Security of Quantum Protocols Against Coherent Measurements*

Andrew Chi-Chih Yao
Department of Computer Science
Princeton University
Princeton, New Jersey 08544

Abstract

The goal of quantum cryptography is to design cryptographic protocols whose security depends on quantum physics and little else. A serious obstacle to security proofs is the cheaters' ability to make *coherent* measurements on the joint properties of large composite states. With the exception of *commit* protocols, no cryptographic primitives have been proved secure when coherent measurements are allowed. In this paper we develop some mathematical techniques for analyzing probabilistic events in Hilbert spaces, and prove the security of a canonical quantum oblivious transfer protocol against coherent measurements.

1 Introduction

Work on quantum cryptography was started by Wiesner [Wi70] twenty-five years ago. Much knowledge on how to exploit quantum physics for cryptographic purposes has been gained through the work of Bennet and Brassard ([BBBW83][BB84][BBBSS92]), and later Crépeau ([Cr90][BC91][BBCS92][Cr94]). Furthermore, prototypes for implementing some of these algorithms have been built ([BB89][TRT93][TRT94]).

How to design securely the important cryptographic primitive *oblivious transfer* in quantum cryptography has received much attention in the recent literature [BBCS92][Cr90][Cr94][MS94]. Central to all the proposed protocols is the transmission of a large number of polarized photons from Alice to Bob. At present, the strongest security result [MS94] obtained is that if Bob is allowed to make arbitrary measurements only on *individual* photons, then neither Alice nor Bob may cheat successfully with more than an exponentially small probability. An interesting open question is whether these oblivious transfer protocols are secure when Bob may store these photons and make *coherent* measurements, i.e., measuring joint properties of these photons.

Coherent measurements seem to be beyond the current technology ([BBCS92]). However, it is of interest to design secure protocols based solely on quantum physics and not reliant on the limitation imposed by the available technology. It is particularly useful to examine the oblivious transfer primitive in this context, since it forms the basis of many other protocols (see [Ki88]). Previously, only the bit commitment primitive has been shown to have a protocol secure against coherent measurements [BCJL93].

In this paper we prove that the canonical quantum oblivious transfer protocol is secure against coherent measurements. For this extended abstract, we consider only the simplest environment for quantum oblivious tranfer, in which Alice's n packets of pho-

*This research was supported in part by the National Science Foundation under grant CCR-9301430.

STOC ' 95, Las Vegas, Nevada, USA
© 1995 ACM 0-89791-718-9/95/0005 .$3 50

tons each contains exactly one photon, that Bob receives and measures each packet perfectly, and thus Alice's test accepts the result only when there is perfect agreement between the corresponding bits in positions tested (where Bob's commited polarizations are the same as Alice's original ones). The security of the more practical protocols can be proved with modifications similar to those used in [BBCS92], and will be left to the complete paper.

Even for this ideal setting, it is a lengthy task to formulate the oblivious transfer problem precisely and prove a protocol secure. In the next section, we give a general formulation for protocols in the Hilbert space formalism. We then focus our attention on the canonical quantum oblivious transfer protocol, and the associated security problem against a cheating Bob. This way we have a concrete example of the formalism and can present the essence of the general proof without undue notational complications. A sketch of the proof is then given in the last section.

2 Model and Result

A (2-party) *quantum protocol* is a pair of quantum machines interacting through a quantum channel in some specified way. Initially, each machine is in some mixed quantum state. Formally, consider the direct product H of three Hilbert spaces H_A, H_B, H_C. Alternately between A and B, the party $D \in \{A, B\}$ carries out a measurement on the current mixed state using decompositions controlled in D's portion of the space (i.e., $H_D \otimes H_C$), which collapses the state according to the result of the measurement; D then carries out a unitary transformation in $H_D \otimes H_C$, which in turn induces a unitary transformation on the space H. The measurements and unitary transformations are designed so that in the end each of A amd B obtains some useful information about their joint initial state.

Although the above description is general enough to incorporate classical computations and transmissions of classical information, it is useful to separate out the classical parts in describing protocols. We also remark that to estimate the resources needed for the protocol one may want to give a less uniform description with H_A, H_B, H_C changing over time. For example, the number of photons used in the second round may be much less than in the first round, and thus can be described by a much smaller H_C.

We now specialize to the *oblivious transfer* problem (first raised by Rabin [Ra81]) whose goal is as follows. Alice has a secret bit β drawn from a certain distribution. At the end of the protocol, either Bob learns the value b (and knows it) or Bob gains no further information about b, with each possibility occurring with probability $1/2$; Alice learns nothing about which event takes place.

We consider a canonical quantum oblivious transfer protocol (as in [BBCS92]). Let $U = \{+, \times\}^n \times \{0, 1\}^n$, where $+$, $\times$ stand for the rectilinear and diagonal bases respectively.

Step 1: Alice picks a random uniformly chosen $u = (a, g) \in U$, and sends to Bob photons i, $1 \leq i \leq n$, with polarizations given by bases $a[i]$ and states $g[i]$.

