On the Existence of Loss-Tolerant Quantum Oblivious Transfer Protocols

Jamie Sikora

IQC, University of Waterloo

September 15, 2010

Abstract

Oblivious Transfer is the cryptographic primitive where Alice sends one of two bits to Bob but is oblivious to the bit received. Using quantum communication we can build oblivious transfer protocols with security provably better than any protocol built using classical communication. However, with imperfect apparatus one needs to consider other strategies. In this paper we present an oblivious transfer protocol which is impervious to lost messages with bias 0.4295.

1 Introduction

Quantum information allows us to perform certain cryptographic tasks which are impossible using classical information alone. In 1984 Bennett and Brassard gave a quantum key distribution scheme which is unconditionally secure against an eavesdropper. This lead to many new problems such as finding quantum protocols for other cryptographic primitives such as coin-flipping and oblivious transfer.

Coin-flipping is the cryptographic primitive where Alice and Bob generate a random bit over a communication channel. Aharonov et al. [ATVY00] showed the existence of quantum coin-flipping protocols where neither party can force the outcome with probability 1. Ambainis [Amb01] then showed a protocol where neither party can force the outcome with probability higher than 0.75. As for lower bounds, Mayers, Lo and Chau showed that perfect coin-flipping is impossible and then Kitaev [Kit03] extended this bound to show that in any quantum coin-flipping protocol one of the parties can force the outcome with probability at least 0.707. The question of whether or not this bound is optimal was finally answered by Chailloux and Kerenidis [CK09] showing the existence of protocols approaching Kitaev's bound.

Another cryptographic primitive which has been studied is oblivious transfer. Oblivious transfer is interesting since it can be used to construct secure two-party protocols [EGL82], [Cré87], [Rab81]. An oblivious transfer protocol, denoted as OT, with bias ε is a protocol where:

- Alice inputs two bits x_0 and x_1;
- Bob inputs an index $b \in \{0,1\}$;
- Bob learns x_b;
- Cheating Alice can learn b (without Bob aborting) with maximum probability $\frac{1}{2}+\varepsilon_A$;
- Cheating Bob can learn (x_0, x_1) (without Alice aborting) with maximum probability $\frac{1}{2}+\varepsilon_B$;
- $\varepsilon = \max\{\varepsilon_A, \varepsilon_B\}$.

Note that when Bob is honest he learns x_b thus cheating Bob learns (x_0, x_1) with probability at least $1/2$. It was shown in [CKS10] that we can build protocols for OT with bias 0.25 and that no protocol can achieve a bias less than 0.0586. Finding the best bias for OT remains an open problem.

We note here that various settings for oblivious transfer have been studied before such as the noisy-storage model and bounded-storage model. In this paper we study only information theoretic security but we allow the possibility of lost messages.

Loss-tolerance is the security notion where neither party can cheat to their advantage by declaring that a message is lost or by deliberately sending an empty message. Loss-tolerance was first applied to quantum coin-flipping by Berlin et al. [BBBG09]. They showed a vulnerability in the best-known coin-flipping protocol construction of Ambainis [Amb01]. They rectified this problem by exhibiting a protocol which is impervious to lost messages and where neither party can force the outcome with probability higher than 0.90. Aharon, Massar, and Silman [AMS10] generalized this protocol to a family of loss-tolerant coin-flipping protocols with security slightly better at the cost of using more qubits in the communication. Recently, Chailloux [Cha10] improved Berlin et al.'s protocol so that no party can cheat with probability higher than 0.859. It remains an open problem to show whether Kitaev's lower bound can be achieved with protocols that are loss-tolerant or whether a better lower bound exists for loss-tolerant protocols.

In this paper we show how to build loss-tolerant OT protocols from loss-tolerant coin-flipping protocols. We use the results of [BBBG09], [AMS10], and [Cha10] to show the existence of loss-tolerant OT protocols where neither party can cheat with probability 1. Precisely, we show the following result.

Theorem 1.1 *If there exists a loss-tolerant coin-flipping protocol with bias ε then there exists a loss-tolerant* OT *protocol with bias at most* $\dfrac{1}{4}+\dfrac{\varepsilon}{2}$.

Since there exists a loss-tolerant coin-flipping protocol with bias 0.359 [Cha10] we have the following theorem.

Theorem 1.2 *There exists a loss-tolerant* OT *protocol with bias at most* 0.4295*.*

2 Definitions

We first define what it means for a protocol to be loss-tolerant.

Definition 2.1 *A* loss-tolerant protocol *is a cryptographic protocol which is impervious to lost messages. That is, neither Alice nor Bob can cheat more by*

- *communicating "lost message" even if it was received;*
- *sending a blank message deliberately.*

If a protocol is not loss-tolerant we say it is loss-vulnerable*.*

We prefix a protocol with "LT−" to indicate that it is loss-tolerant.

