How to Derive Lower Bound on Oblivious Transfer Reduction

Kaoru Kurosawa
Department of Computer and Information Sciences, Ibaraki University,
4-12-1 Nakanarusawa, Hitachi, Ibaraki, 316-8511, Japan.
Email: kurosawa@mx.ibaraki.ac.jp

Wataru Kishimoto
Department of Information and Image Science, Chiba University,
Email: wkishi@faculty.chiba-u.jp

Takeshi Koshiba
Division of Mathematics, Electronics and Informatics,
Graduate School of Science and Engineering, Saitama University,
255 Shimo-Okubo, Sakura, Saitama 338-8570, Japan.
Email: koshiba@tcs.ics.saitama-u.ac.jp

Abstract

Suppose that we are given an ideal oblivious transfer protocol (OT). We wish to construct a larger OT by using the above OT as a blackbox. Then how many instances of the given ideal OT should be invoked ? For this problem, some lower bounds were derived using entropy. In this paper, we show more tight lower bounds by using combinatorial techniques. Roughly speaking, our lower bounds are two times larger than the previous bounds.

Keywords: Oblivious Transfer, Reduction, Lower bound, Combinatorial Approach

1 Introduction

1.1 Background

A two-party protocol called Oblivious Transfer (OT) is a fundamental primitive in cryptography. Most notably, it is known that any secure multiparty computation can be based on OT [11, 8, 9]. A typical form of oblivious transfer is an L-bit $(1, N)$-OT. In this protocol, Alice (who is a sender) has N secret strings $s_0, s_1, \cdots, s_{N-1} \in \{0,1\}^L$, and Bob (who is a receiver) has a secret $c \in \{0, 1, \cdots, N-1\}$. At the end of the protocol, Bob receives s_c (completeness). But he has no information on the other Alice's secret $\{s_0, s_1, \cdots, s_{N-1}\} \setminus \{s_c\}$ (sender's privacy). On the other hand, Alice has no information on Bob's secret c (receiver's privacy).

Several researchers showed how to construct an L-bit $(1, N)$-OT by using an ℓ-bit $(1, n)$-OT as a blackbox in the information theoretic sense (that is, without any computational assumptions) [2, 1, 4], where $L \geq \ell$ and $N \geq n$ usually. Such a realization is called information-theoretic OT-reduction. OT-reduction must be efficient because even the implementation of small OT may be expensive to run. Then how many instances of ℓ-bit $(1, n)$-OT must be invoked so as to obtain L-bit $(1, N)$-OT ? Dodis and Micali considered this problem and showed the first lower bound for this problem [7]. Such a lower bound is called a lower bound for information-theoretic OT-reduction. Wolf and Wullschleger presented another lower bound [10]. All these bounds were derived by using *entropy*.

Recently, Crépeau and Savvides showed a very efficient reduction of a string $(1, 2)$-OT to a bit $(1, 2)$-OT [6]. However, a small error probability is allowed in their model [6, Theorem 2,4].

1.2 Our Contribution

In this paper, we study lower bounds on information-theoretic OT-reduction by using combinatorial techniques. (That is, we study lower bounds on the number of instances of ℓ-bit $(1, n)$-OT which must be invoked so as to obtain L-bit $(1, N)$-OT.) We first derive more tight lower bounds than the previous bounds by using a simple counting argument. Roughly speaking, the proposed bounds are two times larger than the previous bounds. We next improve these bounds by using orthogonal arrays for large L.

Please note that our lower bounds do not contradict with the recent reduction of Crépeau and Savvides [6] because a small error probability is allowed in their model [6, Theorem 2,4].

2 Oblivious Transfer (OT)

As an ℓ-bit $(1,n)$-Oblivious Transfer, imagine an ideal world as follows. Alice has n secret strings of ℓ bits $s_0, s_1, \cdots, s_{n-1} \in \{0,1\}^\ell$, and Bob has a secret $c \in \{0, 1, \cdots, n-1\}$.

1. First, Alice sends $s_0, s_1, \cdots, s_{n-1}$ to a trusted third party (TTP), and Bob sends c to TTP.
2. Next TTP sends s_c to Bob.