Step 2: Bob picks a random uniformly chosen $b \in \{+, \times\}^n$, measures photons i in bases $b[i]$ and records the results as $h[i] \in \{0, 1\}$. (Following [MS94], call this the *first measurement.*) Bob then makes a quantum *commit* (as in [BCJL93]) of all n pairs $(b[i], h[i])$ to Alice.

Step 3: Alice picks a random uniformly chosen subset $R \subseteq \{1, 2, \cdots, n\}$, and tests the commitment made by Bob at positions in R. If any $i \in R$ reveals $a[i] = b[i]$ and $g[i] \neq h[i]$, then Alice stops the protocol; otherwise, the test result is *accepted.*

Step 4: Alice announces the base a. Let T_0 be the set of all $1 \leq i \leq n$ with $a[i] = b[i]$, and let T_1 be the set of all $1 \leq i \leq n$ with $a[i] \neq b[i]$. Bob chooses $I_0, I_1 \subseteq T_0 - R, T_1 - R$ with $|I_0| = |I_1| = 0.24n$, and sends $\{I_0, I_1\}$ in random order to Alice.

Step 5: Alice picks a random $s \in \{0, 1\}$, and sends $s, \beta_s = \beta \oplus_{i \in I_s} g[i]$ to Bob. Bob computes $\beta = \beta_s \oplus_{i \in I_s} h[i]$, if $I_s \subseteq T_0$; otherwise does nothing.

It is clear that the above protocol can be cast in the general form mentioned at the beginning of this section. It is also intuitively clear that the protocol performs correctly if both parties are honest. The harder part is to prove that the protocol satisfies certain desired security conditions even if either party cheats. As mentioned in the Introduction, we focus on the case when Bob is the cheater. (The protocol is also secure against a cheating Alice; we will discuss that further in the complete paper.)

We first give an informal generic description of Bob's possible strategies against the basic protocol. After Alice sends the photons in Step 1, Bob performs a first measurement J on the photons by possibly interacting them with another quantum system he has prepared. Depending on the measurement result $\mathbf{j} = j$, he then makes quantum commits (b, h) to Alice.

Alice picks a random R, and tests the commitment made by Bob at positions in R. If the test is passed, Alice announces the base a. Bob then chooses I_0, I_1 and sends them to Alice. Alice sends s, β_s to Bob.

Bob performs a *second* measurement with result $\mathbf{k} = k$. Note that the second measurement is chosen after Bob learns the values of a, R, s and β_s. Let $\mathbf{X}$ be the random variable corresponding to the state of Bob at the end of the protocol (i.e., j, k, a, R, s, β_s when available).

In each step of the way, Bob may choose to behave in any way. For the classical steps, this freedom is formulated in the standard cryptological way. For the quantum steps, it means that Bob is allowed to perform an arbitrary measurement followed by a unitary transformation. It is not difficult to formulate the above description in Hilbert space terms.

We state the security result first, and then start to discuss the problem more precisely in mathematical notation. We prove the following security result for the protocol.

Theorem 1 There exist constants $\epsilon, \delta > 0$ such that

$$\Pr\left\{ \text{ Info}(\beta|\mathbf{X}) > e^{\;\epsilon n}\right\} \leq 1/2 + \epsilon^{\;\delta n},$$

where $Info(\beta|\mathbf{X})$ is the Shannon information $H(\beta) - H(\beta|\mathbf{X})$.

We identify each $u \in U$ as a unit vector in $\mathbf{C}^N$ where $N = 2^n$. Let B be the Hilbert space (i.e., the set of states of the outside quantum system prepared by Bob to help him cheat) that Bob employs to interact with u, with $\eta \in B$ being the the vector (initial quantum state) prepared by Bob. Consider the Hilbert space $B \otimes \mathbf{C}^N$, in which Bob performs the first measurement J on the initial vector $\eta \otimes u$. From now on we use the notation W for $\eta \otimes \mathbf{C}^N$. For any vector $u \in \mathbf{C}^N$, we use $\hat{u}$ to denote $\eta \otimes u$.

Bob then makes a unitary transformation in $B \otimes \mathbf{C}^N$ corresponding to sending photons for the quantum commit protocol. Alice takes a measurement in $\mathbf{C}^N$ in accordance with the commit protocol. (Strictly speaking, we should choose a much large N (such as 2^{n^2}) so that there is enough states for the commit protocol. We will not do that here, since we will not have to deal with the commit question in this extended abstract.) After some more classical steps, Bob performs the second measurement K on $B \otimes \mathbf{C}^N$, this time trying to gather as much information as possible about β.

We have given the mathematical formulation for the description of an arbitrary cheating Bob. To analyze the security question, one needs to define probability for various events. We will discuss them in the next section. In the remainder of the current section, we introduce some useful notation.

Let $V \subseteq U$ be the set of $u - (+^n, g)$ with $g \in \{0, 1\}^n$; let $V_d \subseteq V$ be the subset of those with number of 1's in g not greater than d. Note that $V = V_n$. We also may regard V and V_d as sets of unit vectors in C^N, just as U can be viewed in this fashion.

Consider any finite-dimensional Hilbert space. For any vector v and subspace V, let v_V denote the projection of v on V. Let L, M be two subspaces. For any vector w, let $\chi(w, M, L) =< w, ((w_M)_L)_M >$.

