On the Possibility of Basing Oblivious Transfer on Weakened Private Information Retrieval

Jen-Hou Chou
Department of Computer Science and Information Engineering
National Taiwan University

Abstract

We consider the problem of reducing Oblivious Transfer to Private Information Retrieval. We give a simple reduction from 1-out-of-2 Oblivious Transfer to Private Information Retrieval, where the reduction is against malicious players.

We also consider the completeness of Private Information Retrieval on weakened assumption. We will give a impossibility result and a possibility result. For impossibility result, we use the technique originating in [24]. For possibility result, we reduce Weak Oblivious Transfer which was proposed in [16] to Weak Private Information Retrieval.

Contents

Chapter 1

Introduction

Oblivious Transfer (OT) that was introduced by Halpern and Rabin [23] is a classic cryptographic primitive in two-party scenario. In it, Alice has a bit b and Bob tries to get it. Bob will get b with probability 1/2, and he knows whether he got b or not. Alice has no idea about whether Bob got b or not.

There are several variants of OT, the most general one is 1-out-of-2 Oblivious Transfer ($\binom{1}{2}$-OT) which was proposed by Even, Goldreich, and Lempel in [19]. In the protocol, Alice has two bits b_0 and b_1 as input, and Bob has a bit c as input. Ideally, Alice should learn nothing new from the Bob, whereas the receiver should learn b_c and nothing more. The relationship between OT and $\binom{1}{2}$-OT had been showed to be equivalent by Crepeau in [12]. Goldreich, Micali, Wigderson [21], and Killian [24] showed $\binom{1}{2}$-OT is complete for all two-party secure computations.

More generalized Oblivious Transfer was proposed. In 1-out-of-n Oblivious Transfer ($\binom{1}{n}$-OT), Alice has n bits b_0, $\ldots$, b_{n-1} as input, and Bob has an index $c \in \{0, \ldots, n-1\}$ as input. Bob wants to get b_c without leaking c to Alice and learns nothing more. In k-out-of-n Oblivious Transfer ($\binom{k}{n}$-OT), Alice has n bits b_0, $\ldots$, b_{n-1} as input, and Bob has k indices $c_1, c_2, \ldots, c_k \in \{0, \ldots, n-1\}$ as input. Bob wants to get $b_{c_1}, \ldots, b_{c_k}$ without leaking his input to Alice and learns nothing more.

Another important cryptographic primitive is Private Information Retrieval(PIR) which was proposed by Chor, Goldreich, Kushilevitz, and Sudan in [11]. The PIR scheme is an interactive protocol between a database D and a user U. The user wants to privately retrieve some information from the database with as low as possible communication complexity from D. More formally, the database is modeled as an n-bit string x, the user retrieves the i-th bit $x[i]$, and gives the database no information about i. We call a PIR protocol non-trivial if its total communication from D is strictly less than the size of database.

Given the completeness of $\binom{1}{2}$-OT, other primitives can be shown complete from $\binom{1}{2}$-OT. Crescenzo, Malkin, and Ostrovsky [15] showed that any non-trivial PIR is complete for all two-party secure computations. They first constructed a $\binom{1}{2}$-OT protocol which is secure against honest-but-curious Bob. Then they constructed a

$\binom{1}{2}$-OT protocol for malicious Bob by using techniques originating in [22, 21], based on commitment schemes and zero-knowledge proofs for NP-complete languages to force Bob following the protocol.

An interesting question in cryptography is that how to implement oblivious transfer based on seemingly weaker primitives. Brassard and Crepeau [6] proposed two weaker models of oblivious transfer and showed their completeness: XOR Oblivious Transfer and Generalized Oblivious Transfer. In XOR Oblivious Transfer, Bob can choose to learn b_0, b_1, or $b_0 \oplus b_1$. In Generalized Oblivious Transfer, Bob can choose to learn b_0, b_1, or all the binary functions of b_0 and b_1.

Cachin [7] also proposed a weaker oblivious transfer called Universal Oblivious Transfer, denoted UOT(X, Y). In Universal Oblivious Transfer, Alice sends a random variable X with alphabet $\mathcal{X}$ and Bob obtains a random variable Y. Bob can secretly specify the distributions $P_{Y|X=x}$ for all $x \in \mathcal{X}$ such that Y does not give Bob complete information about X. UOT(X, Y) is complete for two-party computations when $H(X|Y) > 0$.

