Lower Bounds for Quantum Oblivious Transfer

André Chailloux*
LRI
Université Paris-Sud
andre.chailloux@lri.fr

Iordanis Kerenidis*
CNRS - LRI
Université Paris-Sud
jkeren@lri.fr

Jamie Sikora
IQC
University of Waterloo
jwjsikor@uwaterloo.ca

July 13, 2010

Abstract

Oblivious transfer is a fundamental primitive in cryptography. While perfect information theoretic security is impossible, quantum oblivious transfer protocols can limit the dishonest players' cheating. Finding the optimal security parameters in such protocols is an important open question. In this paper we show that every 1-out-of-2 oblivious transfer protocol allows a dishonest party to cheat with probability bounded below by a constant strictly larger than 1/2. Alice's cheating is defined as her probability of guessing Bob's index, and Bob's cheating is defined as his probability of guessing both input bits of Alice. In our proof, we relate these cheating probabilities to the cheating probabilities of a coin flipping protocol and conclude by using Kitaev's coin flipping lower bound. Then, we present an oblivious transfer protocol with two messages and cheating probabilities at most 3/4. Last, we extend Kitaev's semidefinite programming formulation to more general primitives, where the security is against a dishonest player trying to force the outcome of the other player, and prove optimal lower and upper bounds for them.

1 Introduction

Quantum information enables us to do cryptography with information theoretic security. The first breakthrough result in quantum cryptography is the unconditionally secure key distribution protocol of Bennett and Brassard [BB84]. Since then, a long series of work has studied which other cryptographic primitives are possible in the quantum world. However, the subsequent results were negative. Mayers and Lo, Chau proved the impossibility of secure ideal quantum bit commitment and oblivious transfer and consequently of any type of two-party secure computation [May97, LC97, DKSW07]. On the other hand, several

*Supported in part by ACI Securité Informatique SI/03 511 and ANR AlgoQP grants of the French Ministry and in part by the European Commission under the Integrated Project Qubit Applications (QAP) funded by the IST directorate as Contract Number 015848.

imperfect variants of these primitives have been shown to be possible. Finding the optimal parameters for such fundamental primitives has been since an important open question. The reason for looking at these abstract primitives is that they are the basis for all cryptographic protocols one may wish to construct, including identification schemes, digital signatures, electronic voting, etc. Let us emphasize that in this paper we only look at information theoretic security and we do not discuss computational security or security in restricted models like the bounded-storage or noisy-storage model.

We start with coin flipping, which was first proposed by Blum [Blu81] and has since found numerous applications in two-party secure computation. Even though the results of Mayers and of Lo and Chau exclude the possibility of perfect quantum coin flipping, i.e., where the resulting coin is perfectly unbiased, it still remained open whether one can construct a quantum protocol where no player could bias the coin with probability 1. Aharonov et al. [ATVY00] provided such a protocol where no dishonest player could bias the coin with probability higher than 0.9143. Then, Ambainis [Amb01] described an improved protocol whose cheating probability was at most 3/4. Subsequently, a number of different protocols had been proposed [SR01, NS03, KN04] that achieved the same bound of 3/4.

On the other hand, Kitaev [Kit03], using a formulation of quantum coin flipping as semidefinite programs proved a lower bound of 1/2 on the product of the cheating probabilities for Alice and Bob (see [ABDR04]). In other words, no quantum coin flipping protocol can achieve a cheating probability less than $1/\sqrt{2}$ for both Alice and Bob.

The question of whether 3/4 or $1/\sqrt{2}$ was the right answer has recently been resolved by Chailloux and Kerenidis [CK09] who described a protocol with cheating probability arbitrarily close to $1/\sqrt{2}$. In their protocol they use as a subroutine a weaker variant of coin flipping which is referred to as *weak coin flipping*.

Weak coin flipping protocols with cheating probabilities less than 3/4 were first constructed in [SR02, Amb02, KN04]. The best bound was in fact $1/\sqrt{2}$ until the breakthrough result by Mochon who described a protocol with cheating probability 2/3 [Moc05] and then a protocol that achieves a cheating probability of $1/2 + \epsilon$ for any $\epsilon > 0$ [Moc07]. Hence the optimal biases for weak and strong coin flipping are now known.

The question is still unresolved for quantum bit commitment. On one hand, a bit commitment protocol implies a coin flipping protocol with the same parameters. In fact, most of the known strong coin flipping protocols are of this form: Alice first quantumly commits to a bit a. Then, Bob announces a bit b. Last, Alice reveals bit a and the result of the coin flip is $c = a \oplus b$. Hence, Kitaev's lower bound states that no quantum bit commitment protocol can achieve cheating probabilities lower than $1/\sqrt{2}$. On the other hand, the best protocols we know achieve a value of 3/4. In fact, the only strong coin flipping protocol that achieves a value better than 3/4 is the optimal protocol of Chailloux-Kerenidis, which is not based on a quantum bit commitment scheme, but on Mochon's weak coin flipping protocol. Hence, the question of the optimal bias for quantum bit commitment remains open.

In this paper, we focus on oblivious transfer, which is a universal primitive for any two-party secure computation [Rab81, EGL82, Cré87]. We define a 1-out-of-2 random oblivious transfer protocol with bias ε, denoted here as random-OT, to be a protocol where:

- Alice outputs two uniformly random bits (x_0, x_1)
- Bob outputs x_b for a uniformly random choice of b
- $A_{OT} := \sup\{\Pr[\text{Alice guesses } b \text{ and Bob does not abort }]\} = \frac{1}{2} + \varepsilon_A$
- $B_{OT} := \sup\{\Pr[\text{Bob guesses } (x_0, x_1) \text{ and Alice does not abort }]\} = \frac{1}{2} + \varepsilon_B$
- The bias of the protocol is defined as $\epsilon := \max\{\epsilon_A, \epsilon_B\}$

where the suprema are taken over all strategies for Alice and Bob respectively. Note that in our definition, the bias is not defined just as an upper bound on the cheating probabilities but corresponds to the optimal cheating probability.

We note here that an honest Bob can learn both bits with probability 1/2, since he can learn one bit prefectly and can make a random guess for the other bit.

There is also another variant, denoted as OT, where Alice and Bob have specific values of (x_0, x_1) and b as inputs. We show that the two notions are equivalent with respect to ε.

The first impossibility result for quantum OT with information theoretic security was shown by Lo [Lo97]. The main idea is that if Alice has no information about Bob's index b then Bob can learn both bits in the following way: first, Bob honestly runs the protocol with $b = 0$ to learn x_0 with probability 1; then he locally applies a unitary to his part of the joint final state in order to transform the joint state to the joint final state in the case of $b = 1$ and hence learn x_1. Since, Bob can learn each bit with probability 1, his measurement does not change the state and hence he can perform both of them sequentially.

However, not much was known about the best possible bias that one can get for OT. In high level, OT is the "strongest" primitive, since it implies bit commitment, coin flipping, and in fact any two-party functionality. However, when one looks at the optimal constant values for the bias, then one needs to be more careful. For example, the standard way of constructing a bit commitment protocol from OT is the following: Alice and Bob perform OT with inputs x_0, x_1, where $x_0 \oplus x_1$ is the committed bit. Since, Bob can learn only one of the two inputs, he has no information about the committed bit. On the other hand, in the reveal phase, Alice reveals both bits, and since she has no information about which one Bob has learnt, if she wants to change her mind without getting caught, she can only do it with probability 1/2 (hence her cheating probability is 3/4). Classically, one can then repeat this protocol many times in order to take this probability close to 1/2. As we can see, a perfect OT protocol does not automatically give a perfect bit commitment protocol, as there is a loss in the parameters. Hence, Kitaev's lower bound does not a priori hold for OT, since we do not know how to easily convert an OT protocol to a coin flipping protocol without any loss.

