpha,+^n}|\psi_{\hat{w},\theta'}\rangle |\psi_{\alpha,+^n}\rangle$. Note that $|\langle \psi_{\alpha,+^n}|\psi_{\hat{w},\theta'}\rangle| = |s_{\theta'}|^{d(\alpha,\hat{w})} \times |d_{\theta'}|^{n-d(\alpha,\hat{w})}$. So the magnitude of $\lambda_\alpha = \langle \psi_{\alpha,+^n}|\psi_{\hat{w},\theta'}\rangle$ is very small when $d(\alpha,\hat{w})$ is large. We don't have exactly the small distance property, but for all practical purposes we have it.

The point of these two previous examples is that, in the general case, except with negligible probability, if Bob passes the test, then the small distance property *almost* holds. To prove it, let us define $Info$ as the binary random variable that takes the value 0 if and only if

$$\|M_v P_0 |\psi_{w,\theta}\rangle\| \leq 2^{-\gamma n} \|M_v |\psi_{w,\theta}\rangle\|. \tag{7}$$

This random variable is a function of the random values v and w. Note that the condition $Info = 0$ means that for all practical purposes v and w behave as if M_v had the ϵn-small distance property.

Let us pick some value $\gamma = 10^{-6}$. We want to obtain that if $\Pr(Pass = 1) > 2^{-\gamma n}$ then

$$\Pr(Info = 1 \mid Pass = 1) \leq 2^{-\tau n} \tag{8}$$

where τ is some function of γ. The difficulty with the variable $Info$ is that it concerns the final view of Bob. It would be easier to consider the situation just after the test. Therefore, let us consider the ratio

$$r(\theta, R, \hat{w}) = \frac{\mathrm{Tr}(P_0 \Pi_{\theta,\hat{w}} P_0 \rho)}{\mathrm{Tr}(\Pi_{\theta,\hat{w}} \rho)}$$

where ρ is Alice's preparation and $\Pi_{\theta,\hat{w}} = M^\dagger_{\theta,\hat{w}} M_{\theta,\hat{w}}$. We shall briefly scketch why $\Pr(Pass = 1) > 2^{-\gamma n}$ implies that

$$\langle r(\theta, R, \hat{w}) \rangle_{Pass=1} \leq 2^{-2\tau n} \tag{9}$$

This would do the job: expanding the expression $\langle r(\theta, R, \hat{w})\rangle_{Pass=1}$ and after some algebra, one obtains that (9) implies (8). Note that we can ignore the classical part $|w\rangle_C$ in (9). The density operator on the remaining part is simply, up to a factor, the identity operator. This density operator is best considered in Bob's basis $\{|\psi_{\alpha,\hat{\theta}}\rangle\}$ for the photons. Consider the situation where the information α is first read and next the operation $P_\theta M_{\hat{w}}$ is executed. Let $J[E]$ be the binary random variable that takes the value 0 if and only if $|\psi_{\alpha,\hat{\theta}}\rangle \in W_0[E, \epsilon n]$. The numerator and the denominator in the above ratio correspond respectively to $\Pr(J[E_c] = 0 \wedge \hat{W} = \hat{w} \wedge \Theta = \theta)$ and $\Pr(\hat{W} = \hat{w} \wedge \Theta = \theta)$. Note that given the random variables that exist before $P_w P_a P_s$ is executed, the random variable $Pass$ behaves as the random variable $J[T_0 \cap R]$. Equation 9 simply means that $\Pr(J[E_c] = 0 \wedge J[T_0 \cap R] = 1) \leq 2^{-2\tau n}$. This is not hard to show by considering the classical situation that we have after that $\hat{w}$ is fixed. This concludes our scketchy proof of this section.

We are grateful to Gilles Brassard, Claude Crépeau, Tal Mor and Andrew Yao for fruitful discussion.