We say that the above three party protocol (Alice, Bob, TTP) is the ideal ℓ-bit $(1,n)$-Oblivious Transfer.

By using the above ideal ℓ-bit $(1,n)$-Oblivious Transfer as a building block, we are interested in to construct a *two*-party L-bit $(1,N)$-Oblivious Transfer protocol (Alice, Bob) which satisfies the following three conditions, where $L \geq \ell$ and $N \geq n$.

Completeness. If Alice and Bob follow the protocol, then Bob receives s_c.

Receiver's privacy. For any infinitely powerful $\tilde{A}$, $\tilde{A}$ learns no information on c when $(\tilde{A}, B)$ is executed.

Sender's privacy. For any infinitely powerful $\tilde{B}$, $\tilde{B}$ learns no information on $s_0, s_1, \cdots, s_{N-1}$ other than some s_c when $(A, \tilde{B})$ is executed.

More formally, sender's privacy is defined as follows. For $i = 0, 1, \cdots, N-1$, let S_i denote the random variable induced by $s_i \in \{0,1\}^L$. For each i, we assume that

$$\Pr(S_i = \alpha) > 0$$

for any $\alpha \in \{0,1\}^L$. We also assume that each S_i is independent each other.

Let *view* denote the view of Bob (receiver) which consists of his random coin tosses and the messages that he received from Alice. Let $View$ denote the random variable induced by *view*.

Definition 2.1 *(Sender's privacy) We say that sender's privacy is satisfied if for any infinitely powerful $\tilde{B}$ and his any possible view, there exists $c \in \{0, 1, \cdots, N-1\}$ such that for any $i \neq c$,*

$$\Pr(S_i = \alpha \mid View = view) = \Pr(S_i = \alpha) > 0$$

for any $\alpha \in \{0,1\}^L$.

For two strings R_0 and R_1, let $R_0||R_1$ denote the concatenation.

3 Previous Results

Suppose that we want to construct an L-bit $(1,2)$-OT from t instances of the ideal ℓ-bit $(1,2)$-OT. Brassard, Crépeau and Santha [2] showed a construction such that $t = \kappa L$, where $\kappa > 3.5277$ asymptotically [1]. For a weaker notion of sender's privacy, Brassard and Crépeau [1] showed a more efficient construction such that $t = 2L + s$, where s is a security parameter.

On the other hand, Dodis and Micali showed the first lower bound on t as follows [7].

Proposition 3.1 *Suppose that there exists an L-bit $(1,N)$-OT which invokes t instances of the ideal ℓ-bit $(1,n)$-OT. Then we have*

$$t \geq \frac{L}{\ell} \times \frac{N-1}{n-1}.$$

Wolf and Wullschleger presented another lower bound as follows [10].

Proposition 3.2 *Suppose that there exists an L-bit $(1,N)$-OT which invokes t instances of the ideal ℓ-bit $(1,n)$-OT. Then we have*

$$t \geq \log N / \log n, \qquad (1)$$

$$t \geq L/\ell. \qquad (2)$$

In particular, for $N = n = 2$ and $\ell = 1$, we have the following corollary from Proposition 3.1 and Proposition 3.2. This is the most tight bound known so far for $N = n = 2$ and $\ell = 1$.

Corollary 3.1 *Suppose that there exists an L-bit $(1,2)$-OT which invokes t instances of the ideal 1-bit $(1,2)$-OT. Then we have $t \geq L$.*

Also, eq.(2) is the best known bound for $L \geq \ell$ and $N < 2n - 1$. All the above bounds were derived by using entropy.

4 Our First Lower Bound

In this section, we derive our lower bounds by using a simple counting argument (while the previous bounds were derived by using entropy). We consider the reduction of L-bit $(1, 2)$-OT to 1-bit $(1, 2)$-OT first, and then the reduction of L-bit $(1, n)$-OT to ℓ-bit $(1, n)$-OT. Our bounds are more tight than the previous bounds. See Sec.2 for the definition of ideal OT.