Let us also note that in the quantum setting, one can use a large number of bit commitment protocols in order to construct an OT protocol, something which is not known to be possible classically ([Yao95],[BF10]).

In related work, Salvail, Schaffner and Sotakova [SSS09] have quantitatively studied a different notion of security for OT protocols (and generally any two-party protocols) that they call information leakage. Information leakage is defined as the maximum amount of extra information about the other party's output given the quantum state held by one party. They prove, among other results, that any 1-out-of-2 OT protocol has a constant leakage. Their model is somewhat different, for example they do not allow the players to abort during the protocol, and their security notion is described in terms of mutual information and entropy and does not immediately translate to our security notion of guessing probabilities. However, their results provide more evidence that almost-perfect OT protocols are impossible for different variants of security.

In another work, Jain, Radhakrishnan and Sen [JRS02] showed that in a 1-out-of-n OT protocol, if Alice gets t bits of information about Bob's index b, then Bob gets at least $\Omega(n/2^{O(t)})$ bits of information about Alice's string x.

In this paper, we quantitatively study the bias of quantum oblivious transfer protocols. More precisely, we construct a coin flipping protocol that uses OT as a subroutine and show a relation between the cheating probabilities of the OT protocol and the ones of the coin flipping protocol. Then, using Kitaev's lower bound for coin flipping we derive a non-trivial lower bound (albeit weaker) on the cheating probabilities for OT. More precisely we prove the following theorem.

Theorem 1 *In any quantum oblivious transfer protocol, we have*

$$A_{OT} \cdot f(B_{OT}) \geq 1/2$$

where f is a function that we define later. This implies for the bias ϵ of the protocol that

$$\epsilon \geq \frac{1}{2}\left(\sqrt{\frac{1}{2}+2\sqrt{2}} - \sqrt{\frac{1}{2}}\right) - \frac{1}{2} \approx 0.0586.$$

Moreover, in Section 4 we describe a simple 1-out-of-2 random-OT protocol and analyze the cheating probabilities of Alice and Bob.

Theorem 2 *There exists a quantum oblivious transfer protocol such that $A_{OT} = B_{OT} = \frac{3}{4}$.*

One may wonder if it would be possible to extend Kitaev's semidefinite programming formulation to include the OT primitive and get a stronger lower bound this way. In fact, in Section 5 we describe a generalisation of Kitaev's semidefinite program that captures a variant of the general k-out-of-n OT primitive. Coin flipping, is then the special case of 1-out-of-1 OT. However, there is a big difference. What the semidefinite program formulation captures is the probability that one player can force the outcome of the other one.

More precisely, we define a k-out-of-n forcing oblivious transfer protocol, denoted here as $\binom{n}{k}$-fOT, with *forcing bias* ε as a protocol satisfying:

- Alice outputs n random bits $x := (x_1, \ldots, x_n)$
- Bob outputs a random index set b of k indices and bit string x_b consisting of x_i for $i \in b$
- $A_{b,x_b} := \sup\{\Pr[\text{Alice can force Bob to output } (b, x_b)]\} = \dfrac{\varepsilon_A}{\binom{n}{k} \cdot 2^k}$
- $B_x := \sup\{\Pr[\text{Bob can force Alice to output } x]\} = \dfrac{\varepsilon_B}{2^n}$
- The forcing bias of the protocol is defined as $\epsilon := \max\{\epsilon_A, \epsilon_B\}$

where, again, the suprema are over all strategies of Alice and Bob respectively. First, notice our definition of the bias ε as a multiplicative factor instead of additive. We choose this since the honest probabilities of the two players can be very different and in this case our definition makes more sense.

More importantly, this 'forcing' security definition is exactly what is needed in coin flipping, since there, Alice and Bob know each others outputs and the only cheating is forcing the other player's output in order to get a specific value for the coin. However, this is very different than the probability that one player can guess the outcome of the other player, which is the security guarantee we wish for in an *OT* protocol.

Nevertheless, it is still interesting to know how one can extend Kitaev's semidefinite programming formulation, what are the most general primitives that can be described in this framework, and what are their applications. For these k-out-of-n "forcing" primitives we provide optimal upper and lower bounds.

Theorem 3 *In any* $\binom{n}{k}$-fOT *protocol and consistent* b, x, x_b *we have*

$$B_x \cdot A_{b,x_b} \geq \Pr[\textit{Alice honestly outputs } x \textit{ and Bob honestly outputs } (b, x_b)] = \frac{1}{\binom{n}{k} 2^n}.$$

In particular, the forcing bias satisfies $\varepsilon \geq \sqrt{2}^k$.

Note that for the special case of coin flipping, or else $\binom{1}{1}$-fOT, our bounds are tight (a multiplicative bias of $\sqrt{2}$ is equivalent to a cheating probability of $\frac{1}{\sqrt{2}}$).

Similar to coin flipping, one can get optimal protocols as well for $\binom{n}{k}$-fOT.

Theorem 4 *Let $\gamma > 0$. There exists a protocol for $\binom{n}{k}$-fOT with cheating probabilities:*

$$A_{b,x_b} \leq \frac{\sqrt{2}^k(1+\gamma)}{\binom{n}{k} \cdot 2^k} \quad \text{and} \quad B_x \leq \frac{\sqrt{2}^k(1+\gamma)}{2^n}$$

for consistent b, x, x_b.

2 Preliminaries

2.1 Definitions of Primitives

We assume the reader is familiar with the basic notions of quantum computing. All used notions can be found in [NC00].

In the literature, many different variants of oblivious transfer have been considered. In this paper, we consider two variants of quantum oblivious transfer and for completeness we show that they are equivalent with respect to the bias ϵ.

Definition 1 (Random Oblivious Transfer) *A 1-out-of-2 quantum random oblivious transfer protocol with bias ϵ, denoted here as random-OT, is a protocol between Alice and Bob such that:*

- *Alice outputs two bits (x_0, x_1) or Abort and Bob outputs two bits (b, y) or Abort*
- *If Alice and Bob are honest, they never Abort, $y = x_b$, Alice has no information about b and Bob has no information about $x_{\overline{b}}$. Also, x_0, x_1, b are uniformly random bits.*
- $A_{OT} := \sup\{\Pr[\textit{Alice guesses } b \textit{ and Bob does not Abort}]\} = \frac{1}{2} + \epsilon_A$
- $B_{OT} := \sup\{\Pr[\textit{Bob guesses } (x_0, x_1) \textit{ and Alice does not Abort}]\} = \frac{1}{2} + \epsilon_B$
- *The bias of the protocol is defined as $\epsilon := \max\{\epsilon_A, \epsilon_B\}$*

where the suprema are taken over all cheating strategies for Alice and Bob.

Note that this definition is slightly different from usual definitions because we want the exact value of the cheating probabilities and not only an upper bound. This is because we consider both lower bounds and upper bounds for *OT* protocols but we could have equivalent results using the standard definitions.

An important issue is that we quantify the security against a cheating Bob as the probability that he can guess (x_0, x_1). One can imagine a security definition where Bob's guessing probability is not for (x_0, x_1), but for example for $x_0 \oplus x_1$ or any other function $f(x_0, x_1)$. Since we are mostly interested in lower bounds, we believe our definition is the most appropriate one, since a lower bound on the probability of guessing (x_0, x_1) automatically yields a lower bound on the probability of guessing any $f(x_0, x_1)$.

We now define a second notion of *OT* where the values (x_0, x_1) and b are Alice's and Bob's inputs respectively and show the equivalence between the two notions.