The weakness of above weaker primitives is one-sided: only Bob learns extra information. Damgård, Kilian, and Salvail [16] proposed a general model in two-party computation called Weak Generic Transfer(WGT). In this model, a cheating player can get more information than an honest one. A special case in WGT is Weak Oblivious Transfer ((p,q)-WOT), which is a $\binom{1}{2}$-OT protocol with the following relaxation: with probability at most p, a cheating Alice will learn Bob's choice c, and with probability at most q, a cheating Bob will learn both of Alice's input bits.

Weak Oblivious Transfer was shown to be complete when $p + q < 1$ by reducing $\binom{1}{2}$-OT to it. The reduction consists of two subprotocol. One is to reduce Alice's probability for learning Bob's choice, but it raises Bob's probability for learning Alice's input. The other one is to reduce Bob's probability for learning Alice's input, but it raises Alice's probability for learning Bob's choice. After execute this reduction once, we will get a ($p^{'}$, $q^{'}$)-WOT. If $p + q < 1$, then $p^{'} + q^{'} < p + q$. So if we execute this reduction many times, we will get a (s, t)-WOT where $s + t$ is negligible.

Our Results

Although reductions from $\binom{1}{2}$-OT to PIR had been shown in [15], the $\binom{1}{2}$-OT protocol against malicious Bob is complicated, and the communication complexity is large because of using bit commitment and zero-knowledge proofs for NP-complete languages. In chapter 3, based on the reduction that works anginst honest Bob in [15], we construct a reduction that reduce $\binom{1}{2}$-OT to PIR that works against malicious Bob. Since we don't uses bit commitment and zero-knowledge proofs for NP-complete languages to force Bob following the protocol, the reduction is simpler than the reduction that works against malicious Bob in [15].

We also consider a generalized model of PIR called Weak Private Information Retrieval (WPIR). In chapter 4, we will show the completeness of WPIR. We will give a bound for possibility result, and a bound for impossibility result. However, the bounds are not tight.

Chapter 2

Preliminaries

Let $\mathbb{N}$ be the set of natural numbers. If x is a string, let $x[i]$ denote the i-th bit of x. An interactive Turing machine is a probabilistic Turing machine with a communication tape. An interactive protocol is a pair (A, B) of interactive Turing machines running in probabilistic polynomial time. A transcript of an execution of an interactive protocol is the messages that appear on the communication tapes of the two machines during that execution. Let $t_{A,B}(x, r_A, y, r_B)$ denote the transcript of an execution of an interactive protocol (A, B) with input x for A and y for B and with random strings r_A for A and r_B for B. If $t = t_{A,B}(x, r_A, y, r_B)$ is such a transcript, the output of A is denoted by $A(x, r_A, t)$. Similarly the output of B is denoted by $B(y, r_B, t)$. The notation $(r_B, t) \leftarrow t_{A,B}(x, r_A, y, \cdot)$ denotes the random process of selecting a random string r_B uniformly at random, and setting $t = t_{A,B}(x, r_A, y, r_B)$. Similarly we denote $(r_A, t) \leftarrow t_{A,B}(x, \cdot, y, r_B)$ for the case where A's random string is chosen uniformly at random, and $(r_A, r_B, t) \leftarrow t_{A,B}(x, \cdot, y, \cdot)$ for the case where the random strings for both A and B are chosen uniformly at random.

Private Information Retrieval(PIR)

Informally, a private information retrieval scheme is an interactive protocol between two parties, a database D and a user U. The database holds an n-bit string x, and user holds an index $i \in \{1, \cdots, n\}$. The user wants to get $x[i]$ without leaking his index to database. A trivial way is that database sends x to user. So we only consider the non-trivial private information retrieval in which the bits sent from database to user is less the n.

Definition 1. (Private Information Retrieval) *Let (D, U) be an interactive protocol where D's input x is an n-bit string, and U's input i is an index of n. Then (D, U) is called a private information retrieval protocol if it has the following three properties:*

1. *Correctness: If both parties follow this protocol, then U outputs $x[i]$ at the end of the protocol.*

2. *Security: For each $n \in \mathbb{N}$, each i, $j \in \{1, \ldots, n\}$, each $x \in \{0,1\}^n$, for each polynomial time interactive Turing $D^{'}$, for all constants c, and all sufficiently large k, $|p_i - p_j| \leq k^{-c}$, where*

$$p_i = Pr\{(r_{D'}, r_U, t) \leftarrow t_{D',U}((1^k, x), \cdot, (1^k, n, i), \cdot) : D^{'}(1^k, x, r_{D'}, t) = 1\}$$
$$p_j = Pr\{(r_{D'}, r_U, t) \leftarrow t_{D',U}((1^k, x), \cdot, (1^k, n, j), \cdot) : D^{'}(1^k, x, r_{D'}, t) = 1\}$$

3. *Communication complexity: The bits that sent form D to U is at most $n-1$.*

Property 1 is sometimes relaxed to allowing a negligible probability of error. In this paper, the user always gets the correct output.