Note that if $w \in M$, then $\chi(w, M, L) =< w, (w_L)_M >=< w, w_L >= \|w_L\|^2$. In particular, assume that Alice chooses an initial vector u, if L is a subspace corresponding to a result j for Bob's first measurement, then $\chi(\hat{u}, W, L)$ is equal to the probability for the outcome of the first measurement to be j. The following fact is easy to verify.

Fact 1 Let $t_i, 1 \leq i \leq r$ be vectors in L forming a complete POV, i.e., $\sum_{1 \leq i \leq r} |t_i >< t_i| = 1$ in L. Then

$$\chi(w, M, L) = \sum_i | < w, (t_i)_M > |^2.$$

We now introduce some concepts to quantify how much information can be obtained by Bob. Let $\ell_1 \leq \ell_2 \leq m$ be integers. For any $F \subseteq \{1, 2, \cdots, m\}$ and $y = y_1 y_2 \cdots y_m \in \{0,1\}^m$, the *$F$-parity* of y is $\oplus_{i \in F} y_i$. Let Y_F be the set of y with F-parity equal to 0. For any probability distribution τ on $\{0,1\}^m$, let $p(\tau, F) = \sum_{y \in Y_F} \tau(y)$ and $p(\tau, \ell_1, \ell_2)$ be the value of $p(\tau, F)$ maximizing the difference $|p(\tau, F) - 1/2|$ over all $\ell_1 \leq |F| \leq \ell_2$. In other words, $p(\tau, \ell_1, \ell_2)$ is the best you can do if you want to choose an F with size between ℓ_1 and ℓ_2, and try to predict accurately the F-parity of a random y distributed according to τ.

3 Proof of the Theorem

Because of the form of Theorem 1, we can assume without loss of generality that the second measurement is taken independent of the two bits s, β_s. Let j be any possible result of the first measurement. We further assume that Bob makes an honest commitment (b, h) in Step 2, in the sense that Bob has some specific bits in mind and carry out the quantum commit [BCJL93] dutifully. (It takes extra work to remove these assumptions, which will be given in the complete paper.)

To establish Theorem 1, we give Bob free additional information just before Bob attempts the second measurement K (if Alice has accepted the test result). We supply to Bob the values of $g[i]$ for all positions i with $a[i] = b[i]$. Recall $T_0 = \{i | a[i] = b[i]\}$, and $T_1 = \{i | a[i] \neq b[i]\}$. Let $g_0 = (g[i] | i \in T_0)$ and $g_1 = (g[i] | i \in T_1)$.

Before choosing and performing the second measurement K, Bob has full information about $S = (a, R, g_0)$. Let $\rho_{j,S,k}$ denote the probability distribution of g_1 when the measurement yields result k. Let $\epsilon = \delta = 10^{-6}$. Let $\mathbf{Y}$ be the event that Alice's test is passed. Let $\mathbf{Z}$ denote the event that $|p(\rho_{j,S,k}, 0.12n, 0.24n) - 1/2| > e^{-\epsilon n}$.

We will prove that

$$\Pr\{\mathbf{Y} \wedge \mathbf{Z} \,|\, \mathbf{j} = j\} < O(e^{-\delta n/64}). \qquad (1)$$

This immediately leads to Theorem 1, since at least one of I_0, I_1 must have an intersection with $T_1(a)$ of size between $0.12n$ and $0.24n$, and Alice may choose that I_s. (This is the same argument as was used in [MS94] when only individual measurements are allowed by Bob.)

From now on we consider j to be fixed. Without loss of generality, assume that $b = +^n$ and $h = 0^n$. We also suppress j in some notations; for example, $\rho_{j,S,k}$ will be written as $\rho_{S,k}$. Let $L \subseteq B \otimes \mathbf{C}^N$ be the subspace corresponding to $J = j$. For any $a \in \{+, \times\}^n$, let $T_0(a) = \{i | a[i] = +\}$ and $T_1(a) = \{i | a[i] = \times\}$.

Let $\mathcal{S}$ be the set of $S = (a, R, g_0)$ satisfying $|T_s(a) - 0.5n| \leq 0.01n$ and $0.24n \leq |T_s(a) - R| \leq 0.26n$ for $s \in \{0, 1\}$. The following fact is useful.

Fact 2 $\sum_{S \notin \mathcal{S}} \Pr\{\mathbf{S} = S | \mathbf{j} = j\} \leq 3e^{-\delta n}$.

Proof After the first measurement with result $\mathbf{j} = j$, the system is up to a normalization factor in the mixed state $\sum_{u \in U} |\hat{u}_L >< \hat{u}_L|$. We will show that for this mixed state, the probability of $|T_s(a) - 0.5n| \geq 0.01n$ for some $s \in \{0, 1\}$ is less than $e^{-\delta n}$.

This clearly implies Fact 2, since for any given s and a, $T_s(a) - R$ is statistically a uniform random subset of $T_s(a)$; and for $0.49n \leq |T_s(a)| \leq 0.51n$, the probability for $|T_s(a) - R|$ to be outside the range of $0.24n$ to $0.26n$ is less than $e^{-\delta n}$.