4.1 Lower Bound for $(1, 2)$-OT

Theorem 4.1 *Suppose that there exists an L-bit $(1, 2)$-OT which invokes t instances of the ideal 1-bit $(1, 2)$-OT. Then we have*

$$t \geq 2L - 1.$$

(Proof) Suppose that there exists an L-bit $(1, 2)$-OT which invokes t instances of the ideal 1-bit $(1, 2)$-OT. In the L-bit $(1, 2)$-OT protocol,

- Alice has two secret strings $s_0, s_1 \in \{0, 1\}^L$ and Bob has a choice bit c.
- At the end, Bob receives s_c.

We denote by $Alice(R_A; s_0, s_1)$ Alice who has R_A as her random tape and s_0, s_1 as her input, where $s_0, s_1 \in \{0, 1\}^L$. We also denote by $Bob(R_B; c)$ Bob who has R_B as his random tape and c as his input, where $c \in \{0, 1\}$. Let $com(Alice(R_A; s_0, s_1), Bob(R_B; c))$ denote the communication sequence between $Alice(R_A; s_0, s_1)$ and $Bob(R_B; c)$ other than the t invocations of the ideal 1-bit $(1, 2)$-OT.

Fix R_A, s_0 and s_1 arbitrarily. For some R_0 and $c = 0$, let

$$\mathbf{com_0} = com(Alice(R_A; s_0, s_1), Bob(R_0; 0)). \tag{3}$$

Since Alice learns no information on c, there exists R_1 for $c = 1$ such that

$$\mathbf{com_0} = com(Alice(R_A; s_0, s_1), Bob(R_1; 1)). \tag{4}$$

Denote the ith invocations of the ideal 1-bit $(1, 2)$-OT in $(Alice(R_A; s_0, s_1), Bob(R_0; 0))$ by $\mathbf{OT_0}(i)$ and the one in $(Alice(R_A; s_0, s_1), Bob(R_1; 1))$ by $\mathbf{OT_1}(i)$. Suppose that $Alice(R_A; s_0, s_1)$ has (x_i, y_i) as input in $\mathbf{OT_0}(i)$ and (x'_i, y'_i) in

$\mathbf{OT_1}(i)$. Then $x_i = x'_i$ and $y_i = y'_i$ for $i = 1, \cdots, t$ because $(R_A; s_0, s_1)$ is the same and $\mathbf{com_0}$ is the same in $(Alice(R_A; s_0, s_1), Bob(R_0; 0))$ and $(Alice(R_A; s_0, s_1), Bob(R_1; 1))$. (That is, all the inputs to Alice are the same.)

Next without loss of generality, suppose that $Bob(R_0; 0)$ receives x_i in $\mathbf{OT_0}(i)$ for $i = 1, \cdots, t$. For $\mathbf{OT_1}(i)$, let

$$\Delta = \{i \mid Bob(R_1; 1) \text{ receives } x_i \text{ in } \mathbf{OT_1}(i)\}$$

and let $\delta = |\Delta|$.

(1) Suppose that $\delta = 0$. In this case, $Bob(R_1; 1)$ receives y_i in $\mathbf{OT_1}(i)$ for $i = 1, \cdots, t$. First suppose that $t = even$.

Consider malicious $\tilde{B}$ who behaves in the same way as $Bob(R_0; 0)$ does except for that it receives $Z = (x_1, \cdots, x_{t/2}, y_{(t/2)+1}, \cdots, y_t)$ in the t invocations of the ideal 1-bit $(1, 2)$-OT. $\tilde{B}$ also has $R_0||R_1$ as his random tape, where $||$ denotes concatenation. The view of $\tilde{B}$ is given by $\mathbf{view'} = (R_0||R_1, Z, \mathbf{com_0})$. [1]

It is helpful to note the following: Bob is an interactive Turing machine. But there exists a (usual) algorithm (based on Bob) such that

- it outputs s_0 on input $(R_0, (x_1, \cdots, x_t), \mathbf{com_0})$, and
- it outputs s_1 on input $(R_1, (y_1, \cdots, y_t), \mathbf{com_0})$.

By using this algorithm (Bob), $\tilde{B}$ can compute

- s_0 on input $(R_0||R_1, (x_1, \cdots, x_t), \mathbf{com_0})$, and
- s_1 on input $(R_0||R_1, (y_1, \cdots, y_t), \mathbf{com_0})$.