Definition 2.2 *A* coin-flipping protocol*, denoted* CF*, with bias ε is a protocol with no inputs where*

- *Alice and Bob both output a randomly generated bit $c \in \{0, 1\}$;*
- *Cheating Alice can force Bob to accept a desired outcome for c with maximum probability $\frac{1}{2} + \varepsilon_A$;*
- *Cheating Bob can force Alice to accept a desired outcome for c with maximum probability $\frac{1}{2} + \varepsilon_B$;*
- *$\varepsilon = \max\{\varepsilon_A, \varepsilon_B\}$.*

When we consider "cheating" in this paper we mean that a party digresses from protocol. Also, when we consider a cheating party we assume that the other party follows the protocol honestly. The idea is to design protocols which protect honest parties from dishonest parties.

There is another variant of coin-flipping called *weak coin-flipping*. In weak coin-flipping Alice only desires outcome 0 whereas Bob desires outcome 1. We note here that the results of this paper still hold if we replace coin-flipping with this weaker primitive.

Definition 2.3 *A* random oblivious transfer protocol*, denoted* ROT*, with bias ε is a protocol with no inputs where*

- *Alice outputs two randomly generated bits x_0 and x_1;*

- *Bob outputs a randomly generated index $b \in \{0,1\}$ and learns x_b;*
- *Cheating Alice can learn b (without Bob aborting) with maximum probability $\frac{1}{2} + \varepsilon_A$;*
- *Cheating Bob can learn (x_0, x_1) (without Alice aborting) with maximum probability $\frac{1}{2} + \varepsilon_B$;*
- $\varepsilon = \max\{\varepsilon_A, \varepsilon_B\}$.

Note that cheating Bob learns (x_0, x_1) with probability at least $1/2$ since he can learn x_b perfectly by communicating honestly.

When a party cheats, we only refer to the probability for which they can learn the desired values without the other party aborting. For example, when Bob cheats he outputs a guess for (x_0, x_1) and we are interested in how correct his guess is. We do not suppose, for example, that either bit in Bob's guess is correct with probability 1.

We can also consider a traditional oblivious transfer protocol where Alice gets to choose x_0 and x_1 and Bob gets to choose b.

Definition 2.4 *An* oblivious transfer protocol*, denoted* OT*, with bias ε is a protocol where*

- *Alice inputs two bits x_0 and x_1;*
- *Bob inputs an index $b \in \{0,1\}$;*
- *Bob learns x_b;*
- *Cheating Alice can learn b (without Bob aborting) with maximum probability $\frac{1}{2} + \varepsilon_A$;*
- *Cheating Bob can learn (x_0, x_1) (without Alice aborting) with maximum probability $\frac{1}{2} + \varepsilon_B$;*
- $\varepsilon = \max\{\varepsilon_A, \varepsilon_B\}$.

In the definition above there can be different ways to interpret the bias. For example, we could consider worst case choices over inputs, assuming the inputs are chosen randomly, etc. However, the protocol construction given in this paper is independent of how the inputs are chosen thus we simply leave it as the probability of learning.

3 A Loss-Vulnerable Protocol

In this section we examine a protocol for oblivious transfer and show it is loss-vulnerable. This protocol has the same vulnerability as the best-known coin-flipping protocols based on bit-commitment, see [BBBG09].

A protocol for ROT, which yields a protocol for OT [CKS10], is the following.

Random Oblivious Transfer Protocol [CKS10]

1. Bob randomly chooses $b \in \{0, 1\}$ and creates the state $|\phi_b\rangle := \frac{1}{\sqrt{2}}|bb\rangle + \frac{1}{\sqrt{2}}|22\rangle$. Bob sends one of the qutrits to Alice.
2. Alice randomly chooses $x_0, x_1 \in \{0, 1\}$ and applies the unitary $|a\rangle \to (-1)^{x_a}|a\rangle$, where $x_2 := 0$.
3. Alice returns the qutrit to Bob. Bob now has the two-qutrit 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 has been shown in [CKS10] that Alice can learn b with maximum probability 3/4 and Bob can learn both of Alice's bits with maximum probability 3/4. However there is a different kind of cheating strategy which allows Alice to learn Bob's index b with probability 1 and this is as follows. Suppose Alice measures the first message in the computational basis. If she sees outcome "0" or "1" then she knows with certainty Bob's index b. If the outcome is "2" then she replies to Bob "Sorry I lost your message." Then they restart the protocol and Alice can measure again. This will eventually let Alice learn b perfectly.

4 From LT-Coin-Flipping to LT-Random Oblivious Transfer

Consider the following LT-ROT protocol built using an LT-CF protocol.