Definition 2 (Oblivious Transfer) *A 1-out-of-2 quantum oblivious transfer protocol with bias ϵ, denoted here as OT, is a protocol between Alice and Bob such that:*

- *Alice has input $x_0, x_1 \in \{0,1\}$ and Bob has input $b \in \{0,1\}$. At the beginning of the protocol, Alice has no information about b and Bob has no information about (x_0, x_1)*
- *At the end of the protocol, Bob outputs y or Abort and Alice can either Abort or not*
- *If Alice and Bob are honest, they never Abort, $y = x_b$, Alice has no information about b and Bob has no information about $x_{\overline{b}}$*
- $A_{OT} := \sup\{\Pr[\textit{Alice guesses } b \textit{ and Bob does not Abort}]\} = \frac{1}{2} + \epsilon_A$
- $B_{OT} := \sup\{\Pr[\textit{Bob guesses } (x_0, x_1) \textit{ and Alice does not Abort}]\} = \frac{1}{2} + \epsilon_B$
- *The bias of the protocol is defined as $\epsilon := \max\{\epsilon_A, \epsilon_B\}$*

where the suprema are taken over all cheating strategies for Alice and Bob.

We also define quantum (strong) coin flipping.

Definition 3 *A quantum coin flipping protocol with bias ϵ, denoted here as CF, is a protocol between Alice and Bob who agree on an output $a \in \{0, 1, Abort\}$ such that:*

- *If Alice and Bob are honest then* $\Pr[a = 0] = \Pr[a = 1] = \frac{1}{2}$
- $A_{CF} := \sup\{\max\{\Pr[a = 0], \Pr[a = 1]\}\} = \frac{1}{2} + \epsilon_A$
- $B_{CF} := \sup\{\max\{\Pr[a = 0], \Pr[a = 1]\}\} = \frac{1}{2} + \epsilon_B$
- *The bias of the protocol is defined as $\epsilon := \max\{\epsilon_A, \epsilon_B\}$*

where the suprema are taken over all strategies for Alice and Bob.

2.2 Equivalence between the different notions of Oblivious Transfer

We show the equivalence between OT and random-OT with respect to the bias ϵ.

Proposition 1 *Let P an OT protocol with bias ϵ. We can construct a random-OT protocol Q with bias ϵ using P.*

Proof The construction of the OT protocol Q is pretty straightforward:

1. Alice picks $x_0, x_1 \in_R \{0,1\}$ uniformly at random and Bob picks $b \in_R \{0,1\}$ uniformly at random.

2. Alice and Bob perform the OT protocol P where Alice inputs x_0, x_1 and Bob inputs b. Let y be Bob's output. Note that at this point, Alice has no information about b and Bob has no information about (x_0, x_1).

3. Alice and Bob abort in Q if and only if they abort in P. Otherwise, the outputs of protocol Q are (x_0, x_1) for Alice and (b, y) for Bob.

The outcomes of Q are uniformly random bits since Alice and Bob choose their inputs uniformly at random. All the other requirements that make Q an OT protocol with bias ϵ are satisfied because P is an OT protocol with bias ϵ.

We now prove how to go from a random-OT to an OT protocol.

Proposition 2 *Let P a random-OT protocol with bias ϵ_P. We can construct an OT protocol Q with bias $\epsilon_Q = \epsilon_P$ using P.*

Proof Let P a random-OT protocol with bias ϵ_P. Consider the following protocol Q:

1. Alice has inputs X_0, X_1 and Bob has an input B.

2. Alice and Bob run protocol P and output (x_0, x_1) for Alice and (b, y) for Bob.

3. Bob sends $r = b \oplus B$ to Alice. Let $x'_c = x_{c \oplus r}$, for $c \in \{0, 1\}$.

4. Alice sends to Bob (s_0, s_1) where $s_c = x'_c \oplus X_c$ for $c \in \{0, 1\}$. Let $y' = y \oplus s_B$.

5. Alice and Bob abort in Q if and only if they abort in P. Otherwise, the output of the protocol is y' for Bob.

We now show that our protocol is an OT protocol with inputs with bias ϵ. First, note that the values x'_c are known by Alice and the value y' is known by Bob. Also, notice that $x'_B = x_{B \oplus r} = x_b$.

- Alice and Bob are honest:
  By definition we have $y = x_b$. Then, we have $y' = y \oplus s_B = x_b \oplus s_B = x'_B \oplus s_B = X_B$. Moreover, Alice knows r but has no information about b and hence she has no information about $B = b \oplus r$. Bob knows (s_0, s_1) and r but has no information about $x_{\bar{b}}$, hence he has no information about $X_{\bar{B}} = x'_{\bar{B}} \oplus s_{\bar{B}} = x'_{\bar{b} \oplus r} \oplus s_{\bar{b} \oplus r} = x_{\bar{b}} \oplus s_{\bar{b} \oplus r}$.

- Cheating Alice:
  Alice picks r and $B = b \oplus r$. Hence

$$
\begin{aligned}
A_{OT}(Q) &= \sup\{\Pr[\text{Alice guesses } B \text{ and Bob does not Abort}]\} \\
&= \sup\{\Pr[\text{Alice guesses } b \text{ and Bob does not Abort}]\} = A_{OT}(P).
\end{aligned}
$$

- Cheating Bob: Bob picks a random r, sends r to Alice and then Alice picks (s_0, s_1). We have $X_c = x'_c \oplus s_c = x_{c\oplus r} \oplus s_c$ so it is equivalent for Bob to guess (X_0, X_1) and (x_0, x_1). Hence

$$\begin{aligned} B_{OT}(Q) &= \sup\{\Pr[\text{Bob guesses } (X_0, X_1) \text{ and Alice does not Abort}]\} \\ &= \sup\{\Pr[\text{Bob guesses } (x_0, x_1) \text{ and Alice does not Abort}]\} = B_{OT}(P). \end{aligned}$$

We can now conclude for the biases

$$\epsilon_Q = \max\{A_{OT}(Q), B_{OT}(Q)\} - \frac{1}{2} = \max\{A_{OT}(P), B_{OT}(P)\} - \frac{1}{2} = \epsilon_P.$$

2.3 Technical Claims

Claim 1 ([DW09] following [Nay99]) *Suppose we have a classical random variable X, uniformly distributed over $[n] = \{1, \ldots, n\}$. Let $x \to |\phi_x\rangle$ be some encoding of $[n]$, where $|\phi_x\rangle$ is a pure state in a d-dimensional space. Let $P_1, \ldots, P_n$ be the measurement operators applied for decoding; these sum to the d-dimensional identity operator. Then the probability of correctly decoding in case $X = x$ is*

$$p_x = ||P_x|\phi_x\rangle||^2 \leq \mathrm{Tr}(P_x).$$

The expected success probability is

$$\frac{1}{n}\sum_{x=1}^{n} p_x \leq \frac{1}{n}\sum_{x=1}^{n} \mathrm{Tr}(P_x) = \frac{1}{n}\mathrm{Tr}\left(\sum_{x=1}^{n} P_x\right) = \frac{1}{n}\mathrm{Tr}(I) = \frac{d}{n}.$$

Claim 2 *Let $|X\rangle$ be a pure state, Q a projection, and $|Y\rangle$ a pure state such that $Q|Y\rangle = |Y\rangle$. Then we have*

$$\|Q|X\rangle\|_2^2 \geq |\langle X|Y\rangle|^2.$$

Proof Using Cauchy-Schwarz we have

$$|\langle X|Y\rangle|^2 = |\langle X|Q|Y\rangle|^2 \leq \|Q|X\rangle\|_2^2 \, \||Y\rangle\|_2^2 = \|Q|X\rangle\|_2^2.$$