Property 2 says that for any two distinct indices i and j, database can distinguish between the messages that user uses i as input and the messages that user uses j as input with a negligible probability. Thus database can't learn user's input.

1-out-of-2 Oblivious Transfer($\binom{1}{2}$-OT)

Informally, a 1-out-of-2 Oblivious Transfer scheme is an interactive protocol between two parties, Alice A and Bob B. Alice holds two bits b_0 and b_1, and Bob holds a bit c. Bob wants to get b_c from Alice without leaking c to Alice. Alice also wants to protect $b_{\bar{c}}$ from leaking it to Bob.

Definition 2. (1-out-of-2 Oblivious Transfer) *Let (A, B) be an interactive protocol where A's input is a pair of bits (b_0, b_1), and B's input is a bit c. We say that (A, B) is a 1-out-of-2 Oblivious Transfer protocol if it holds that:*

1. *Correctness: If both parties follow this protocol, then B outputs b_c at the end of the protocol.*

2. *Privacy against Alice: For all probabilistic polynomial time Alice $A^{'}$, all b_0, b_1 $\in \{0,1\}$, all constant d, and all sufficiently large k,*

$$Pr\{c \leftarrow 0, 1; (r_{A'}, r_B, t) \leftarrow t_{A',B}((1^k, b_0, b_1), \cdot, (1^k, c), \cdot) : \\ A^{'}(1^k, b_0, b_1, r_{A'}, t) = c\} \leq 1/2 + k^{-d}$$

3. *Privacy against Bob: For all probabilistic polynomial time Bob $B^{'}$ all b_0, $b_1 \in \{0,1\}$, all $c^{'} \in \{0,1\}$, and all random strings $r_{B'}$, there exists $c \in \{0,1\}$ such that for all constant d, and all sufficiently large k,*

$$Pr\{(b_0, b_1) \leftarrow 0, 1^2; (r_A, t) \leftarrow t_{A,B'}((1^k, b_0, b_1), \cdot, (1^k, c^{'}), r^{'}_B) : \\ B^{'}(1^k, c^{'}, r_{B'}) = b_{\bar{c}}\} \leq 1/2 + k^{-d}$$

As in PIR, the property 1 is sometimes relaxed to allowing a negligible probability of error. In this paper, Bob always gets the correct output.

1-out-of-2 Weak Oblivious Transfer((p,q)-$\binom{1}{2}$-WOT)

A 1-out-of-2 Weak Oblivious Transfer scheme is a generalized 1-out-of-2 Oblivious Transfer scheme in which the security properties are relaxed. A 1-out-of-2 Weak Oblivious Transfer scheme is a interactive protocol between two parties, Alice A and Bob B. Alice holds two bits b_0 and b_1, and Bob holds a bit c. Bob wants to get b_c from Alice. But Bob can know c with some, and Alice also can know $b_{\bar{c}}$ with some probability.

Definition 3. ((p,q)-$\binom{1}{2}$-WOT) *Let (A,B) be an interactive protocol where A's input is a pair of bits (b_0,b_1), and B's input is a bit c. We say that (A,B) is a (p,q)-$\binom{1}{2}$-WOT protocol if it holds that:*

1. *Correctness: If both parties follow this protocol, then B outputs b_c at the end of the protocol.*
2. *Privacy against Alice: For all probabilistic polynomial time Alice A', her probability for exactly knowing Bob's input c is at most p.*
3. *Privacy against Bob: For all probabilistic polynomial time Bob B', his probability for exactly knowing Alice's input (b_0,b_1) is at most q.*

Note the relaxation is that one player can know the other player's input with some probability, otherwise he should learns nothing from the other player. For example, Alice can know c with probability p, it means that Alice's probability for guessing c correctly is $p + (1-p)/2 = 1/2 + p/2$, so the bias for Alice to guess c correctly is $p/2$. Similarly, the bias for Bob to guess $b_{\bar{c}}$ correctly is $q/2$.