Let v be any unit vector in L. Consider the mixed state (up to a normalization factor)

$$\sum_{u\in U} |(\acute{u})_v >< (\acute{u})_v|. \qquad (2)$$

It suffices to show that, for this mixed state, the probability of $|T_1(a) - 0.5n| \geq 0.01n$ is less than $e^{-\delta n}$. (The $s = 0$ case is implied by this result, since $|T_0(a)| = n - |T_1(a)|$.)

By the definition of projection, one can write v_W as $\eta \otimes \sum_{\alpha\in V} \lambda_\alpha \alpha$. Let $U_m \subseteq U$ be the set of (a, g) with $|T_1(a)| = m$. Then the probability of $|T_1(a)| = m$ is proportional to

$$\begin{aligned}\sum_{u\in U_m} &| < \acute{u}, v > |^2 \\ &= \sum_{u\in U_m} | < u, \sum_{\alpha\in V} \lambda_\alpha \alpha > |^2 \\ &= \sum_{\alpha,\beta\in V} \sum_{u\in U_m} \lambda_\alpha \lambda^*_\beta < u, \alpha >< \beta, u > .\end{aligned}$$

A calculation shows that $\sum_{u\in U_m} < u, \alpha >< \beta, u >$ is equal to 0 if $\alpha \neq \beta$ and $\binom{n}{m} 2^m (2^{-m/2})^2 = \binom{n}{m}$ if $\alpha = \beta$. It follows that the probability of $|T_1(a)| = m$ is exactly $\binom{n}{m}/2^n$ for the mixed state (2), and hence the probability of $|T_1(a) - 0.5n| \geq 0.01n$ is less than $e^{-\delta n}$. This proves Fact 2. □

To prove (1), we first consider a special case. Let $\epsilon' = 1/40$. Assume that L has the following *low weight* property: the projection of every vector $v \in L$ on W is of the form $\acute{u}$ where u is a linear combination of vectors in $V_{\epsilon' n}$.

Lemma 1 For any $S \in \mathcal{S}$ and any k,

$$\Pr\{\mathbf{Z} \,|\, \mathbf{j} = j, \mathbf{S} = S, \mathbf{k} = k\} = 0.$$

Proof Let $S = (a, R, g_0^{(0)})$. Let $m = |T_1(a)| \geq 0.49n$. Let $v = t_k \in L$ be the vector corresponding to the measurement result $\mathbf{k} = k$. By assumption, one can write v_W as $\eta \otimes \sum_{\alpha\in V_{\epsilon' n}} \lambda_\alpha \alpha$.

We are interested in the probability distribution of the string $g_1 = (g_1[i] | i \in T_1(a)) \in \{0, 1\}^m$. For each $x \in \{0, 1\}^m$, let $u_x = (a, g)$ where $g_0 = g_0^{(0)}$ and $g_1 = x$.

Let $\gamma = \sum_y | < \acute{u}_y, v > |^2$. Then

$$\rho_{S,k}(x) = | < \acute{u}_x, v > |^2/\gamma.$$

Consider any $F \subseteq T_1(a)$ with $0.12n \leq |F| \leq 0.24n$. We have

$$\begin{aligned}\gamma &\sum_{x\in Y_F} \rho_{S,k}(x) \\ &= \sum_{x\in Y_F} | < \acute{u}_x, v > |^2 \\ &= \sum_{x\in Y_F} | < \acute{u}_x, v_W > |^2 \\ &= \sum_{x\in Y_F} \sum_{\alpha,\beta\in V_{\epsilon' n}} \lambda_\alpha \lambda^*_\beta < u_x, \alpha >< \beta, u_x > \\ &= \sum_{\alpha,\beta\in V_{\epsilon' n}} \lambda_\alpha \lambda^*_\beta \sum_{x\in Y_F} < u_x, \alpha >< \beta, u_x > .\end{aligned}$$

Let V' be the set of all $\alpha = (+^n, g) \in V_{\epsilon' n}$ with $g[i] = g_0^{(0)}[i]$ for all $i \in T_0[a]$. Let $\alpha = (+^n, g_\alpha), \beta = (+^n, g_\beta) \in V'$. For any x, let σ_x be the number of positions $i \in T_1(a)$ satisfying $g_\alpha[i] \neq g_\beta[i]$ and $g[i] = 1$ (where $u_x = (a, g)$). Then $< u_x, \alpha >< \beta, u_x >= (-1)^{\sigma_x} 2^{-m}$. In particular, $| < u_x, \alpha > |^2 = 2^{-m}$. If $\alpha \neq \beta$, there must be an equal number of $x \in Y_F$ with even and odd σ_x, as the Hamming distance between α and β is $\leq 2\epsilon' n < |F|$. This implies $\sum_{x\in Y_F} < u_x, \alpha >< \beta, u_x >= 0$.