Loss-Tolerant Random Oblivious Transfer Protocol

1. Alice and Bob perform an LT-CF protocol with bias ε so that Alice and Bob output the shared random bit $c \in \{0, 1\}$.
2. If $c = 0$ then Alice chooses b, x_0, x_1 at random and sends b, x_b to Bob.
3. If $c = 1$ then Bob chooses b, x_0, x_1 at random and sends x_0, x_1 to Alice.
4. If the LT-CF protocol is aborted then Alice and Bob abort.

We see that this defines a valid ROT protocol since the outputs are random and Bob learns x_b.

Loss-Tolerance The LT-CF protocol is loss-tolerant by definition. Since the rest of the messages are classical there is no loss of information if messages are lost; they can simply be sent again.

Cheating Alice, Bob We see that if $c = 0$ then Alice learns b perfectly and if $c = 1$ then she learns b with probability 1/2. Thus Alice can learn b with probability

$$\Pr[c = 0] + \frac{1}{2}\Pr[c = 1] \le \Pr[c = 0] + \frac{1}{2}(1 - \Pr[c = 0]) = \frac{1}{2} + \frac{1}{2}\Pr[c = 0] \le \frac{3}{4} + \frac{\varepsilon}{2},$$

since $\Pr[c = 0] \le \frac{1}{2} + \varepsilon$.

Showing Bob can learn (x_0, x_1) with probability at most $\frac{3}{4} + \frac{\varepsilon}{2}$ follows the same argument.

We have shown the following lemma.

Lemma 4.1 *If there exists an* LT-CF *protocol with bias* ε *then there exists an* LT-ROT *protocol with bias at most* $\dfrac{1}{4} + \dfrac{\varepsilon}{2}$.

5 From LT-Random Oblivious Transfer to LT-Oblivious Transfer

Consider the following LT-OT protocol built using an LT-ROT protocol.

Loss-Tolerant Oblivious Transfer Protocol

1. Alice chooses her inputs x_0 and x_1 and Bob chooses his input b.
2. Alice and Bob perform an LT-ROT protocol with bias ε so that Alice outputs (x'_0, x'_1) and Bob outputs $(b', x'_{b'})$.
3. If the LT-ROT protocol is aborted then Alice and Bob abort.
4. Bob sends $b \oplus b'$ to Alice. They define $x'_c = x'_{c \oplus b \oplus b'}$ for $c \in \{0, 1\}$.
5. Alice sends $(x_0 \oplus x'_0, x_1 \oplus x'_1)$ to Bob. Bob adds $x_b \oplus x'_b$ to x'_b to get x_b.

We see that this defines a valid OT protocol since Bob learns x_b consistent with their inputs. It has been shown [CKS10] that this OT protocol has the same bias as the ROT subroutine. This OT protocol is loss-tolerant because the ROT protocol is loss-tolerant and the other messages are classical.

Lemma 5.1 *If there exists an* LT-ROT *protocol with bias* ε *then there exists an* LT-OT *protocol with bias* ε*.*

The following theorem follows from Lemmas 4.1 and 5.1.

Theorem 5.2 *If there exists an* LT-CF *protocol with bias* ε *then there exists an* LT-OT *protocol with bias at most* $\frac{1}{4} + \frac{\varepsilon}{2}$*.*

Since there exists an LT-CF protocol with bias 0.359 [Cha10] we have the following theorem.

Theorem 5.3 *There exists an* LT-OT *protocol with bias at most* 0.4295*.*

6 Summary and Open Questions

The table below summarizes the best-known lower and upper bounds for the bias of loss-tolerant protocols.

bias ε	LT-CF	LT-ROT	LT-OT
Lower Bound	$1/\sqrt{2} - 1/2$ [Kit03]	0.0586 [CKS10]	0.0586 [CKS10]
Upper Bound	0.359 [Cha10]	0.4295 (this paper)	0.4295 (this paper)

Finding the best loss-tolerant protocols for the primitives discussed in this paper remains an open problem. It would be interesting to see if the best-known lower bounds can be achieved with protocols that are loss-tolerant or if there are larger lower bounds for this restricted class of protocols.

References

[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.

[AMS10] N. Aharon, S. Massar, and J. Silman. A family of loss-tolerant quantum coin flipping protocols. quant-ph:1006.1121. 2010.

[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.

[BBBG09] Guido Berlin, Gilles Brassard, Felix Bussieres, and Nicolas Godbout. Fair loss-tolerant quantum coin flipping. *Physical Review A*, 80 (062321), 2009.

[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.

[Cha10] André Chailloux. Improved loss-tolerant quantum coin-flipping. quant-ph:1009.0044. 2010.

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

[CKS10] André Chailloux, Iordanis Kerenidis, and Jamie Sikora. Lower bounds for quantum oblivious transfer. quant-ph:1007.1875. 2010.

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

[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.

[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.

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

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