An immediate question is that can $\binom{1}{2}$-OT be reduced to (p,q)-$\binom{1}{2}$-WOT? It is intuitive that if Alice or Bob get too much information from the other player, (p,q)-$\binom{1}{2}$-WOT shouldn't be complete in the two-party scenario, so $\binom{1}{2}$-OT can't be reduced to (p,q)-$\binom{1}{2}$-WOT. The following theorem was proved in [16].

Theorem 2.1. *$\binom{1}{2}$-OT can be reduced to (p,q)-$\binom{1}{2}$-WOT iff $p + q < 1$.*

Note that the reduction in [16] works for the (p,q)-$\binom{1}{2}$-WOT that defined above. However, if we define (p,q)-$\binom{1}{2}$-WOT as that Alice can guess Bob's input correctly with probability $1/2 + p/2$, and Bob can guess Alice input correctly with probability $1/2 + q/2$, the reduction also works. We will use this feature in later.

Cheating Behavior

There are two cheating behavior in the two-party scenario. The first one, called semi-honest(honest-but-curious), is that a cheating player follows the protocol, and tries to break the protocol according to the information he got. The second one, called malicious, is that a cheating player may not follow the protocol, and tries to break the protocol. For example, if a protocol says that a player A should choose a string x randomly, then for a malicious player $A^{'}$, he may choose x according to some information he got, and tries to get more advantage to break the protocol.

Mathematical Backgrounds

Definition 4. *Let x be a random variable where $x \in \{0, 1\}$. we define the advantage for guessing x as:*

$$|Pr\{x = 0\} - Pr\{x = 1\}|$$

Lemma 2.2. *Let x_1, x_2, $\cdots$, x_n be n independent randomly variables where $x_i \in \{0, 1\}$, and $|Pr\{x_i = 0\} - Pr\{x_i = 1\}| \leq \epsilon$ for all $i \in \{1, \cdots, n\}$. Let $x = \oplus_{i=1}^{n} x_i$, then*

$$|Pr\{x = 0\} - Pr\{x = 1\}| \leq \epsilon^n$$

Proof. Let $y_1, y_2, \cdots, y_n$ be n independent randomly variables and $y = \Pi_{i=1}^{n} y_i$, where

$$y_i = \begin{cases} 1 & \text{if } x_i = 0 \\ \text{-1} & \text{if } x_i = 1 \end{cases}$$

So $Pr\{x_i = 0\} - Pr\{x_i = 1\} = E[y_i]$, the expected value of y_i, and solving $Pr\{x = 0\} - Pr\{x = 1\}$ is equivalent to solving the expected value of y.

$$\begin{aligned} |E[y]| &= |E[\Pi_{i=1}^{n} y_i]| \\ &= \Pi_{i=1}^{n} |E[y_i]| \\ &= \Pi_{i=1}^{n} |Pr\{x_i = 0\} - Pr\{x_i = 1\}| \\ &\leq \epsilon^n \end{aligned}$$

□

The lemma says that if for each random variable x_i where $i \in \{1, \cdots, n\}$, we can only guess its value correctly with advantage ϵ, then we can only guess $x = \oplus_{i=1}^{n} x_i$ correctly with advantage ϵ^n, which is negligible when n is large.

Chapter 3

Malicious PIR implies OT

In this chapter we will present a $\binom{1}{2}$-OT protocol that works against malicious players from any PIR scheme. The protocol is based on the $\binom{1}{2}$-OT protocol against semi-honest players in [15], and is simpler than their protocol for malicious players.

Protocol 1. $\binom{1}{2}$*-OT*
A's input: b_0*,* $b_1 \in \{0,1\}$*.*
B's input: $c \in \{0,1\}$*.*

1. *A randomly chooses* n *strings* $X_1, X_2, ..., X_n$*, where* $X_i \in \{0,1\}^k$*, for all* $i \in \{1,2,...,n\}$

2. *A randomly chooses* $2n$ *indices* $I_0^1, I_0^2, ..., I_0^n$ *and* $I_1^1, I_1^2, ..., I_1^n$*, where* $I_i^j \in \{1,2,...,k\}$*, and sends them to B*