For all other $\alpha, \beta \in V_{\epsilon' n}$, it is easy to see that $< u_x, \alpha >< \beta, u_x >= 0$ for all x. Thus, $\sum_{x\in Y_F} < u_x, \alpha >< \beta, u_x >= 0$ for all $\alpha \neq \beta$. This leads to

$$\begin{aligned}\gamma &\sum_{x\in Y_F} \rho_{S,k}(x) \\ &= \sum_{\alpha\in V_{\epsilon' n}} \sum_{x\in Y_F} |\lambda_\alpha|^2 | < u_x, \alpha > |^2 \\ &\quad + \sum_{\alpha,\beta\in V_{\epsilon' n}} \lambda_\alpha \lambda^*_\beta \sum_{x\in Y_F} < u_x, \alpha >< \beta, u_x > \\ &= 2^{-m} |Y_F| \sum_{\alpha\in V'} |\lambda_\alpha|^2 \\ &= (1/2) \sum_{\alpha\in V'} |\lambda_\alpha|^2.\end{aligned}$$

A similar calculation (summing x over all m-bit strings) shows that $\gamma = \sum_{\alpha\in V'} |\lambda_\alpha|^2$. This shows that $\sum_{x\in Y_F} \rho_{S,k}(x) = 1/2$. This proves Lemma 1. □

It follows from Fact 2 and Lemma 1 that

$$\begin{aligned}\Pr\{&\mathbf{Y} \wedge \mathbf{Z} \,|\, \mathbf{j} = j\} \\ &\leq \sum_{S\not\in\mathcal{S}} \Pr\{\mathbf{S} = S | \mathbf{j} = j\} +\end{aligned}$$

$$\sum_{S\in\mathcal{S}}\sum_{k}\Pr\{\mathbf{S}=S,\mathbf{k}=k|\mathbf{j}=j\} \times \Pr\{\mathbf{Z}\,|\,\mathbf{j}=j,\mathbf{S}=S,\mathbf{k}=k\} \le 3e^{-\delta n}.$$

This proves (1) for the Special Case. We now turn to the general case. Our plan is show that we can approximate the quantity $| < \hat{u}_x, v > |^2 - | < \hat{u}_x, (t_k)_W > |^2$ by $| < \hat{u}_x, (t_k)_{W_1} > |^2$ sufficiently accurately that we can carry out the calculations in the proof of Lemma 1 for the general case.

Let $W_1 \subseteq W$ be the subspace spanned by $\eta \otimes v$ where $v \in V_{\epsilon' n}$; let $W_2 \subseteq W$ be the subspace spanned by $\eta \otimes v$ where $v \in V_n - V_{\epsilon' n}$.

Recall that, for any $u \in U$, $\chi(\hat{u}, W, L)$ is equal to the probability of $\mathbf{j} = j$ when Alice initially prepares the photons in state u. Thus, for any $D \subseteq U$, $\frac{1}{|D|}\sum_{u\in D}\chi(\hat{u}, W, L)$ is the probability of $\mathbf{j} = j$, given that initially u is randomly chosen from D.

For each $S = (a, R, g_0)$, let $\Gamma_S \subseteq U$ be the set of $u = (a, g)$ consistent with S. Let ξ_S be the probability that Alice accepts the test result, given that S is the current state with j being the result of the first measurement. (In the present situation, ξ_S is either 0 or 1.)

Definition Let $\mathcal{T}$ be the set of S satisfying

$$\xi_S \sum_{u\in\Gamma_S}\chi(\hat{u}, W_2, L) \le e^{-\delta n/4}\sum_{u\in\Gamma_S}\chi(\hat{u}, W, L).$$

For any $S = (a, R, g_0)$, consider the second measurement $t_1, t_2, \cdots, t_\ell$ (with $\sum_k |t_k >< t_k| = 1$ on L) chosen by Bob.

Definition Let $K_0(S)$ denote the set of the measurement results k such that

$$\xi_S \sum_{u\in\Gamma_S} | < \hat{u}, (t_k)_{W_2} > |^2 \le e^{-\delta n/8}\sum_{u\in\Gamma_S} | < \hat{u}, (t_k)_W > |^2.$$

Let $\mathcal{T}' = \mathcal{T} \cap \mathcal{S}$. There are two phenomena we like to demonstrate. First, take a random execution of the protocol, we show that we get an $S \in \mathcal{T}'$ and $k \in K_0(S)$ with probability $1 - O(e^{-\delta n/8})$; this is (essentially) done in the next two lemmas. Second, $S \in \mathcal{T}'$ and $k \in K_0(S)$ implies that we can replace W by W_1 when we do certain calculations involving a random u from Γ_S.

Lemma 2 states that, conditioned on $\mathbf{j} = j$, the probability for $S \notin \mathcal{T}$ is less than $e^{-\delta n/4}$. The 2^n factor on the left-hand side comes from the fact that S is defined as (a, g_0, R), and thus each u has 2^n S with $u \in \Gamma_S$.

