Direct Reduction of String $(1, 2)$-OT to Rabin's OT

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

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

It is known that string $(1, 2)$-OT and Rabin's OT are equivalent. However, two steps are required to construct a string $(1, 2)$-OT from Rabin's OT. The first step is a construction of a bit $(1, 2)$-OT from Rabin's OT, and the second step is a construction of a string $(1, 2)$-OT from the bit $(1, 2)$-OT. No direct reduction is known. In this paper, we show a direct reduction of string $(1, 2)$-OT to Rabin's OT by using a deterministic randomness extractor. Our reduction is much more efficient than the previous two-step reduction.

Keywords: Oblivious Transfer, Reduction

1 Introduction

Suppose that Alice (database company) has two secret strings, s_0 and s_1. Bob (user) wants to buy one s_c of them. But he wants to keep his privacy. That is, it must be that Alice does not know which one Bob bought. On the other hand, Alice wants to keep her privacy. That is, it must be that Bob does not know s_{1-c}. A two-party protocol which realizes the above goal is called a string $(1, 2)$-OT. The protocol is called a bit $(1, 2)$-OT if s_0 and s_1 are single bits.

On the other hand, suppose that Alice wants to send a mail to Bob. However, the mail system is so bad that Bob receives the mail with prob-

ability 1/2. Notice that Alice does not know if Bob received or not. A two-party protocol which realizes the above situation is called Rabin's OT.

It is known that a string $(1,2)$-OT, a bit $(1,2)$-OT and Rabin's OT are all equivalent. That is, there is a reduction between any two of them. Brassard et al. showed reductions of string $(1,2)$-OT to bit $(1,2)$-OT [2, 1]. Crépeau showed a reduction of 1-bit $(1,2)$-OT to Rabin's OT [4].

However, no direct reduction is known from string $(1,2)$-OT to Rabin's OT. Hence this reduction must be two steps. The first step is a construction of a bit $(1,2)$-OT from Rabin's OT, and the second step is a construction of a string $(1,2)$-OT from the bit $(1,2)$-OT.

In this paper, we show a direct reduction of string $(1,2)$-OT to Rabin's OT by using a deterministic randomness extractor. Our reduction is much more efficient than the previous two-step reduction. To construct L-bit $(1,2)$-OT, the former invokes Rabin's OT almost $2L$ times while the latter invokes it more than $21sL$ times, where s is a security parameter.

Rabin's OT is equivalent to an erasure channel. Hence our result implies that we can construct a string $(1,2)$-OT efficiently from an erasure channel.

(Related work) Independently of our work, Imai, Morozov and Nascimento showed another direct reduction of string $(1,2)$-OT to Rabin's OT which uses privacy amplificaiton technique [8]. In their reduciton, however, Alice has to send a random matrix to Bob at the last step which we do not require. Also, roughly speaking, the number of invocations of Rabin's OT is two times more than our reduction.

2 Preliminaries

2.1 $(1,2)$-Oblivious Transfer

In L-bit $(1,2)$-OT, Alice has two secret strings $s_0, s_1 \in \{0,1\}^L$ and Bob has a secret bit c. Then the following three conditions must be satisfied.

- At the end of the protocol, Bob receives s_c. This condition is called *completeness*.
- But Bob learns no information other than s_c. This condition is called *sender's privacy*.

- On the other hand, Alice has no information on c. This condition is called *receiver's privacy.*

More formally, we define sender's privacy as follows. For two random variables P and Q, we say that P and Q are ϵ-close if

$$|P - Q| = \frac{1}{2} \sum_{\alpha} |\Pr(P = \alpha) - \Pr(Q = \alpha)| \leq \epsilon.$$

For $i = 0, 1$, let S_i denote the random variable induced by $s_i \in \{0,1\}^L$. 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*. Let $S_i(view)$ be the random variable induced by s_i conditioned on $View = view$.

We assume that S_0 and S_1 are independent of each other.

Definition 2.1 *We say that L-bit $(1,2)$-OT satisfies (ϵ, δ)-statistical sender's privacy if for any (cheating) receiver Bob, either $S_0(view)$ is ϵ-close to S_0 with probability more than $1-\delta$, or $S_1(view)$ is ϵ-close to S_1 with probability more than $1 - \delta$, where the probability is taken over view. That is,*

$$\Pr_{view}(|S_i(view) - S_i| < \epsilon) > 1 - \delta.$$

We say that L-bit $(1,2)$-OT satisfies perfect sender's privacy if it satisfies $(0,0)$-statistical sender's privacy.