3. *For* $i = 1$ *to* n*, A and B invoke the PIR protocol, where A plays the role of database and uses* X_i *as database string, and B plays the role of user and uses* I_c^i *as index. Let* $Y_1, Y_2, ..., Y_n$ *denote the bits that B retrieved.*

4. *A sets* $m_0 = b_0 \oplus X_1[I_0^1] \oplus X_2[I_0^2] \oplus ... \oplus X_n[I_0^n]$*, and* $m_1 = b_1 \oplus X_1[I_1^1] \oplus X_2[I_1^2] \oplus ... \oplus X_n[I_1^n]$*, and sends* m_0 *and* m_1 *to B.*

5. *B computes* $b_c = m_c \oplus Y_1 \oplus Y_2 \oplus ... \oplus Y_n$*.*

Correctness: If A and B both follow this protocol, B can get $X_i[I_c^i]$ at each execution of PIR. After step 5, B knows $X_1[I_c^1]$, $X_2[I_c^2]$, $\cdots$, $X_n[I_c^n]$ and m_c. With these information, B can compute b_c correctly.

Privacy Against Alice: Informally speaking, B's security follows from the user's privacy in the PIR protocol. Since the PIR protocol guarantees that A gets no information about the index used by B, A cannot tell between the two indices. For the sake of contradiction, assume that after running this protocol, A can compute c with probability at least $1/2 + \delta$, where δ non-negligible. It means that A can guess which index sequence is the retrieved indices with probability $1/2 + \delta$. since all the PIR invocations are independent, then for some position $j \in \{1, \cdots, n\}$, A can tell which index is used by user between I_0^j and I_1^j with non-negligible probability $1/2 + \delta/n$, a contradiction.

Privacy Against Bob: If Bob is semi-honest, the security had been shown in [15]. So suppose Bob is malicious. Since Alice chooses all strings and all indices, and Bob sends no messages to Alice except the execution of the PIR subprotocol, then the only cheating way for malicious Bob is that he uses indices that different from I_c^i in some execution of the PIR subprotocol. There are totally $2n$ indices, and the PIR subprotocol is only invoked n times. Hence, for some $c^{'} \in \{0, 1\}$, Bob uses at most half of the n indices of $I_{c^{'}}^i$. Since Alice sends at most $k - 1$ bits to Bob in each execution of PIR subprotocol, Bob has some error probability to guess $X[I_{c^{'}}^i]$ if he didn't choose $I_{c^{'}}^i$ in the $i - th$ execution of PIR subprotocol. In order to show Alice's privacy against Bob, we need the following lemma that was proved in [15].

Lemma 3.1. *Let* $(D,\, U)$ *be a PIR scheme with database length* k *and communication complexity* $c_D(k)$*. Let* j *be chosen uniformly from* $\{1, \cdots, k\}$ *at random and* x *be chosen uniformly from* $\{0, 1\}^k$*. Then there exists a constant* $l > 0$ *such that for every interactive Turing machine* $U^{'}$*, every* $r_{U'}$*, and every* k*,either*

$$Pr\{(r_D, t) \leftarrow t_{D,U'}((1^k, x), \cdot, 1^k, r_{u'}) : U^{'}(1^l, r_{U'}, t, j) \neq x_k\} > l.$$

or

$$Pr\{(r_D, t) \leftarrow t_{D,U'}((1^k, x), \cdot, 1^k, r_{u'}) : U^{'}(1^l, r_{U'}, t, j) \neq x_k\} \geq (1 - c_D(k)/k)^2.$$

The lemma says that for a uniformly chosen data string x for D, every cheating user $U^{'}$, after running $(D, U^{'})$, has a non-negligible probability that fails in reconstructing a data bit $x[j]$ in a uniformly chosen location j. So every cheating Bob only can guess $x[j]$ with advantage at most ϵ, which is related to l or $(1 - c_D(k)/k)^2$.

WLOG, we assume that Bob chooses at least $n/2$ indices from $I_0^1, \ldots, I_0^n$ to invoke the PIR subprotocol. So there are at least $n/2$ indices that not chosen by Bob in $I_1^1, \ldots, I_1^n$. Assume that Bob chooses $I_0^1, \ldots, I_0^t$ and $I_1^{t+1}, \ldots, I_1^n$, and Bob wants to guess $b_1 = m_1 \oplus X_1[I_1^1] \oplus \ldots \oplus X_t[I_1^t] \oplus X_{t+1}[I_1^{t+1}] \oplus \ldots \oplus X_n[I_1^n]$. By **Lemma 2.2.**, we know that Bob's advantage for guessing $X_1[I_1^1] \oplus \ldots \oplus X_t[I_1^t]$ is at most ϵ^{n-t} $\leq \epsilon^{n/2}$. So Bob's advantage for guessing b_1 is at most $\epsilon^{n/2}$.