Lemma 2

$$\frac{1}{2^n}\frac{1}{|U|}\sum_{S\notin\mathcal{T}}\sum_{u\in\Gamma_S}\chi(\hat{u}, W, L) \le e^{-\delta n/4}\frac{1}{|U|}\sum_{u\in U}\chi(\hat{u}, W, L).$$

Proof We delay the proof to the end of this section. □

Lemma 3 If $S \in \mathcal{T}$, then

$$\sum_{k\notin K_0(S)}\sum_{u\in\Gamma_S} | < \hat{u}, (t_k)_W > |^2 \le e^{-\delta n/8}\sum_{u\in\Gamma_S}\chi(u, W, L).$$

Proof Otherwise, we have from the definition of $K_0(S)$,

$$\begin{aligned}\xi_S &\sum_{k\notin K_0(S)}\sum_{u\in\Gamma_S} | < \hat{u}, (t_k)_{W_2} > |^2\\ &> \sum_{k\notin K_0(S)}\sum_{u\in\Gamma_S} e^{-\delta n/8} | < \hat{u}, (t_k)_W > |^2\\ &> e^{-\delta n/8}e^{-\delta n/8}\sum_{u\in\Gamma_S}\chi(u, W, L),\end{aligned}$$

contradicting the assumption $S \in \mathcal{T}$. This proves Lemma 3. □

Now for the second step. Let $S \in \mathcal{T}'$ and $k \in K_0(S)$. We show that either $\xi_S \le e^{-\delta n/16}$ or

$$\Pr\{\mathbf{Z}\,|\,\mathbf{j} = j, \mathbf{S} = S, \mathbf{k} = k\} < O(e^{-\delta n/64}). \qquad (3)$$

(We do not take advantage of the fact ξ_S being either 0 or 1, to keep the discussion more general than needed for the present case.)

Equation (3) is the analog of Lemma 1 for the general case. As in the special case discussed at the start of this section, (3) and the discussions preceding it imply immediately (1) and hence Theorem 1.

If $\xi_S \leq e^{-\delta n/16}$, then we are done. Assume $\xi_S > e^{-\delta n/16}$. Since $k \in K_0(S)$, we have

$$\xi_S \sum_{u \in \Gamma_S} | < \hat{u}, (t_k)_{W_2} > |^2 \leq e^{-\delta n/8} \sum_{u \in \Gamma_S} | < \hat{u}, (t_k)_W > |^2.$$

As $\xi_S > e^{-\delta n/16}$, we have

$$\sum_{u \in \Gamma_S} | < \hat{u}, (t_k)_{W_2} > |^2 < e^{-\delta n/16} \sum_{u \in \Gamma_S} | < \hat{u}, (t_k)_W > |^2. \quad (4)$$

Let Γ'_S be the set of $u \in \Gamma_S$ satisfying

$$| < \hat{u}, (t_k)_{W_2} > |^2 \leq e^{-\delta n/32} | < \hat{u}, (t_k)_W > |^2.$$

Then

$$\sum_{u \in \Gamma_S - \Gamma'_S} | < \hat{u}, (t_k)_W > |^2 \leq e^{-\delta n/32} \sum_{u \in \Gamma_S} | < u, (t_k)_W > |^2;$$

since otherwise, we have

$$\begin{aligned} \sum_{u \in \Gamma_S - \Gamma'_S} & | < \hat{u}, (t_k)_{W_2} > |^2 \\ & > e^{-\delta n/32} \sum_{u \in \Gamma_S - \Gamma'_S} | < \hat{u}, (t_k)_W > |^2 \\ & > e^{-\delta n/32} e^{-\delta n/32} \sum_{u \in \Gamma_S} | < \hat{u}, (t_k)_W > |^2, \end{aligned}$$

contradicting (4). This means that, taking a random u chosen according to $\rho_{S,k}$, the probability of $u \in \Gamma'_S$ being true is greater than $1 - e^{-\delta n/32}$.

Take any $u \in \Gamma'_S$. Then

$$| < \hat{u}, (t_k)_{W_2} > | \leq e^{-\delta n/64} | < \hat{u}, (t_k)_W > |.$$

Hence

$$\begin{aligned} | < \hat{u}, & (t_k)_{W_1} > | \\ & = | < \hat{u}, (t_k)_W > - < \hat{u}, (t_k)_{W_2} > | \\ & \geq | < u, (t_k)_W > | - | < \hat{u}, (t_k)_{W_2} > | \\ & \geq (1 - e^{-\delta n/64}) | < \hat{u}, (t_k)_W > |. \end{aligned}$$

Thus,

$$\begin{aligned} | < \hat{u}, & (t_k)_{W_1} > |^2 \\ & \leq | < \hat{u}, (t_k)_W > |^2 \\ & \leq (1 + O(e^{-\delta n/64})) | < \hat{u}, (t_k)_{W_1} > |^2. \end{aligned}$$

To summarize, we have shown that for a typical S that passes Alice' test, the information (about the initial vector u) available to Bob after the second measurement is almost identical to that in the special case discussed earlier. The arguments used in the proof of Lemma 1 can then be used to prove (3).

To complete the proof of Theorem 1, it remains to prove Lemma 2, to which we now turn our attention.

Let ξ_u be the probability that Alice accepts the test, conditioned on u being the initial vector and the first measurement yielding result j. Note that $\xi_u = 2^{-n} \sum_{S, u \in \Gamma_S} \xi_S$.

Fact 3 Let $\alpha, \beta \in V_n$. If $\alpha \neq \beta$, then $\sum_{u \in U} \xi_u < u, \alpha >< \beta, u >= 0$.