□

Claim 3 *Suppose $\theta, \theta' \in [0, \pi/4]$. If $|\langle\psi|\phi\rangle| \geq \cos(\theta)$ and $|\langle\phi|\xi\rangle| \geq \cos(\theta')$ then*

$$|\langle\psi|\xi\rangle| \geq \cos(\theta + \theta').$$

Proof Define the angle between two pure states $|\psi\rangle$ and $|\phi\rangle$ as $A(\psi, \phi) := \arccos|\langle\psi|\phi\rangle|$. This is a metric (see [NC00] page 413). Thus we have

$$\arccos|\langle\psi|\xi\rangle| = A(\psi, \xi) \leq A(\psi, \phi) + A(\phi, \xi) = \arccos|\langle\psi|\phi\rangle| + \arccos|\langle\phi|\xi\rangle| \leq \theta + \theta'.$$

Taking the cosine of both sides yields the result. □

Claim 4 *Let $\theta, \rho \in [0, \pi/4]$. Then*

$$\cos(\theta + \rho) \geq \cos^2(\theta) + \cos^2(\rho) - 1.$$

Proof Wlog suppose that $\theta \geq \rho$. Consider the function

$$f(\theta) = \cos(\theta + \rho) - \cos^2(\theta) + \sin^2(\rho)$$

for fixed ρ. Taking its derivative we get

$$f'(\theta) = -\sin(\theta + \rho) + \sin(2\theta)$$

which is nonnegative for $\theta \in [\rho, \pi/4]$. Since $f(\rho) = 0$, we conclude that $f(\theta) \geq 0$ for $\theta \in [\rho, \pi/4]$ which gives the desired result. □

3 A Lower Bound on Any Oblivious Transfer Protocol

In this section we prove that the bias of any random-OT protocol, and hence any OT protocol, is bounded below by a constant. We start from a random-OT protocol and first show how to construct a coin flipping protocol. Then, we prove a relation between the cheating probabilities of the coin flipping protocol and those in the random-OT protocol. Last, we use Kitaev's lower bound for coin flipping to derive a lower bound for any OT protocol.

3.1 From Oblivious Transfer to Coin Flipping

Coin Flipping Protocol via random-OT

1. Alice and Bob perform the OT protocol to create (x_0, x_1) and (b, x_b) respectively. If the OT protocol is aborted then so is the coin flipping protocol.
2. Alice sends $c \in_R \{0, 1\}$ to Bob.
3. Bob sends b and $y = x_b$ to Alice.
4. If x_b from Bob is consistent with Alice's bits then the output of the protocol is $c \oplus b$. Otherwise Alice aborts.

By definition, A_{OT} and B_{OT} denote the optimal cheating probabilities for Alice and Bob in the random-OT protocol and A_{CF} and B_{CF} denote the optimal cheating probabilities for Alice and Bob in the coin flipping protocol. Kitaev's lower bound says that $A_{CF}B_{CF} \geq 1/2$. We use this inequality to derive an inequality involving A_{OT} and B_{OT}.

Theorem 1 *In any quantum oblivious transfer protocol, we have*

$$A_{OT} \cdot f(B_{OT}) \geq 1/2$$

for the function f defined as[1]

$$f(z) = \frac{1}{6}(3\sqrt{3}\sqrt{27z^2 - 2z} + 27z - 1)^{1/3} + \frac{1}{6}(3\sqrt{3}\sqrt{27z^2 - 2z} + 27z - 1)^{-1/3} + 1/3.$$

This implies that the bias ϵ of the protocol satisfies

$$\epsilon \geq \frac{1}{2}\left(\sqrt{\frac{1}{2} + 2\sqrt{2}} - \sqrt{\frac{1}{2}}\right) - \frac{1}{2} \approx 0.0586.$$

In what follows we prove the above theorem.

Let $\neg\bot_A^{CF}$ (resp. $\neg\bot_B^{CF}$) denote the event "Alice (resp. Bob) does not abort during the entire coin flipping protocol". Let $\neg\bot_A^{OT}$ (resp. $\neg\bot_B^{OT}$) denote the event "Alice (resp. Bob) does not abort during the random-OT subroutine".

Cheating Alice By definition, A_{OT} is the optimal probability of Alice guessing b in the random-OT protocol without Bob aborting. Suppose Alice desires to force 0 in the coin flipping protocol (a similar argument can be made if she wants 1). Bob must not abort and Alice must send $c = b$ in her last message. Notice also that in our coin flipping protocol, Bob can abort only in the OT subroutine and hence $\neg\bot_B^{OT} \equiv \neg\bot_B^{CF}$. Thus,

$$A_{CF} = \sup\{\Pr[\text{ (Alice sends } c = b)\wedge\neg\bot_B^{CF}]\} = \sup\{\Pr[\text{ (Alice guesses } b)\wedge\neg\bot_B^{OT}]\} = A_{OT}.$$

where the suprema are taken over all possible strategies for Alice.

Cheating Bob By definition, B_{OT} is the optimal probability of Bob learning both bits in the random-OT protocol without Alice aborting. Thus,

$$\begin{aligned} B_{OT} &= \sup\{\Pr[\text{ (Bob guesses } (x_0, x_1)) \wedge \neg\bot_A^{OT}]\} \\ &= \sup\{\Pr[\neg\bot_A^{OT}] \cdot \Pr[\text{ (Bob guesses } (x_0, x_1))|\neg\bot_A^{OT}]\}. \end{aligned}$$

where the suprema are taken over all strategies for Bob.

If Bob wants to force 0 in the coin flipping protocol (a similar argument works if he wants to force 1), then first, Alice must not abort in the random-OT protocol and second, Bob must send $b = c$ as well as the correct x_c such that Alice does not abort in the last round of the coin flipping protocol. This is equivalent to saying that Bob succeeds if he guesses x_c and Alice does not abort in the random-OT protocol. Since c is chosen by Alice uniformly at random, we can write the probability of Bob cheating as

[1] f is the inverse function of $g(x) = x(2x-1)^2$ on some domain, see the proof for more details.

$$\begin{aligned} B_{CF} &= \max \left\{ \frac{1}{2} \Pr[(\text{Bob guesses } x_0) \wedge \neg\bot_A^{OT}] + \frac{1}{2} \Pr[(\text{Bob guesses } x_1) \wedge \neg\bot_A^{OT}] \right\} \\ &= \max \left\{ \Pr[\neg\bot_A^{OT}] \cdot \left(\frac{1}{2} \Pr[(\text{Bob guesses } x_0) | \neg\bot_A^{OT}] + \frac{1}{2} \Pr[(\text{Bob guesses } x_1) | \neg\bot_A^{OT}] \right) \right\}. \end{aligned}$$

Notice that we use "max" instead of "sup" above. This is because an optimal strategy exists for every coin flipping protocol. This is a consequence of strong duality in the semidefinite programming formalism of [Kit03], see [ABDR04] for details.

Let us now fix Bob's optimal cheating strategy in the CF protocol. For this strategy, let $p = \Pr[(\text{Bob guesses } x_0)|\neg\bot_A^{OT}]$, $q = \Pr[(\text{Bob guesses } x_1)|\neg\bot_A^{OT}]$ and $a = \frac{p+q}{2}$. Note that wlog, we can assume that Bob's measurements are projective measurements. This can be done by increasing the dimension of Bob's space. Also, Alice has a projective measurement on her space to determine the bits (x_0, x_1).

We use the following lemma to relate B_{CF} and B_{OT}.

Lemma 1 (Learning-In-Sequence Lemma) *Let $p, q \in [1/2, 1]$. Let Alice and Bob share a joint pure state. Suppose Alice performs on her space a projective measurement $M = \{M_{x_0,x_1}\}_{x_0,x_1 \in \{0,1\}}$ to determine the values of (x_0, x_1). Suppose there is a projective measurement $P = \{P_0, P_1\}$ on Bob's space that allows him to guess bit x_0 with probability p and a projective measurement $Q = \{Q_0, Q_1\}$ on his space that allows him to guess bit x_1 with probability q. Then, there exists a measurement on Bob's space that allows him to guess (x_0, x_1) with probability at least $a(2a-1)^2$ where $a = \frac{p+q}{2}$.*

We postpone the proof of this lemma to Subsection 3.2.