2.2 Rabin's Oblivious Transfer

In Rabin's OT, Alice has a secret bit b. At the end of the protocol, Bob receives b with probability $1/2$. On the other hand, Alice does not know if Bob received b or not. (Rabin's OT can be viewed as an erasure channel.)

2.3 Reduction of Crépeau

Crépeau showed a reduction of 1-bit $(1,2)$-OT to Rabin's OT [4]. In his reduction, Rabin's OT must be invoked at least $64s/3 > 21s$ times, where s is a security parameter such that

- Completeness: $\Pr(\text{Honest Bob receives } s_c) > 1 - 2^{-s}$, and

- $(0, 2^{-s})$-statistical sender's privacy is satisfied.

However, no direct reduction of *string* $(1,2)$-OT to Rabin's OT is known.

3 Deterministic Extractor

An (n,k)-bit-fixing source is a distribution X on $\{0,1\}^n$ on which $n-k$ bits are fixed and the remaining k bits are uniform and independent each other. A deterministic bit-fixing source extractor is a function $E : \{0,1\}^n \to \{0,1\}^L$ which on input an arbitrary (n,k)-bit-fixing source, outputs L bits that are statistically-close to uniform.

Definition 3.1 *(bit-fixing source on S). A distribution $X = (X_{i_1}, X_{i_2}, \cdots, X_{i_n})$ over $\{0,1\}^n$ is a bit-fixing source on $S = \{i_1, \cdots, i_k\} \subseteq \{1, \cdots, n\}$ if the joint distribution of $X_{i_1}, X_{i_2}, \cdots, X_{i_k}$ is uniformly distributed over $\{0,1\}^k$ and for every $i \notin S$, X_i is a fixed constant.*

Definition 3.2 *((n,k)-bit-fixing source). A distribution X over $\{0,1\}^n$ is an (n,k)-bit-fixing source if there exists a subset $S = \{i_1, \cdots, i_k\} \subseteq \{1, \cdots, n\}$ such that X is a bit-fixing source on S.*

Definition 3.3 *(deterministic extractor). A function $E : \{0,1\}^n \to \{0,1\}^L$ is a deterministic (k,ϵ)-bit-fixing source extractor if for every (n,k)-bit-fixing source X, the distribution $E(X)$ (obtained by sampling x from X and computing $E(x)$) is ϵ-close to the uniform distribution on L bit strings.*

Kurosawa, Johansson and Stinson showed the first deterministic extractor under the name of almost $(n-k)$-resilient functions [10]. Canetti, Dodis, Halevi, Kushilevitz and Sahai showed a probabilistic construction of deterministic extractors [3]. Kamp and Zuckerman [9] and then Gabizon, Raz and Shaltiel [6] showed an explicit construction of deterministic extractors. The deterministic extractor of [6] extracts $(1-o(1))k$ bits whenever $k > (\log n)^c$ for some universal constant $c > 0$. For $k \gg \sqrt{n}$, the extracted bits have statistical distance $2^{-n^{\Omega(1)}}$ from uniform, and for $k \leq \sqrt{n}$, the extracted bits have statistical distance $k^{-\Omega(1)}$ from uniform. For $k \gg \sqrt{n}$, their construction is described as follows.

Proposition 3.1 *For every constant $0 < \gamma < 1/2$, there exists an integer n' (depending on γ) such that: for any $n > n'$ and any k, there is an explicit deterministic (k, ϵ)-bit-fixing source extractor $E : \{0,1\}^n \to \{0,1\}^L$, where $L = k - n^{1/2+\gamma}$ and $\epsilon = 2^{-\Omega(n^\gamma)}$.*

Consider $k = n^{1/2+\alpha}$ for some constant $0 < \alpha < 1/2$. We can choose any $\gamma < \alpha$ and extract $L = n^{1/2+\alpha} - n^{1/2+\gamma}$ bits.

4 Direct Reduction of *String* $(1,2)$-OT to Rabin's OT

No direct reduction of *string* $(1,2)$-OT to Rabin's OT is known. In this section, we show a direct and efficient reduction of *string* $(1,2)$-OT to Rabin's OT.