Now fix the above $\mathbf{view'}$, and do not fix R_A, s_0 and s_1 any more. Then $\tilde{B}$ has no information on either s_0 or s_1 from Sender's privacy. Without loss of generality, suppose that $\tilde{B}$ has no information on s_0. This means that for any L-bit string $\alpha \in \{0, 1\}^L$,

$$\Pr(S_0 = \alpha \mid View = \mathbf{view'}) = \Pr(S_0 = \alpha) > 0.$$

[1]Alternatively, we can say that $\tilde{B}$ behaves in the same way as $Bob(R_1; 1)$ does except for that it receives $Z = (x_1, \cdots, x_{t/2}, y_{(t/2)+1}, \cdots, y_t)$ in the t invocations of the ideal 1-bit $(1, 2)$-OT. This is possible because $\tilde{B}$ has $R_0||R_1$ as his random tape, and $\mathbf{com_0}$ is the same in the two simulations of Bob.

On the other hand, $(x_{t/2+1}, \cdots, x_t)$ are not fixed in **view′**. This means that $(x_{t/2+1}, \cdots, x_t) \in \{0,1\}^{t/2}$ uniquely determine $s_0 \in \{0,1\}^L$. In other words, there exists an onto mapping $F : \{0,1\}^{t/2} \rightarrow \{0,1\}^L$. This implies that $t/2 \geq L$. Hence

$$t \geq 2L. \tag{5}$$

Next suppose that $t = odd$. Let $t_0 = \lfloor t/2 \rfloor$ and $t_1 = \lceil t/2 \rceil$. Consider malicious $\tilde{B}$ who receives $(x_1, \cdots, x_{t_0}, y_{t_1}, \cdots, y_t)$ in the t invocations of the ideal $(1,2)$-OT. Then by using the same argument as above, we obtain that $t_0 \geq L$ or $t_1 \geq L$. Hence $t_1 \geq L$. This means that $t_0 = t_1 - 1 \geq L - 1$. Therefore,

$$t = t_0 + t_1 \geq L + (L-1) = 2L - 1. \tag{6}$$

From eq.(5) and eq.(6), we obtain that $t \geq 2L - 1$.

(2) Finally, suppose that $\delta > 0$. Then by applying the same argument to $\{1, \cdots, t\} \setminus \Delta$, we obtain that $t - \delta \geq 2L - 1$. This means that $t \geq 2L - 1$.

Q.E.D.

4.2 Generalization to $(1, n)$-OT

Theorem 4.2 *Suppose that there exists an L-bit $(1,n)$-OT which invokes t instances of the ideal ℓ-bit $(1,n)$-OT. Then we have*

$$t \geq 2\lceil L/\ell \rceil - 1.$$

(Proof) Suppose that there exists an L-bit $(1,n)$-OT which invokes t instances of the ideal ℓ-bit $(1,n)$-OT. In the L-bit $(1,n)$-OT protocol,

- Alice has n secret strings $s_0, \cdots, s_{n-1} \in \{0,1\}^L$ and Bob has a secret $c \in \{0, \cdots, n-1\}$.
- At the end, Bob receives s_c.

We use the same notation and the same argument as shown in the proof of Theorem 4.1. Although $c \in \{0, \cdots, n-1\}$, we consider $Bob(R_0; 0)$ for $c = 0$ and $Bob(R_1; 1)$ for $c = 1$.

First suppose that $t = even$. Then similarly to the proof of Theorem 4.1, there exists an onto mapping $F : \{0,1\}^{\ell t/2} \rightarrow \{0,1\}^L$. This implies that $\ell t/2 \geq L$. Hence we have

$$t \geq \lceil 2L/\ell \rceil. \tag{7}$$

Next suppose that $t = odd$. Then similarly to the proof of Theorem 4.1, we have

$$t = t_0 + t_1 \geq \lceil L/\ell \rceil - 1 + \lceil L/\ell \rceil = 2\lceil L/\ell \rceil - 1. \qquad (8)$$

From eq.(7) and eq.(8), we obtain that $t \geq 2\lceil L/\ell \rceil - 1$. Q.E.D.