We now construct a cheating strategy for Bob for the OT protocol: Run the optimal cheating CF strategy and look at Bob's state after step 1 conditioned on $\neg\bot_A^{OT}$. Note that this event happens with nonzero probability in the optimal coin flipping strategy since otherwise the success probability is 0. The optimal CF strategy gives measurements that allow Bob to guess x_0 with probability p and x_1 with probability q. Bob uses these measurements and the procedure of Lemma 1 to guess (x_0, x_1). Let b be the probability he guesses (x_0, x_1). From Lemma 1, we have that $b \geq a(2a-1)^2$. By definition of B_{OT} and B_{CF}, we have:

$$b = \Pr[\ (\text{Bob guesses } (x_0, x_1))|\neg\bot_A^{OT}] \leq \frac{B_{OT}}{\Pr[\neg\bot_A^{OT}]} \quad \text{and} \quad a = \frac{B_{CF}}{\Pr[\neg\bot_A^{OT}]}.$$

This gives us

$$\frac{B_{OT}}{\Pr[\neg\bot_A^{OT}]} \geq \frac{B_{CF}}{\Pr[\neg\bot_A^{OT}]} \left(2\frac{B_{CF}}{\Pr[\neg\bot_A^{OT}]} - 1 \right)^2 \implies B_{OT} \geq B_{CF} \left(2B_{CF} - 1 \right)^2,$$

where the implication holds since $B_{CF} \geq 1/2$.

We now calculate an upper bound on B_{CF} as a function of B_{OT}. Let $g(x) = x(2x-1)^2$. It can be easily checked that g is bijective from $[0.5, 1]$ to $[0, 1]$ and increasing. Let f be the inverse function of g from $[0, 1]$ to $[0, 0.5]$. Since g is increasing, f is also increasing. Hence, since $B_{OT} \geq g(B_{CF})$ and $B_{CF} \in [0.5, 1]$, we conclude that

$$B_{CF} \leq f(B_{OT}).$$

We can write f analytically using computer software to get the following function

$$f(z) = \frac{1}{6}(3\sqrt{3}\sqrt{27z^2 - 2z} + 27z - 1)^{1/3} + \frac{1}{6}(3\sqrt{3}\sqrt{27z^2 - 2z} + 27z - 1)^{-1/3} + 1/3.$$

Kitaev's lower bound states that $A_{CF}B_{CF} \geq 1/2$. From this, we have

$$A_{OT}f(B_{OT}) \geq A_{CF}B_{CF} \geq 1/2.$$

We now proceed to give the lower bound for the bias. Since f is increasing, we have

$$(\varepsilon + 1/2) \cdot f(\varepsilon + 1/2) \geq A_{OT}f(B_{OT}) \geq A_{CF}B_{CF} \geq 1/2.$$

Solving the inequality we show that ε must satisfy

$$\varepsilon \geq \frac{1}{2}\left(\sqrt{\frac{1}{2} + 2\sqrt{2}} - \sqrt{\frac{1}{2}}\right) - \frac{1}{2} \approx 0.0586.$$

□

3.2 Proof of the Learning-In-Sequence Lemma

The Learning-in-Sequence Lemma follows from the following simple geometric result.

Lemma 2 *Let $|\psi\rangle$ be a pure state and let $\{C, I - C\}$ and $\{D, I - D\}$ be two projective measurements such that*

$$\cos^2(\theta) := \|C|\psi\rangle\|_2^2 \geq \frac{1}{2} \quad \text{and} \quad \cos^2(\theta') := \|D|\psi\rangle\|_2^2 \geq \frac{1}{2}.$$

Then we have

$$\|DC|\psi\rangle\|_2^2 \geq \cos^2(\theta)\cos^2(\theta + \theta').$$

Proof Define the following states

$$|X\rangle := \frac{C|\psi\rangle}{\|C|\psi\rangle\|_2}, \quad |X'\rangle := \frac{(I - C)|\psi\rangle}{\|(I - C)|\psi\rangle\|_2}, \quad |Y\rangle := \frac{D|\psi\rangle}{\|D|\psi\rangle\|_2}, \quad |Y'\rangle := \frac{(I - D)|\psi\rangle}{\|(I - D)|\psi\rangle\|_2}.$$

Then we can write $|\psi\rangle = \cos(\theta)|X\rangle + e^{i\alpha}\sin(\theta)|X'\rangle$ and $|\psi\rangle = \cos(\theta')|Y\rangle + e^{i\beta}\sin(\theta')|Y'\rangle$ with $\alpha, \beta \in \mathbb{R}$. Then we have

$$\begin{aligned} \|DC|\psi\rangle\|_2^2 &= \cos^2(\theta)\,\|D|X\rangle\|_2^2 \\ &\geq \cos^2(\theta)|\langle Y|X\rangle|^2 \quad \text{using Claim 2} \\ &\geq \cos^2(\theta)\cos^2(\theta+\theta') \quad \text{using Claim 3.} \quad \square \end{aligned}$$

□

We now prove Lemma 1.

Proof Let $|\Omega\rangle_{\mathcal{AB}}$ be the joint pure state shared by Alice and Bob, where $\mathcal{A}$ is the space controlled by Alice and $\mathcal{B}$ the space controlled by Bob.

Let $M = \{M_{x_0,x_1}\}_{x_0,x_1\in\{0,1\}}$ be Alice's projective measurement on $\mathcal{A}$ to determine her outputs x_0, x_1. Let $P = \{P_0, P_1\}$ be Bob's projective measurement that allows him to guess x_0 with probability $p = \cos^2(\theta)$ and $Q = \{Q_0, Q_1\}$ be Bob's projective measurement that allows him to guess x_1 with probability $q = \cos^2(\theta')$. These measurements are on $\mathcal{B}$ only. Recall that $a = \frac{p+q}{2} = \frac{\cos^2(\theta)+\cos^2(\theta')}{2}$. We consider the following projections on $\mathcal{AB}$:

$$C = \sum_{x_0,x_1} M_{x_0,x_1} \otimes P_{x_0} \quad \text{and} \quad D = \sum_{x_0,x_1} M_{x_0,x_1} \otimes Q_{x_1}.$$

C (resp. D) is the projection on the subspace where Bob guesses correctly the first bit (resp. the second bit) after applying P (resp. Q).

A strategy for Bob to learn both bits is simple: apply the two measurements P and Q one after the other, where the first one is chosen uniformly at random.

The projection on the subspace where Bob guesses (x_0, x_1) when applying P then Q is

$$E = \sum_{x_0,x_1} M_{x_0,x_1} \otimes Q_{x_1} P_{x_0} = DC.$$

Similarly, the projection on the subspace where Bob guesses (x_0, x_1) when applying Q then P is

$$F = \sum_{x_0,x_1} M_{x_0,x_1} \otimes P_{x_0} Q_{x_1} = CD.$$

With this strategy Bob can guess both bits with probability

$$\begin{aligned} & \frac{1}{2}\left(||E|\Omega\rangle||_2^2 + ||F|\Omega\rangle||_2^2\right) \\ =\ & \frac{1}{2}\left(||DC|\Omega\rangle||_2^2 + ||CD|\Omega\rangle||_2^2\right) \\ \geq\ & \frac{1}{2}\left(\cos^2(\theta) + \cos^2(\theta')\right)\cos^2(\theta+\theta') \quad \text{using Lemma 2} \\ \geq\ & \frac{1}{2}\left(\cos^2(\theta) + \cos^2(\theta')\right)\left(\cos^2(\theta) + \cos^2(\theta') - 1\right)^2 \quad \text{using Claim 4} \\ =\ & a(2a-1)^2. \end{aligned}$$

Note that we can use Lemma 2 since Bob's optimal measurement to guess x_0 and x_1 succeeds for each bit with probability at least 1/2. $\square$

4 A Two-Message Protocol With Bias $1/4$

We present in this section a random-*OT* protocol with bias 1/4. This also implies, as we have shown, an *OT* protocol with inputs with the same bias.