Proof It can be verified by a simple calculation. □

Fact 4 Let $\alpha \in V_n - V_{\epsilon' n}$. Then $\sum_{u \in U} \xi_u | < u, \alpha > |^2 < 2^{(1-\delta)n}$.

Proof Let ℓ be the number of 1's in α; by definition, $\ell > \epsilon' n$. For any $a \in \{+, \times\}^n$, let $\#a$ denote the number of i with $a[i] = +$ and $\alpha[i] = 1$. Divide U into $U_1 \cup U_2$, where U_1 is the set of $u = (a, g)$ with $\#a \geq \ell/4$, and U_2 is the set of those u with $\#a < \ell/4$.

Let $u = (a, g) \in U$. Then $| < u, \alpha > |^2 = 0$ unless $g[i] = \alpha[i]$ whenever $a[i] = +$, and in this latter case $| < u, \alpha > |^2 = 2^{-(n - r_a)}$ where r_a is the number of $+$'s in a. It follows that

$$\begin{aligned} \sum_{u \in U_2} & | < u, \alpha > |^2 \\ & \leq \sum_{0 \leq m < \ell/4} \sum_{0 \leq m' \leq n - \ell} \binom{\ell}{m} \binom{n - \ell}{m'} \\ & \qquad \times 2^{n-(m+m')} 2^{-(n-(m+m'))} \\ & \leq 2^{(1-\delta)n}/2. \end{aligned}$$

Now, note that any $u \in U_1$ must satisfy $\xi_u \leq 2^{-\delta n}/2$.

We have thus

$$\begin{aligned}\sum_{u\in U}\xi_u| < u,\alpha > |^2 & \\ &\leq \sum_{u\in U_2} | < u,\alpha > |^2 + \sum_{u\in U_1} \xi_u | < u,\alpha > |^2 \\ &< 2^{(1-\delta)n} + (2^{-\delta n}/2) \sum_{u\in U_1} | < u,\alpha > |^2 \\ &\leq 2^{(1-\delta)n}.\end{aligned}$$

This proves Fact 4. □

Fact 5

$$\sum_{u\in U}\xi_u\chi(\hat{u},W_2,L) \leq e^{-\delta n/2}\sum_{u\in U}\chi(\hat{u},W,L).$$

Proof Choose any orthonormal base $t_1, t_2, \cdots, t_\ell$ for L. By Fact 1, we have

$$\begin{aligned}\sum_{u\in U}\xi_u\chi(\hat{u},W_2,L) & \\ &= \sum_{u\in U}\xi_u\sum_{i}| < \hat{u},(t_i)_{W_2} > |^2 \\ &= \sum_{i}\sum_{u\in U}\xi_u| < \hat{u},(t_i)_{W_2} > |^2. \quad (5)\end{aligned}$$

We will prove that for each i

$$\begin{aligned}\sum_{u\in U}\xi_u| < \hat{u},(t_i)_{W_2} > |^2 & \\ &\leq e^{-\delta n/2}\sum_{u\in U}| < \hat{u},(t_i)_W > |^2. \quad (6)\end{aligned}$$

Clearly, (5), (6) and Fact 1 imply

$$\begin{aligned}\sum_{u\in U}\xi_u\chi(\hat{u},W_2,L) & \\ &\leq e^{-\delta n/2}\sum_{u\in U}\sum_{i}| < \hat{u},(t_i)_W > |^2 \\ &= \epsilon^{\ \delta n/2}\sum_{u\in U}\chi(\hat{u},W,L).\end{aligned}$$

To prove (6), assume that $(t_i)_W - \eta\otimes\sum_{\alpha\in V_n}\lambda_\alpha\alpha$. Then $(t_i)_{W_2} = \eta\otimes\sum_{\alpha\in V_n-V_{\epsilon' n}}\lambda_\alpha\alpha$. Thus,

$$\begin{aligned}\sum_{u\in U}\xi_u| < \hat{u},(t_i)_{W_2} > |^2 & \\ &= \sum_{u\in U}\xi_u| < u, \sum_{\alpha\in V_n-V_{\epsilon' n}}\lambda_\alpha\alpha > |^2 \\ &= \sum_{u\in U}\sum_{\alpha,\beta\in V_n-V_{\epsilon' n}}\xi_u\lambda_\alpha\lambda_\beta^* < u,\alpha > < \beta,u > \\ &= \sum_{\alpha,\beta\in V_n-V_{\epsilon' n}}\lambda_\alpha\lambda_\beta^*\sum_{u\in U}\xi_u < u,\alpha > < \beta,u > .\end{aligned}$$

Using Facts 3, 4, we then have

$$\begin{aligned}\sum_{u\in U}\xi_u| < \hat{u},(t_i)_{W_2} > |^2 & \\ &= \sum_{\alpha\in V_n-V_{\epsilon' n}}|\lambda_\alpha|^2\sum_{u\in U}\xi_u| < \hat{u},\alpha > |^2 \\ &\leq 2^{(1-\delta)n}\sum_{\alpha\in V_n-V_{\epsilon' n}}|\lambda_\alpha|^2. \quad (7)\end{aligned}$$