5 Improved Bounds

In this section, we improve our lower bounds by using orthogonal arrays for large L.

5.1 Orthogonal Array

We define orthogonal arrays as follows.

Definition 5.1 *An orthogonal array $OA(m, k, d)$ is a $k \times m^d$ matrix of m symbols such that in any d rows, every one of the possible m^d tuples of symbols appears exactly once.*

Then Bush bound is known as follows [3, 5].

Proposition 5.1 (Bush bound) *An orthogonal array $OA(m, k, d)$ with $d > 1$ exists only if*

$$k \leq \begin{cases} m + d - 1 & \text{if } \ m \text{ even and } d \leq m, \\ m + d - 2 & \text{if } \ m \text{ odd and } 3 \leq d \leq m, \\ d + 1 & \text{if } \ d \geq m. \end{cases}$$

5.2 Improvement of Theorems 4.1 and 4.2

By using Bush bound, we can improve Theorems 4.1 and 4.2 as shown below.

Theorem 5.1 *For $L \geq 3$, suppose that there exists an L-bit $(1, 2)$-OT which invokes t instances of the ideal 1-bit $(1, 2)$-OT. Then we have*

$$t \geq 2L.$$

Theorem 5.2 *Let L/ℓ be an integer such that $L/\ell \geq 2^\ell + 1$. Suppose that there exists an L-bit $(1, n)$-OT which invokes t instances of the ideal ℓ-bit $(1, n)$-OT. Then we have*

$$t \geq 2L/\ell.$$

5.3 Proof of Theorem 5.1

From Theorem 4.1, it holds that $t \geq 2L-1$. Suppose that $t = 2L-1$. We use the same notation as in the proof of Theorem 4.1. Fix $R_0, R_1, \mathbf{com_0}, \mathbf{view}'$ as shown in the proof of Theorem 4.1.

Let Y_0 be the set of all $(y_1, \cdots, y_t)$ such that

$$\Pr(\text{ Bob receives } s_1 = 0^L \text{ }) > 0.$$

Let P be a $t \times |Y_0|$ matrix which consists of all $(y_1, \cdots, y_t)^T \in Y_0$. We will show that P is an $\mathrm{OA}(2, t, L-1)$.

Similarly to the proof of Theorem 4.1, consider malicious $\tilde{B}$ who receives

$$Z = (x_1, \cdots, x_L, y_{L+1}, \cdots, y_{2L-1})$$

in the t instances of the ideal 1-bit $(1,2)$-OT. It must be that $\tilde{B}$ has no information on either s_0 or s_1. Suppose that $\tilde{B}$ has no information on s_0. Then similarly to deriving eq.(5), we obtain that $L-1 \geq L$. However, this is a contradiction.

Therefore, $\tilde{B}$ has no information on s_1. In this case, there must exist an onto mapping $F : \{(y_1, \cdots, y_L)\} \to \{s_1\}$. This means that there exists a bijection between $\{(y_1, \cdots, y_L)\}$ and the set of s_1 because $\{s_1\} = \{0,1\}^L$. Hence for any $\gamma \in \{0,1\}^L$,

$$\Pr((y_1, \cdots, y_L) = \gamma) > 0.$$

In particular, we have

$$\Pr((y_1, \cdots, y_{L-1}) = 0^{L-1}) > 0.$$

Now for $(y_1, \cdots, y_{L-1}) = 0^{L-1}$, we can see that there exists a bijection between $\{(y_L, \cdots, y_{2L-1})\}$ and the set of s_1 such that $(y_1, \cdots, y_{L-1}, y_L, \cdots, y_{2L-1}) = (0^{L-1}, \beta)$ determines s_1 uniquely.

In particular, there exists a unique $\beta \in \{0,1\}^L$ such that $(y_1, \cdots, y_{2L-1}) = (0^{L-1}, \beta)$ determines $s_1 = 0^L$. This means that $(0^{L-1}, \beta)^T$ is a column of P and 0^{L-1} appears exactly once in the first $L-1$ rows. By the same argument, in the first $L-1$ rows, each $L-1$ bit string appears exactly once.