> Random Oblivious Transfer Protocol
>
> 1. Bob chooses $b \in_R \{0,1\}$ and creates the state $|\phi_b\rangle := \frac{1}{\sqrt{2}}|bb\rangle + \frac{1}{\sqrt{2}}|22\rangle$.
> 2. Alice chooses $x_0, x_1 \in_R \{0,1\}$ and applies the unitary $|a\rangle \rightarrow (-1)^{x_a}|a\rangle$, where $x_2 := 0$.
> 3. Alice returns the qutrit to Bob who now has the state $|\psi_b\rangle := \frac{(-1)^{x_b}}{\sqrt{2}}|bb\rangle + \frac{1}{\sqrt{2}}|22\rangle$.
> 4. Bob performs on the state $|\psi_b\rangle$ the measurement $\{\Pi_0 = |\phi_b\rangle\langle\phi_b|, \Pi_1 := |\phi'_b\rangle\langle\phi'_b|, I - \Pi_0 - \Pi_1\}$, where $|\phi'_b\rangle := \frac{1}{\sqrt{2}}|bb\rangle - \frac{1}{\sqrt{2}}|22\rangle$.
>   If the outcome is Π_0 then $x_b = 0$, if it is Π_1 then $x_b = 1$, otherwise he aborts.

It is clear that Bob can learn x_0 or x_1 perfectly. Moreover, note that if he sends half of the state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ then he can also learn $x_0 \oplus x_1$ perfectly (although in this case he does not learn either of x_0 or x_1). We now show that it is impossible for him to perfectly learn both x_0 and x_1 and also that his bit is not completely revealed to a cheating Alice.

Theorem 2 *In the protocol described above, we have $A_{OT} = B_{OT} = \frac{3}{4}$.*

Proof We analyze the cheating probabilities of each party.

Cheating Alice

Define Bob's space as $\mathcal{B}$ and let $\sigma_b := \mathrm{Tr}_{\mathcal{B}}(|\phi_b\rangle\langle\phi_b|)$ denote the two reduced states Alice may receive in the first message. Then, the optimal strategy for Alice to learn b is to perform the optimal measurement to distinguish between σ_0 and σ_1. In this case, she succeeds with probability

$$\frac{1}{2} + \frac{1}{4}\left\|\sigma_0 - \sigma_1\right\|_{tr} = \frac{3}{4},$$

(see for example [KN04]). Alice's optimal measurement is, in fact, a measurement in the computational basis. If she gets outcome $|0\rangle$ or $|1\rangle$ then she knows b with certainty. If she gets outcome $|2\rangle$ then she guesses. Notice also, that even after this measurement she can return the measured qutrit to Bob and the outcome of Bob's measurement will always be either Π_0 or Π_1. Hence, Bob will never abort.

Cheating Bob

Bob wants to learn both bits (x_0, x_1). We now describe a general strategy for Bob:

- Bob creates $|\psi\rangle = \sum_i \alpha_i |i\rangle_{\mathcal{A}} |e_i\rangle_{\mathcal{B}}$ and sends the $\mathcal{A}$ part to Alice. The $|e_i\rangle$'s are not necessarily orthogonal but $\sum_i |\alpha_i|^2 = 1$.
- Alice applies U_{x_0,x_1} on her part and sends it back to Bob. He now has the state $|\psi_{x_0,x_1}\rangle = \sum_i \alpha_i (-1)^{x_i} |i\rangle |e_i\rangle$ recalling that $x_2 := 0$.

At the end of the protocol, Bob applies a two-outcome measurement on $|\psi_{x_0,x_1}\rangle$ to get his guess for (x_0, x_1).

From this strategy, we create another strategy with the same cheating probability where Bob sends a pure state. We define this strategy as follows:

- Bob creates $|\psi'\rangle = \sum_i \alpha_i |i\rangle_{\mathcal{A}}$ and sends the whole state to Alice.
- Alice applies U_{x_0,x_1} on her part and sends it back to Bob. He now has the state $|\psi'_{x_0,x_1}\rangle = \sum_i \alpha_i (-1)^{x_i} |i\rangle$ recalling that $x_2 := 0$.
- Bob applies the unitary $U : |i\rangle|0\rangle \rightarrow |i\rangle|e_i\rangle$ to $|\psi'_{x_0,x_1}\rangle|0\rangle$ and obtains $|\psi_{x_0,x_1}\rangle$.

To determine (x_0, x_1), Bob applies the same measurement as in the original strategy.

Clearly both strategies have the same success probability. When Bob uses the second strategy, Alice and Bob are unentangled after the first message and Alice sends back a qutrit to Bob. Using Claim 1, we have

$$\Pr[\text{Bob correctly guesses } (x_0, x_1)] \leq 3/4.$$

Note that there is a strategy for Bob to achieve 3/4. Bob wants to learn both bits (x_0, x_1). Suppose he creates the state

$$|\psi\rangle := \frac{1}{\sqrt{3}}|0\rangle + \frac{1}{\sqrt{3}}|1\rangle + \frac{1}{\sqrt{3}}|2\rangle$$

and sends it to Alice. The state he receives is

$$|\psi_{x_0,x_1}\rangle := \frac{1}{\sqrt{3}}(-1)^{x_0}|0\rangle + \frac{1}{\sqrt{3}}(-1)^{x_1}|1\rangle + \frac{1}{\sqrt{3}}|2\rangle.$$

Then, Bob performs a projective measurement in the 4-dimensional basis $\{|\Psi_{x_0,x_1}\rangle : x_0, x_1 \in \{0,1\}\}$ where

$$|\Psi_{x_0,x_1}\rangle := \frac{1}{2}(-1)^{x_0}|0\rangle + \frac{1}{2}(-1)^{x_1}|1\rangle + \frac{1}{2}|2\rangle + \frac{1}{2}(-1)^{x_0 \oplus x_1}|3\rangle.$$

The probability that Bob guesses the two bits x_0, x_1 correctly is

$$\sum_{x_0,x_1} \frac{1}{4} \Pr[\text{Bob guesses } (x_0, x_1)] = \sum_{x_0,x_1} \frac{1}{4} |\langle \Psi_{x_0,x_1} | \psi_{x_0,x_1} \rangle|^2 = \frac{3}{4}.$$

Note that in our protocol Alice never aborts.

5 Oblivious Transfer as a Forcing Primitive

Here, we discuss a variant of oblivious transfer, as a generalisation of coin flipping, that can be analyzed using an extention of Kitaev's semidefinite programming formalism.

Definition 4 (Forcing Oblivious Transfer) *A k-out-of-n forcing oblivious transfer protocol, denoted here as $\binom{n}{k}$-fOT, with* forcing bias ε *is a protocol satisfying:*

- *Alice outputs n random bits $x := (x_1, \ldots, x_n)$*
- *Bob outputs a random index set b of k indices and bit string x_b consisting of x_i for $i \in b$*
- $A_{b,x_b} := \sup\{\Pr[\textit{Alice can force Bob to output } (b, x_b)]\} = \dfrac{\varepsilon_A}{\binom{n}{k} \cdot 2^k}$
- $B_x := \sup\{\Pr[\textit{Bob can force Alice to output } x]\} = \dfrac{\varepsilon_B}{2^n}$
- *The forcing bias of the protocol is defined as $\epsilon = \max\{\epsilon_A, \epsilon_B\}$*

where the suprema are taken over all strategies of Alice and Bob.