Remark Note that our reduction is a black-box reduction. It means that the $\binom{1}{2}$-OT protocol uses the PIR protocol as a subroutine with the only guarantee that the bits sent from database to user is strictly less then the size of database. The reduction doesn't rely on any specific features of the implementation of the PIR protocol, and doesn't need and additional assumption about the implementation. Thus any idealized implementation of this primitive (as a black-box) will also work for this reduction.

Chapter 4

The Completeness of Weak PIR

In this chapter, we discuss the question: In a two-party scenario, how weak can a weak PIR model be that is still complete? For this purpose, we define a weak PIR model. Then, we will give two bounds, one is for impossibility result and the other is for possibility result.

4.1 Definition

We define the weak PIR model in a intuitive way:

Definition 5. *A (p, k) WPIR is a two-party protocol between a database D and a user U, where D's input x is a n-bits string and U's input i is an index of n. The model has three properties:*

1. *Correctness: If both parties follow this protocol, then U outputs $x[i]$ at the end of the protocol.*
2. *Security: After this protocol, for any cheating Database D', he can know U's index i with probability at most p.*
3. *Communication complexity: The bits that sent form Database to User is at most k.*

4.2 Impossibility Results

Is any (p, k)-WPIR protocol strong enough so that it can be complete? Intuitively speaking, if p becomes larger and larger, database will get more and more information; and if k is larger and larger, user will get more information. So how large van p and k be so that a (p, k)-WPIR is still complete?

It is well known that in a two-player setting with only noiseless communication, OT with information theoretic security is not possible, even if players are semi-honest [24]. Hence, if any two-player protocol can be securely implemented with only noiseless communication, then OT can not be reduced to it.

Now, we show how to implement a (p, k)-WPIR in this manner for $p \geq 1/k$. Consider the following protocol, in which Database D's input x is a string of length n, and User U's input i is an index from $\{1, \ldots, n\}$.

Protocol 2. *Sim*(p, k)*-WPIR*

1. *U chooses $k-1$ indices from $\{1, \ldots,\ i-1\}$, $\{i+1,\ \ldots,\ n\}$ at random, and sends them and i to D in a random order.*

2. *D sends the k bits of x to U according to the k indices he received.*

By a straightforward analysis, since all the information D gets is the k indices, the probability p that D can know U's index is at most $1/k$. So this is a valid (p, k)-WPIR protocol where $p = 1/k$. Suppose we have an $\binom{1}{2}$-OT protocol based on a (p, k)-WPIR protocol where $p = 1/k$. If we replace each execution of (p, k)-WPIR by Sim(p, k)-WPIR, then the $\binom{1}{2}$-OT protocol should still be secure since Sim(p, k)-WPIR has the same security and communication complexity with (p, k)-WPIR. Therefore, we get a $\binom{1}{2}$-OT with only noiseless communication, a contradiction.

The above argument was for $p = 1/k$. If $p > 1/k$, choose $p' = 1/k$, the impossibility argument works for (p', k)-WPIR$_1$. Since $p' < p$, a (p', k)-WPIR primitive also meets the requirements of a (p, k)-WPIR. Therefore, if OT can't be reduced to (p', k)-WPIR, it can't be reduced to (p, k)-WPIR, either. We conclude the above arguments to the following lemma.

Lemma 4.1. *There is no reduction from OT to (p, k)-WPIR for any $p \geq 1/k$, even if only security against semi-honest parties is required.*

4.3 Reducing Weak OT to Weak PIR

The previous section shows the impossibility results for $p \geq 1/k$. An immediate question is: When $p < 1/k$, can OT be reduced to (p, k)-WPIR? In this section, we will give a bound for possibility result.