The above observation holds in any $L-1$ rows. Hence P is an $\mathrm{OA}(2, t, L-1)$. Then from Bush bound, it must be that

$$t \leq (L-1) + 1 = L$$

because $L \geq 3 > 2$. However, this is impossible because $t = 2L - 1$.

Hence it must be that $t \geq 2L$.

5.4 Proof of Theorem 5.2

From our assumption, $\eta = L/\ell$ is an integer. From Theorem 4.2, it holds that $t \geq 2L/\ell - 1 = 2\eta - 1$. Suppose that $t = 2\eta - 1$. We use the same notation as in the proof of Theorem 4.2. For $c \in \{0, \cdots, n-1\}$, we consider $Bob(R_0; 0)$ for $c = 0$ and $Bob(R_1; 1)$ for $c = 1$ as in the proof of Theorem 4.2. Note that $Alice(R_A; s_0, s_1)$ has (x_i, y_i) as input in both $\mathbf{OT_0}(i)$ and $\mathbf{OT_1}(i)$ where $x_i,\ y_i \in \{0, 1, \ldots, 2^\ell - 1\}$. Fix $R_0, R_1, \mathbf{com_0}, \mathbf{view'}$ as shown in the proof of Theorem 4.1.

Let Y_0 be the set of all $(y_1, \cdots, y_t)$ such that

$$\Pr(\text{ Bob receives } s_1 = 0^L\ ) > 0.$$

Let P be a $t \times |Y_0|$ matrix which consists of all $(y_1, \cdots, y_t)^T \in Y_0$. We will show that P is an $\mathrm{OA}(2^\ell, t, \eta - 1)$.

Similarly to the proof of Theorem 4.1, consider malicious $\tilde{B}$ who receives

$$Z = (x_1, \cdots, x_\eta, y_{\eta+1}, \cdots, y_{2\eta-1})$$

in the $t\ (= 2\eta - 1)$ instances of the ideal ℓ-bit $(1, n)$-OT. It must be that $\tilde{B}$ has no information on either s_0 or s_1. Suppose that $\tilde{B}$ has no information on s_0. Then similarly to deriving eq.(7), we obtain that $\ell(\eta - 1) \geq L$. Since $\ell\eta = L$, it implies $L - \ell \geq L$. However, this is a contradiction.

Therefore, $\tilde{B}$ has no information on s_1. In this case, there must exist an onto mapping $F : \{(y_1, \cdots, y_\eta)\} \to \{s_1\}$. This means that there exists a bijection between $\{(y_1, \cdots, y_\eta)\}$ and the set of s_1 because $|\{(y_1, \cdots, y_\eta)\}| = |\{0, 1, \ldots, 2^\ell - 1\}^\eta| = 2^{\ell\eta} = 2^L$ and $|\{s_1\}| = |\{0, 1\}^L| = 2^L$. Hence for any $\gamma \in \{0, 1, \ldots, 2^\ell - 1\}^\eta$,

$$\Pr((y_1, \cdots, y_\eta) = \gamma) > 0.$$

In particular, we have

$$\Pr((y_1, \cdots, y_{\eta-1}) = 0^{\eta-1}) > 0.$$

Now for $(y_1, \cdots, y_{\eta-1}) = 0^{\eta-1}$, we can see that there exists a bijection between $\{(y_\eta, \cdots, y_{2\eta-1})\}$ and the set of s_1 such that $(y_1, \cdots, y_{\eta-1}, y_\eta, \cdots, y_{2\eta-1}) = (0^{\eta-1}, \beta)$ determines s_1 uniquely.

In particular, there exists a unique $\beta \in \{0, 1, \ldots, 2^\ell - 1\}^\eta$ such that $(y_1, \cdots, y_{2\eta-1}) = (0^{\eta-1}, \beta)$ determines $s_1 = 0^L$. This means that $(0^{\eta-1}, \beta)^T$ is a column of P and $0^{\eta-1}$ appears exactly once in the first $\eta - 1$ rows. By the same argument, in the first $\eta - 1$ rows, each $\beta \in \{0, 1, \ldots, 2^\ell - 1\}^{\eta-1}$ appears exactly once.