The main difference in this new primitive is the definition of security. Here, we design protocols to protect against a dishonest party being able to *force* a desired value as the output of the other player. In the previous section (and in the literature) oblivious transfer protocols are designed to protect against the dishonest party *learning* the other party's output. Notice, for example, that in coin flipping we can design protocols to protect against a dishonest party forcing a desired outcome, but both players *learn* the coin outcome perfectly.

The primitive we have defined is indeed a generalization of coin flipping since we can cast the problem of coin flipping as a 1-out-of-1 forcing oblivious transfer protocol. Of course, in $\binom{1}{1}$-fOT Alice always knows Bob's index set so the forcing bias is the only interesting notion of security in this case.

As we said, we define the bias ε as a multiplicative factor instead of additive, since the honest probabilities can be much different and in this case our definition makes more sense. To relate this bias to the one previously studied in coin flipping we have that coin flipping protocols with bias $\varepsilon \leq \sqrt{2} + \delta$ exist for any $\delta > 0$, see [CK09], and weak coin flipping protocols with bias $\varepsilon \leq 1 + \delta$ exist for any $\delta > 0$, see [Moc07].

5.1 Extending Kitaev's Lower Bound to Forcing Oblivious Transfer

We now extend Kitaev's formalism from the setting of coin flipping to the more general setting of $\binom{n}{k}$-fOT.

Suppose Alice and Bob have private spaces $\mathcal{A}$ and $\mathcal{B}$, respectively, and both have access to a message space $\mathcal{M}$ each initialized in state $|0\rangle$. Then, we can define an m-round $\binom{n}{k}$-fOT protocol using the following parameters:

- Alice's unitary operators $U_{A,1}, \ldots, U_{A,m}$ which act on $\mathcal{A} \otimes \mathcal{M}$
- Bob's unitary operators $U_{B,1}, \ldots, U_{B,m}$ which act on $\mathcal{M} \otimes \mathcal{B}$
- Alice's POVM $\{\Pi_{A,abort}\} \cup \{\Pi_{A,x} : x \in \mathbb{Z}_2^n\}$ acting on $\mathcal{A}$, one for each outcome
- Bob's POVM $\{\Pi_{B,abort}\} \cup \left\{\Pi_{B,(b,x_b)} : b \text{ a k-element subset of n indices}, x_b \in \mathbb{Z}_2^k\right\}$ acting on $\mathcal{B}$, one for each outcome

We now show the criteria for which the parameters above yield a proper $\binom{n}{k}$-fOT protocol. In a proper protocol we require that Alice and Bob's measurements are consistent and that the outcomes are uniformly random when the protocol is followed honestly. Define

$$|\psi\rangle := (I_{\mathcal{A}} \otimes U_{B,m})(U_{A,m} \otimes I_{\mathcal{B}}) \cdots (I_{\mathcal{A}} \otimes U_{B,1})(U_{A,1} \otimes I_{\mathcal{B}})|0\rangle_{\mathcal{A}\otimes\mathcal{M}\otimes\mathcal{B}}$$

to be the state at the end of an honest run of the protocol. Then, we require the unitary and measurement operators to satisfy the following condition:

$$\left\|(\Pi_{A,x} \otimes I_{\mathcal{M}} \otimes \Pi_{B,(b,x_b)})|\psi\rangle\right\|_2^2 = \frac{1}{\binom{n}{k}2^n} \text{ for } (x, b, x_b) \text{ consistent.}$$

Similar to coin flipping, we can capture cheating strategies as semidefinite programs. Bob can force Alice to output a specific $x \in \mathbb{Z}_2^n$ with maximum probability equal to the optimal value of the following semidefinite program

$$\begin{array}{llcll}
B_x = \max & \langle \Pi_{A,x} \otimes I_{\mathcal{M}}, \rho_{A,N} \rangle & & & \\
\text{subject to} & \mathrm{Tr}_{\mathcal{M}}(\rho_{A,0}) & = & |0\rangle\langle 0|_{\mathcal{A}} & \\
& \mathrm{Tr}_{\mathcal{M}}(\rho_{A,j}) & = & \mathrm{Tr}_{\mathcal{M}}(U_{A,j}\rho_{A,j-1}U_{A,j}^*), & \text{for } j \in \{1, \ldots, N\} \\
& \rho_{A,0}, \ldots, \rho_{A,N} & \in & \mathrm{Pos}(\mathcal{A} \otimes \mathcal{M}), & \text{for } j \in \{0, \ldots, N\}
\end{array}$$

where $\mathrm{Pos}(\mathcal{H})$ is the set of positive semidefinite matrices over the Hilbert space $\mathcal{H}$. The states ρ_i represent the part of the state under Alice's control after Bob sends his i'th message. The constraints above are necessary since Bob cannot apply a unitary on $\mathcal{A}$. They are also sufficient since Bob can maintain a purification during the protocol consistent with the states above to achieve a cheating probability given by the corresponding objective value.

To capture Alice's cheating strategies we can do the same as for the cheating Bob and examine the states under Bob's control during the course of the protocol. That is, Alice can force Bob to output a specific k-element subset b and $x_b \in \mathbb{Z}_2^k$ with maximum probability equal to the optimal value of the following semidefinite program

$$\begin{array}{llrcll} A_{b,x_b} = \max & \langle I_{\mathcal{M}} \otimes \Pi_{B,(b,x_b)}, \rho_{B,N} \rangle & & & & \\ \text{subject to} & & \mathrm{Tr}_{\mathcal{M}}(\rho_{B,0}) & = & |0\rangle\langle 0|_{\mathcal{B}} & \\ & & \mathrm{Tr}_{\mathcal{M}}(\rho_{B,j}) & = & \mathrm{Tr}_{\mathcal{M}}(U_{B,j}\rho_{B,j-1}U_{B,j}^*), & \text{for } j \in \{1,\ldots,N\} \\ & & \rho_{B,0},\ldots,\rho_{B,N} & \in & \mathrm{Pos}(\mathcal{M}\otimes\mathcal{B}), & \text{for } j \in \{0,\ldots,N\} \end{array}$$

The proofs that these capture the optimal cheating probabilities are the same as those used for coin flipping in [Kit03] and [ABDR04]. Using these semidefinite programs we can prove the following Theorem.

Theorem 3 *In any* $\binom{n}{k}$-fOT *protocol and consistent* b, x, x_b *we have*

$$B_x \cdot A_{b,x_b} \geq \Pr[\textit{Alice honestly outputs } x \textit{ and Bob honestly outputs } (b,x_b)] = \frac{1}{\binom{n}{k}2^n}.$$

In particular, the forcing bias satisfies $\varepsilon \geq \sqrt{2}^k$.

Once we extended the semidefinite programming formulation, the proof of the theorem follows almost directly from the proof in [Kit03] and [ABDR04] for coin flipping except that the honest outcome probabilities are different in our case. Namely, for $|\psi\rangle$ defined above, we have

$$\left\| (\Pi_{A,x} \otimes I_{\mathcal{M}} \otimes \Pi_{B,(b,x_b)})|\psi\rangle \right\|_2^2 = \frac{1}{\binom{n}{k}2^n}$$

when x, b, and x_b are consistent and 0 otherwise.

5.2 A Protocol with Optimal Forcing Bias

In this section we prove Theorem 4. First, consider the following protocol which achieves the bound in Theorem 3 but is asymmetric. Alice sends n random bits to Bob. Bob, then, outputs b, a random k-index subset of n indices, and x_b. In this protocol Bob can force a desired outcome with probability $\frac{1}{2^n}$ and Alice can force a desired outcome with probability $\frac{1}{\binom{n}{k}}$. Thus the product of the cheating probabilities is optimal, that is it achieves the lower bound in Theorem 3. However the protocol is asymmetric. This can be easily remedied using coin flipping. We present an optimal protocol with this security definition.