Lemma 4.2. *Let n be the length of Database's input and l be defined as in* **Lemma 3.1.**. *$\binom{1}{2}$-OT can be reduced to (p, k)-WPIR for either $p < \frac{1}{k} - \frac{2(n-k)}{n} - \frac{1}{n}$ or $p < \frac{1}{k} - 2t + \frac{n+k-1}{n}$ where $t = 1 - l$.*

Proof. We describe our proof idea. In the previous chapter, we construct a protocol that reduce OT to PIR. So if we replace each execution of PIR by Weak PIR, can we get a protocol that reduce Weak OT to Weak PIR? Consider the following protocol:

Protocol 3. $(p^{'}, q^{'})$-$WOT(b_0, b_1)(c)$

1. *A randomly chooses an n-bit string x.*
2. *B randomly chooses two indices I_0 and I_1, where I_0 and $I_1 \in \{1, 2, ..., n\}$, and sends them to A.*
3. *A and B invoke the Weak PIR protocol (p, k) WPIR, where A plays the role of database and uses x as input, and B plays the role of user and uses I_c as input. Let Y denote the bit that B retrieved.*
4. *A sets $m_0 = b_0 \oplus X[I_0]$, and $m_1 = b_1 \oplus X[I_1]$, and sends m_0 and m_1 to B.*
5. *B computes $b_c = m_c \oplus Y$.*

This protocol is a simplified version of **Protocol 1**, so the correctness follows. Now, we look at what $p^{'}$ and $q^{'}$ are. It's clear that if A knows B's index c if and only if he knows which index that B used in the execution of Weak PIR. Since the execution of Weak PIR has probability p that leak the index c to Database, the probability that A knows c is at most p.

We now start looking at what $q^{'}$ is. What is the best way of Bob for guessing $b_{\bar{c}}$? Since Bob only knows two randomly chosen indices I_0, I_1, and the messages he got during the execution the PIR subprotocol, his best way for guessing $b_{\bar{c}}$ is to guess $x[I_{\bar{c}}]$ according to these information. Therefore, the probability that Bob knows $b_{\bar{c}}$ is equivalent to the probability that Bob knows $X[I_{\bar{c}}]$ after the execution of the PIR subprotocol. By **Lemma 3.1.**, we know that the probability that Bob fails to reconstruct $X[I_{\bar{c}}]$ is non-negligible. For example, if $k = n - 1$, the failure probability is at least $(1 - k/n)^2$, and if $k \leq k/2$, the failure probability is constant. Thus, the probability that Bob learns both $X[I_c]$ and $X[I_{\bar{c}}]$ is at most either $(2kn - k^2)/n^2$ or some constant t. Since (p, q)-WOT means that Bob can guess $b_{\bar{c}}$ correctly with probability at most $1/2 + q/2$, Therefore

$$\begin{aligned} q^{'} &\leq 2(\frac{2kn - k^2}{n^2} - \frac{1}{2}) \\ &= \frac{k-1}{n} + \frac{3kn - 2k^2 - n^2 + n}{n^2} \\ &< \frac{k-1}{n} + \frac{2kn + n^2 - 2k^2 - n^2 + n}{n^2} \\ &< \frac{k-1}{n} + \frac{2k(n-k) + n}{n^2} \\ &< \frac{k-1}{n} + \frac{2(n-k)}{n} + \frac{1}{n} \end{aligned}$$

or

$$\begin{aligned} q^{'} &\leq 2(t-\frac{1}{2}) \\ &< \frac{k-1}{n}+2t-\frac{n+k-1}{n}. \end{aligned}$$

Therefore, if $q^{'} < \frac{k-1}{n}+\frac{2(n-k)}{n}+\frac{1}{n}$, we choose $p^{'} < \frac{1}{k}-\frac{2(n-k)}{n}-\frac{1}{n}$ such that

$$\begin{aligned} p^{'}+q^{'} &< \frac{1}{k}-\frac{1}{n}+\frac{k-1}{n}+\frac{1}{n} \\ &= \frac{1}{k}+\frac{k-1}{n} \\ &< \frac{1}{k}+\frac{k-1}{k} \\ &= 1, \end{aligned}$$

and if $q^{'} < \frac{k-1}{n}+2t-\frac{n+k-l}{n}$, we choose $p^{'} < \frac{1}{k}-2t+\frac{n+k-1}{n}$ such that $p^{'}+q^{'} < 1$.
□

Bibliography

[1] A. Ambainis, "Upper Bound on the Communication Complexity of Private Information Retrieval", In Proc. of 24th ICALP, 1997.

[2] Y. Aumann, Y. Z. Ding, and M. O. Rabin, "Everlasting Security in the Bounded Storage Model".

[3] A. Beimel, T. Malkin and S. Micali, "The All-or-Nothing Nature of Two-Party Secure Computation", In Proc. of Crypto 99, 1999.