References

1. C.H. Bennett, Quantum cryptography using any two nonorthogonal states, *Physical Review Letters*, vol. 68, no. 21, 25 May 1992, pp. 3121 – 2124.
2. 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.
3. C.H. Bennett and G. Brassard, The dawn of a new era for quantum cryptography: The experimental prototype is working!, *Sigact News*, vol. 20, no. 4, 1989,pp. 78–82.
4. 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. Preliminary version in Advances in Cryptology - *Eurocrypt '90 Proceedings*, May 1990, Springer – Verlag, pp. 253 – 265.
5. 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.
6. G. Brassard, C. Crépeau, M. Sántha, Oblivious Transfers and Intersecting Codes, *IEEE Transactions in Information Theory*, 1996, (to appear).
7. C.H. Bennett, T. Mor, J. Smolin, The Parity Bit in Quantum Cryptography, Los Alamos preprint archive `quant-ph/9604040`, April 1996.
8. E. Biham, T. Mor, On the Security of Quantum Cryptography Against Collective Attacks Los Alamos preprint archive `quant-ph/9605007`, May 1996.
9. C.H. Bennett, G. Brassard and N.D. Mermin, Quantum cryptography without Bell's theorem, *Physical Review Letters*, vol. 8, no. 5, 3 February 1992, pp. 557 – 559.
10. C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin and W.K. Wootters, Purification of Noisy Entanglement and Faithful Teleportation via Noizy Channels. *Physical Review Letters*, vol. 76, pp. 722 (1996).

11. C. Crépeau, Equivalence Between Two Flavors of Oblivious Transfers, *Advances in Cryptology* — Crypto '87 Proceeding, August 1987, Springer – Verlag, pp. 350 – 354.
12. C. Crépeau, Correct and Private Reductions among Oblivious Transfers, Ph.D. Thesis, Massachusetts Institute of Technology, 1990.
13. C. Crépeau, Quantum oblivious transfer, *Journal of Modern Optics*, vol. 41, no. 12, December 1994, pp. 2445 – 2454.
14. D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, A. Sanpera, Quantum privacy amplification and the security of quantum cryptography over noizy channels. Los Alamos preprint archive `quant-ph/9604039`, April 1996.
15. A.K. Ekert, Quantum cryptography based on Bell's theorem, *Physical Review Letters*, vol. 67, no. 6, 5 August 1991, pp. 661 – 663.
16. R. J. Hughes, G. G. Luther, G. L. Morgan, C. G. Peterson and C. Simmons Quantum cryptography over underground optical fibers, *Advances in Cryptology: Proceeding of CRYPTO'96.*
17. D. Mayers, On the security of the Quantum Oblivious Transfer and Key Distribution protocols, *Advances in Cryptology: Proceeding of CRYPTO'95*, Lecture Notes in Computer Science, vol. 963, Springer – Verlag, Berlin, 1995, pp. 124 – 135.
18. D. Mayers explained the details of his attack against the BCJL protocol at the 4th workshop on quantum information theory organized by G. Brassard in Montréal, October 1995.
19. D. Mayers, The Trouble with Quantum Bit Commitment, Los Alamos preprint archive `quant-ph/9603015`, Mars 1996.
20. D. Mayers, Unconditionally Secure Quantum Bit Commitment is impossible (to be published).
21. 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.
22. A. Muller, J. Breguet and N. Gisin, Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km, *Europhysics Letters*, vol. 23, no. 6, 20 August 1993, pp. 383 – 388.
23. J.G. Rarity, P.C.M. Owens and P.R. Tapster, Quantum random number generation and key sharing, *Journal of Modern Optics*, vol. 41, no. 12, December 1994, pp. 2435 – 2444.
24. P.D. Townsend, J.G. Rarity and P.R. Tapster, Single photon interference in a 10 km long optical fibre interferometer, *Electronics Letters*, vol. 29, no. 7, April 1993, pp. 634 – 635.
25. 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.
26. M.N. Wegman, J.L. Carter, New hash function and their use in authentification and set equality, *Journal of Computer and System Sciences*, vol. 22, 1981, pp. 265 – 279.
27. A. Yao, Security of Quantum Protocols Against Coherent Measurements, in *Proceedings of the 26th Symposium on the Theory of Computing*, June 1995, pp. 67 – 75.