An Optimal $\binom{n}{k}$-fOT Protocol with Forcing Bias $\sqrt{2}^k$

1. Bob outputs a random index set b of k indices and sends the result to Alice.
2. Alice and Bob play a coin flipping game with bias $\sqrt{2}+\delta$ (for a $\delta > 0$ sufficiently small) to determine each bit in x_b.
3. Alice randomly chooses her bits not in b.

Theorem 4 *For any $\gamma > 0$ we can choose a $\delta > 0$ such that the $\binom{n}{k}$-fOT protocol above satisfies for consistent b, x, x_b*

$$A_{b,x_b} \leq \frac{\sqrt{2}^k(1+\gamma)}{\binom{n}{k}\cdot 2^k} \quad \text{and} \quad B_x \leq \frac{\sqrt{2}^k(1+\gamma)}{2^n}$$

Proof Fix $\gamma > 0$ and a coin flipping parameter $\delta > 0$ small enough so that $\left(\frac{1}{\sqrt{2}}+\frac{\delta}{2}\right)^k \leq \frac{\sqrt{2}^k(1+\gamma)}{2^k}$. This can be achieved by taking $\delta = O(\frac{\gamma}{k})$. This sets an upper bound on the probability of forcing a k bit-string using k coin flipping protocols each with a maximum cheating probability of $\frac{1}{\sqrt{2}}+\frac{\delta}{2}$. We now analyze each party cheating. For Alice cheating, she has no control over the index set but she can try to force a particular bit-string for x_b. Her maximum cheating probability is

$$\frac{1}{\binom{n}{k}}\cdot\left(\frac{1}{\sqrt{2}}+\frac{\delta}{2}\right)^k \leq \frac{1}{\binom{n}{k}}\cdot\frac{\sqrt{2}^k(1+\gamma)}{2^k} = \frac{\sqrt{2}^k(1+\gamma)}{\binom{n}{k}2^k}.$$

Bob has no control over Alice's $n-k$ remaining bits so Bob can cheat with maximum probability

$$\frac{1}{2^{n-k}}\cdot\left(\frac{1}{\sqrt{2}}+\frac{\delta}{2}\right)^k \leq \frac{1}{2^{n-k}}\cdot\frac{\sqrt{2}^k(1+\gamma)}{2^k} = \frac{\sqrt{2}^k(1+\gamma)}{2^n}. \quad \square$$

For the special case of $\binom{2}{1}$-fOT we have the following corollary.

Corollary 1 (Optimal $\binom{2}{1}$-fOT)
There exists a $\binom{2}{1}$-fOT protocol where each party has honest outcome probabilities of $1/4$ and neither party can cheat with probability higher than $\frac{1}{\sqrt{8}}(1+\gamma)$, for any $\gamma > 0$.

Note that we have strong coin flipping protocols with $poly(m)$ rounds that achieve $\delta = \frac{1}{poly(m)}$. Hence, our protocol also achieves $\gamma = \frac{1}{poly(m)}$ with $poly(m)$ rounds.

Last, we remark that this protocol is completely classical with the exception of the quantum coin flipping subroutines. This is similar to the optimal coin flipping protocol in [CK09] designed using classical messages and optimal quantum weak coin flipping subroutines.

References

[ABDR04] Andris Ambainis, Harry Buhrman, Yevgeniy Dodis, and Hein Rohrig. Multiparty quantum coin flipping. In *CCC '04: Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, pages 250–259, Washington, DC, USA, 2004. IEEE Computer Society.

[Amb01] Andris Ambainis. A new protocol and lower bounds for quantum coin flipping. In *STOC '01: Proceedings of the thirtieth annual ACM symposium on Theory of computing*, Washington, DC, USA, 2001. IEEE Computer Society.

[Amb02] Andris Ambainis. Lower bound for a class of weak quantum coin flipping protocols, 2002. quant-ph/0204063.

[ATVY00] Dorit Aharonov, Amnon Ta-Shma, Umesh V. Vazirani, and Andrew C. Yao. Quantum bit escrow. In *STOC '00: Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pages 705–714, New York, NY, USA, 2000. ACM.

[BB84] Bennett and Brassard. Quantum cryptography: Public key distribution and coin tossing. in Proc. Of IEEE Inter. Conf. on Computer Systems and Signal Processing, Bangalore, Kartarna, (Institute of Electrical and Electronics Engineers, New York, 1984.

[BF10] Niek Bouman and Serge Fehr. Sampling in a quantum population, and applications. In *CRYPTO 2010*, 2010.

[Blu81] Manuel Blum. Coin flipping by telephone. In *CRYPTO*, pages 11–15, 1981.

[CK09] Andre Chailloux and Iordanis Kerenidis. Optimal quantum strong coin flipping. *Foundations of Computer Science, Annual IEEE Symposium on*, 0:527–533, 2009.

[Cré87] Claude Crépeau. Equivalence between two flavours of oblivious transfer. In *Advances in Cryptology: CRYPTO '87*, 1987.

[DKSW07] Giacomo Mauro D'Ariano, Dennis Kretschmann, Dirk Schlingemann, and Reinhard F. Werner. Reexamination of quantum bit commitment: the possible and the impossible. *Physical Review A*, 76:032328, 2007.

[DW09] Andrew Drucker and Ronald Wolf. Quantum proofs for classical theorems, 2009.

[EGL82] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. In *Advances in Cryptology: Proceedings of CRYPTO 82*, 1982.

[JRS02] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. A theorem about relative entropy of quantum states with an application to privacy in quantum communication. In *Proceedings of 43rd IEEE Symposium on Foundations of Computer Science (FOCS)*, 2002.

[Kit03] A Kitaev. Quantum coin-flipping. Presentation at the 6th workshop on quantum information processing (qip 2003), 2003.

[KN04] I. Kerenidis and A. Nayak. Weak coin flipping with small bias. *Inf. Process. Lett.*, 89(3):131–135, 2004.

[LC97] Hoi-Kwong Lo and H. F. Chau. Is quantum bit commitment really possible? *Phys. Rev. Lett.*, 78(17):3410–3413, Apr 1997.

[Lo97] Hoi-Kwong Lo. Insecurity of quantum secure computations. *Phys. Rev. A*, 56(2):1154–1162, 1997.

[May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78(17):3414–3417, Apr 1997.

[Moc05] C. Mochon. Large family of quantum weak coin-flipping protocols. *Phys. Rev. A*, 72(2):022341–+, August 2005.

[Moc07] Carlos Mochon. Quantum weak coin flipping with arbitrarily small bias. WCF, 2007. quant-ph:0711.4114.

[Nay99] Ashwin Nayak. Optimal lower bounds for quantum automata and random access codes. *Foundations of Computer Science, Annual IEEE Symposium on*, 0:369, 1999.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information.* Cambridge University Press, New York, NY, USA, 2000.

[NS03] Ashwin Nayak and Peter Shor. Bit-commitment-based quantum coin flipping. *Phys. Rev. A*, 67(1):012304, Jan 2003.

[Rab81] Michael Rabin. How to exchange secrets by oblivious transfer. In *Technical Report TR-81, Aiken Computation Laboratory, Harvard University*, 1981.

[SR01] R. W. Spekkens and T. Rudolph. Degrees of concealment and bindingness in quantum bit commitment protocols. *Physical Review A*, 65:012310, 2001.

[SR02] Robert Spekkens and Terry Rudolph. Quantum protocol for cheat-sensitive weak coin flipping. *Phys. Rev. Lett.*, 89(22):1–4, Nov 2002.

[SSS09] Louis Salvail, Christian Schaffner, and Miroslava Sotakova. On the power of two-party quantum cryptography. In *ASIACRYPT 2009*, 2009.

[Yao95] Andrew Yao. Security of quantum protocols against coherent measurements. In *Proceedings of 26th Annual ACM Symposium on the Theory of Computing*, pages 67–75, 1995.