[4] C. H. Bennett, G. Brassard, C. Crepeau, and U. Maurer, "Generalized Privacy Amplification", IEEE Transactions of Information Theory, 41(6), 1995.

[5] G. Brassard, C. Crepeau and J. M. Robert, "All-or-Nothing Disclosure of Secrets", In Crypto'86, 1987, pp. 234-238.

[6] G. Brassard and C. Crepeau, "Oblivious Transfer and Privacy Amplification", EUROCRYPT'97, LNCS series, vol. 1223, pp. 334-347. C. Cachin, "On the foundations of Oblivious Transfer", EUROCRYPT'98, LNCS series, vol.1403, pp. 361-374.

[7] G. Brassard, C. Crepeau, and M. Santha. "Oblivious Transfer and Intersecting Codes". IEEE Trans. Info. Theory, vol. 42, No. 6, pp. 1769-1780. 1996.

[8] C. Cachin, "On the Foundations of Oblivious Transfer", EUROCRYPT'98, LNCS series, vol. 1403, pp. 361-374.

[9] C. Cachin, C. Crepeau, and S. Marcil,"Onlivious Transfer with a Momory Bounded Receiver", In Proc. of 39th FOCS, 1998.

[10] C. Cachin and U. Maurer, "Unconditional Security Against Memory Bounded Adversaries", In Advances in Cryptology - Crypto'97, 1997.

[11] B. Chor, abd N. Gilboa, "Computationally Private Information Retrieval", In Proc. of 29th STOC, 1997.

[12] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private Information Retrieval", FOCS 1995, pp. 41-50.

[13] C. Crepeau, "Equivalence Between Two Flavours of Oblivious Transfer", CRYPTO'87, LNCS series, pp. 350-354.

[14] C. Crepeau, "Efficient Cryptographic Protocols based on Noisy Channels", Eurocrypt'97, LNCS series, vol. 1233, pp. 306-317.

[15] C. Crepeau and J. Kilian, "Achieving Oblivious Transfer using Weakened Security Assumptions", FOCS 88, pp. 42-52.

[16] G. D. Crescenzo, T. Malkin, and R. Ostrovsky, "Single Database Private Information Implies Oblivious Transfer", EUROCRYPT 2000, LNCS 1807, pp. 122-138.

[17] I. Damgård, J. Kilian, and L. Salvail, "On the (Im) possibility of Basing Oblivious Transfer and Bit Commitment on Weakened Security Assumptions". EUROCRYPT'99, LNCS 1592, pp.56-73.

[18] A. De-Santis and P. Persiano, "Zero-Knowledge Proofs of Knowledge without Interaction", In Proc. of 33rd FOCS, 1992.

[19] Y. Z. Ding, "Oblivious Transfer in the Bounded Storage Model", Crypto 2001, pp. 155-170.

[20] S. Even, O. Goldreich, and A. Lempel, "A randomized Protocol for signing contracts", Communications of the ACM, Vol. 28, No. 6, 1985, pp. 637-647.

[21] U. Feige and A. Shamir, "Witness Indistinguishable and Witness Hiding Protocols", In Proc. of 23rd STOC, 1990.

[22] O. Goldreich, S. Micali, and A. Wigderson, "How to play ANY mental game", Proceedings of the 19th Annual ACM Symposium on the Theory of Computing, 1987, pp. 218-229.

[23] O. Goldreich, S. Micali, and A. Wigderson, "Proofs that Yield Nothing but their Validiaty, and a Methodology of Cryptographic Protocol Design", In Journal of the ACM, vol. 38, 1991, pp. 691-729.

[24] J. Halpern and M.O. Rabin, "A Logic to Reason about likehood", Proceedings of the 15th Annual ACM Symposium on the Theory of Computing, 1983, pp. 310-319.

[25] J. Kilian, "A general completeness theorem for 2-party games", Proceedings of the 23rd Annual ACM Symposium on the Theory of Computing, 1991, pp. 553-560.

[26] J. Kilian, "Founding Cryptography on Oblivious Transfer", STOC 1988, pp. 20-31.

[27] U. Maurer and S. Wolf, "Privacy Amplification Secure Against Active Adversaries", In Advances in Cryptology - Crypto'97, 1997.

[28] M. Naor, "Bit Commitment Using Pseudorandom Generators", Journal of cryptology 1991, pp. 151-158.