4.1 Proposed Reduction

We show how to realize *string* $(1,2)$-OT from p-OT directly and efficiently, where p-OT is a generalization of Rabin's OT. In p-OT, Alice has a secret bit b. At the end of the execution of the protocol, Bob receives b with probability p. On the other hand, Alice does not know if Bob received b or not. Rabin's OT is a special case such that $p = 1/2$.

Alice and Bob agree on a positive integer n and $0 < \delta < \sqrt{2}p/3$. Let $N = n(p - \delta/\sqrt{2})$ and $k = n(p - 3\delta/\sqrt{2})/2$. Suppose that there exists a deterministic (k, ϵ)-bit-fixing source extractor $E : \{0,1\}^N \to \{0,1\}^L$.

Then our L-bit $(1,2)$-OT is described as follows.

1. Alice chooses $x_1, \cdots, x_n \in \{0,1\}$ randomly.
2. For $i = 1, \cdots, n$, Alice and Bob execute p-OT on x_i.
3. Bob chooses $U_0, U_1 \subseteq \{1, \cdots, n\}$ such that $|U_0| = |U_1| = N$, $U_0 \cap U_1 = \emptyset$ and he knows x_i for each $i \in U_c$. He then sends (U_0, U_1) to Alice.
4. Suppose that

$$U_0 = \{i_1, \cdots, i_N\}, \quad U_1 = \{j_1, \cdots, j_N\}.$$

Define

$$R_0 = (x_{i_1}, \cdots, x_{i_N}), \quad R_1 = (x_{j_1}, \cdots, x_{j_N}).$$

Alice sends $y_0 = E(R_0) \oplus s_0$ and $y_1 = E(R_1) \oplus s_1$ to Bob.

5. Bob computes $s_c = E(R_c) \oplus y_c$.

4.2 Security

Now we will prove that the above protocol implements L-bit $(1,2)$-OT correctly with probability more than $1 - 2e^{-n\delta^2}$. More formally, it satisfies

- Completeness. Pr(Honest Bob receives s_c) $> 1 - 2e^{-n\delta^2}$, and
- $(\epsilon, 2e^{-n\delta^2})$-statistical sender's privacy.

Proposition 4.1 *(Hoeffding) [7] Let $x_1, x_2, \cdots, x_n$ be independent Bernoulli variables. If $\Pr(x_i = 1) = p$ for $1 \le i \le n$, then for all $0 \le \gamma \le 1$, we have*

$$\Pr\left(\left|\frac{\sum_{i=1}^{n} x_i}{n} - p\right| \ge \gamma\right) \le 2e^{-2n\gamma^2}.$$

Let

$$X = \{x_i \mid \text{Bob received } x_i \text{ at step 2}\}.$$

Then by applying the Hoeffding Bound,

$$n\left(p - \frac{\delta}{\sqrt{2}}\right) \le |X| \le n\left(p + \frac{\delta}{\sqrt{2}}\right)$$

with probability more than $1 - 2e^{-n\delta^2}$. Therefore,

1. There exists $U_c \subseteq \{1, \cdots, n\}$ such that $|U_c| = n(p - \delta/\sqrt{2})$ and he knows x_i for each $i \in U_c$. Hence honest Bob can receive s_c with probability more than $1 - 2e^{-n\delta^2}$.
2. Bob knows at most $M = n(p + \delta/\sqrt{2})$ bits among $x_1, \cdots, x_n$ with probability more than $1 - 2e^{-n\delta^2}$. On the other hand, $|U_0| + |U_1| = 2n(p - \delta/\sqrt{2})$. Hence Bob has no information on the rest of

$$|U_0| + |U_1| - M = 2n\left(p - \frac{\delta}{\sqrt{2}}\right) - n\left(p + \frac{\delta}{\sqrt{2}}\right) = n\left(p - \frac{3\delta}{\sqrt{2}}\right) = 2k$$

bits. Hence either R_0 or R_1 is a (N, k)-bit-fixing source for Bob. Therefore he has (almost) no information on either s_0 or s_1 because E is a deterministic (k, ϵ)-bit-fixing source extractor and $y_i = E(R_i) \oplus s_i$ for $i = 0, 1$. It means that ϵ-statistical sender's privacy is satisfied.