The above observation holds in any $\eta-1$ rows. Hence P is an $\mathrm{OA}(2^\ell, t, \eta - 1)$. Then from Bush bound, it must be that

$$t \leq (\eta - 1) + 1 = \eta$$

because $\eta - 1 \geq 2^\ell$ from our assumption. However, this is impossible because $t = 2\eta - 1$.

Hence it must be that $t \geq 2\eta$.

6 Discussion

The following table shows a comparison of our bounds with the best known bounds. It is clear that our bounds are more tight.

Reduction	L-bit $(1, 2)$-OT to 1-bit $(1, 2)$-OT	L-bit $(1, n)$-OT to ℓ-bit $(1, n)$-OT
Previous	$t \geq L$ (Corollary 3.1)	$t \geq L/\ell$ (eq.(2))
This paper (1)	$t \geq 2L - 1$ (Theorem 4.1)	$t \geq 2\lceil L/\ell \rceil - 1$ (Theorem 4.2)
This paper (2)	$t \geq 2L$ if $L \geq 3$ (Theorem 5.1)	$t \geq 2L/\ell$ if $\eta = L/\ell$ is an integer and $\eta \geq 2^\ell + 1$ (Theorem 5.2)

Brassard, Crépeau and Santha [2] showed L-bit $(1, 2)$-OT which runs $n = \kappa L$ instances of 1-bit $(1, 2)$-OT, where $\kappa > 3.5277$ asymptotically [1]. Hence our bound of Theorem 5.1 has approached to the optimum.

We derived our bounds by using our combinatorial techniques while the previous bounds [7, 10] were derived by using entropy. We believe that our approach gives a new insight to the intuitive and essential understanding of oblivious transfer.

References

[1] G. Brassard and C. Crépeau: Oblivious transfers and privacy amplification. In, B. Kariski, *Advances in Cryptology — EUROCRYPT 1997*, Lecture Notes in Computer Science 1233, Springer, pp.334–347 (1997)

[2] G. Brassard, C. Cŕepeau and M. Santha: Oblivious transfers and intersecting codes. IEEE Transactions on Information Theory 42(6), pp.1769–1780 (1996)

[3] K. A. Bush: Orthogonal arrays of index unity. Annals of Mathematical Statistics 23, pp.426–434 (1952)

[4] C. Cachin: On the foundations of oblivious transfer. In, K. Nyberg (ed.), *Advances in Cryptology — EUROCRYPT 1998*, Lecture Notes in Computer Science 1403, Springer, pp.361–374 (1998)

[5] C.Colbourn and J.Dinitz: The CRC Handbook of Combinatorial Designs, CRC Press (1996)

[6] C. Crépeau and G. Savvides: Optimal reductions between oblivious transfers using interactive hashing. In, S. Vaudenay (ed.), *Advances in Cryptology — EUROCRYPT 2006*, Lecture Notes in Computer Science 4004, Springer, pp.201–221 (2006)

[7] Y. Dodis and S. Micali: Lower bounds for oblivious transfer reductions. In, J. Stern (ed.), *Advances in Cryptology — EUROCRYPT 1999*, Lecture Notes in Computer Science 1592, Springer, pp.42–55 (1999)

[8] O. Goldreich, S. Micali and A. Wigderson: How to play any mental game or a completeness theorem for protocols with honest majority. *Proc. 19th ACM Symposium on Theory of Computing*, pp.218–229 (1987)

[9] J. Kilian: Founding cryptography on oblivious transfer. *Proc. 20th ACM Symposium on Theory of Computing*, pp.20–31 (1988)

[10] S. Wolf and J. Wullschleger: New monotones and lower bounds in unconditional two-party computation. In, V. Shoup (ed.), *Advances in Cryptology — CRYPTO 2005*, Lecture Notes in Computer Science 3621, Springer, pp.467–477 (2005)

[11] A. C. Yao: How to generate and exchange secrets (Extended Abstract). *Proc. 27th IEEE Symposium on Foundations of Computer Science*, pp.162–167 (1986)