Similarly, we have

$$\begin{aligned}\sum_{u\in U}| < \hat{u},(t_i)_W > |^2 & \\ &= \sum_{\alpha,\beta\in V_n}\lambda_\alpha\lambda_\beta^*\sum_{u\in U} < u,\alpha > < \beta,u > \\ &= \sum_{\alpha\in V_n}|\lambda_\alpha|^2 2^n \\ &\geq 2^n\sum_{\alpha\in V_n-V_{\epsilon' n}}|\lambda_\alpha|^2. \quad (8)\end{aligned}$$

Clearly, (7) and (8) imply (6), and hence Fact 5. □

We now prove Lemma 2. Assume to the contrary,

$$\frac{1}{2^n}\sum_{S\notin T}\sum_{u\in\Gamma_S}\chi(\hat{u},W,L) > e^{-\delta n/4}\sum_{u\in U}\chi(\hat{u},W,L).$$

Then, from the definition of T and the above inequality, we have

$$\begin{aligned}\frac{1}{2^n}\sum_{\text{all } S}\xi_S\sum_{u\in\Gamma_S}\chi(\hat{u},W_2,L) & \\ &\geq \frac{1}{2^n}\sum_{S\notin T}\xi_S\sum_{u\in\Gamma_S}\chi(\hat{u},W_2,L) \\ &> \frac{1}{2^n}\epsilon^{-\delta n/4}\sum_{S\notin T}\sum_{u\in\Gamma_S}\chi(\hat{u},W,L) \\ &> e^{-\delta n/2}\sum_{u\subset U}\chi(\hat{u},W,L). \quad (9)\end{aligned}$$

Now

$$\begin{aligned}\sum_{\text{all } S}\xi_S\sum_{u\in\Gamma_S}\chi(\hat{u},W_2,L) & \\ &= \sum_{u\in U}2^n\chi(\hat{u},W_2,L)\frac{1}{2^n}\sum_{S,u\in\Gamma_S}\xi_S \\ &= \sum_{u\in U}2^n\chi(\hat{u},W_2,L)\xi_u, \quad (10)\end{aligned}$$

From (9) and (10) we have

$$\sum_{u\in U}\xi_u\chi(\hat{u},W_2,L) > e^{-\delta n/2}\sum_{u\in U}\chi(\hat{u},W,L),$$

contradicting Fact 5. This proves Lemma 2 and thus Theorem 1.

References

[BB84] C. Bennet and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, December 1984, 175-179.

[BB89] C. Bennet and G. Brassard, "The dawn of a new era for quantum cryptography: the experimental prototype is working," *SIGACT News*, **20** (1989), 78-82.

[BBBSS92] C. Bennet, F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, **5** (1992), 3-28.

[BBBW83] C. Bennet, G. Brassard, S. Breidbard, and S. Wiesner, "Quantum cryptography, or unforgeable subway tokens," in *Advances in Cryptology: Proceedings of CRYPTO'82*, Plenum Press, 1983, 267-275.

[BBCS92] C. Bennet, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, "Practical quantum oblivious transfer," in *Proceedings of CRYPTO'91*, Lecture Notes in Computer Science, Volume 576, Springer-Verlag, Berlin, 1992, 351-366.

[BC91] G. Brassard and C. Crépeau, "Quantum bit commitment and coin tossing protocols," in *Advances in Cryptology: Proceedings of CRYPTO'90*, Lecture Notes in Computer Science, Volume 537, Springer-Verlag, Berlin, 1991, 49-61.

[BCJL93] G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois, "A quantum bit commitment scheme provably unbreakable by both parties," *Proceedings of 1993 IEEE Annual Symposium on Foundations of Computer Science*, November 1993, 362-369.

[Cr90] C. Crépeau, "Correct and private reductions among oblivious transfers," Ph.D. thesis, Department of EECS, MIT, 1990.

[Cr94] C. Crépeau, "Quantum oblivious transfer," in *Journal of Modern Optics*, special issue on quantum cryptography, to appear.

[Ki88] J. Kilian, "Founding cryptography on oblivious transfer," *Proceedings of 1988 ACM Annual Symposium on Theory of Computing*, May 1988, 20-31.

[Ma94b] D. Mayers, "Quantum transformation and generalized measurements," preprint, distributed at *Workshop on Quantum Computing and Communication*, National Institute of Standards and Technology, Gaithersburg, Maryland, August 18-19, 1994.

[MS94] D. Mayers and L. Salvail, "Quantum oblivious transfer is secure against individual measurements," preprint, distributed at *Workshop on Quantum Computing and Communication*, National Institute of Standards and Technology, Gaithersburg, Maryland, August 18-19, 1994.

[Ra81] M. Rabin, "How to exchange secrets by oblivious transfer," technical report TR-81, Aiken Computation Laboratory, Harvard University, 1981.

[TRT93] P. Townsend, J. Rarity, and P. Tapster, "Single photon interference in a 10km long optical fibre interferometer," *Electronic letters*, **29** (1993), 634-635.

[TRT94] P. Townsend, J. Rarity, and P. Tapster, "Enhanced single photon visibility in a 10km long prototype quantum cryptography channel," *Electronic letters*, to appear.

[Wi70] S. Wiesner, "Conjugate coding," *SIGACT News* **15** (1983), 78-88; manuscript *circa* 1970.