4.3 Comparison

Rabin's OT is a special case such that $p = 1/2$. Suppose that $p = 1/2$ in our protocol. Then we obtain L-bit $(1, 2)$-OT which satisfies $(\epsilon, 2e^{-n\delta^2})$-statistical sender's privacy for any $0 < \delta < \sqrt{2}/6$ if there exists a deterministic (k, ϵ)-bit-fixing source extractor $E : \{0,1\}^N \to \{0,1\}^L$ with $N = n(0.5 - \delta/\sqrt{2})$ and $k = n(0.5 - 3\delta/\sqrt{2})$.

If we use a deterministic extractor of Gabizon, Raz and Shaltiel [6], then we have

$$L = (1 - o(1))k = (1 - o(1))n(\frac{1}{2} - \frac{3}{\sqrt{3}}\delta) \approx n/2.$$

It means that we invoke Rabin's OT approximately $n \approx 2L$ times to construct L-bit $(1, 2)$-OT.

On the other hand, the previous reduction of L-bit $(1, 2)$-OT to Rabin's OT requires 2-step reduction. In the first step, we can construct a 1-bit $(1, 2)$-OT from Rabin's OT by using the reduction of Crépeau [4]. In the second step, we can construct an L-bit $(1, 2)$-OT from the 1-bit $(1, 2)$-OT. The first step requires at least $21s$ invocations of Rabin's OT as shown in Sec.2.3, where s is the security parameter. Brassard and Crépeau showed the second step which runs $n = 2L + s'$ instances of 1-bit $(1, 2)$-OT, where s' is a security parameter [1]. Hence the previous reduction requires at least $21sL$ invocations of Rabin's OT.

See the following table for comparison. From this table, we see that our reduction is much more efficient than the previous reduction.

	the number of invocations of Rabin's OT to construct L-bit $(1, 2)$-OT
Previous	at least $21sL$
This paper	almost $2L$

5 Discussion

5.1 Technical Difference From Crépeau's Reduction

Technical differences between our reduction and Crépeau's reduction [4] are as follows. The main difference is that we use a deterministic extractor $E : \{0,1\}^N \to \{0,1\}^L$ while Crépeau used $E : \{0,1\}^N \to \{0,1\}$ such that

$$E(x_1, \cdots, x_N) = x_1 \oplus \cdots \oplus x_N.$$

Using deterministic extractors allows us to construct a direct and efficient reduction of L-bit $(1,2)$-OT to Rabin's OT.

Another difference is that he used Bernshtein's Law of large numbers while we use Hoeffding bound which is more tight.

5.2 Informal Lower Bound

It is very hard to derive a lower bound on the number t of invocations of Rabin's OT to construct L-bit $(1,2)$-OT. Hence we consider an ideal model such that if t instances of Rabin's OT are executed, then Bob receives the bit b that Alice sent in $\lceil t/2 \rceil$ instances, and nothing in the rest of the instances.

In this section, we derive a lower bound on t in this ideal model, and show that our reduction almost satisfies the equality. For each i, we assume that

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

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

Theorem 5.1 *In the ideal model, suppose that there exists a protocol which realizes L-bit $(1,2)$-OT from t instances of Rabin's OT. Also suppose that perfect sender's privacy is satisfied. Then we have*

$$t \geq 2L.$$

(Proof) Consider an L-bit $(1,2)$-OT protocol which invokes Rabin's OT t times. Suppose that Alice sent a bit x_i in the ith invocation of Rabin's OT for $i = 1, \cdots, t$. Without loss of generality, suppose that Bob received $X = (x_1, \cdots, x_u)$ in the first $u = \lceil t/2 \rceil$ invocations of Rabin's OT, and nothing for $i = u+1, \cdots, t$.

Fix the view of Bob arbitrarily. From the perfect sender's privacy, Bob has no information on either s_0 or s_1. Without loss of generality, suppose that Bob has no information on s_0. Then for any L-bit string $\alpha \in \{0,1\}^L$,

$$\Pr(S_0(view) = \alpha) = \Pr(S_0 = \alpha) > 0.$$

On the other hand, if Bob knows the erased $(x_{u+1}, \cdots, x_t)$, then he must be able to compute s_0. This can be seen as follows. Suppose that Bob is honest and he has $c = 0$. Then he receives some part of X, and can compute s_0. Also, Alice has no information on c. Therefore, if Bob knows the whole X, then he can compute s_0.

This means that there exists an onto mapping F from $\{0,1\}^{t-u}$ to $\{0,1\}^L$. It implies that $t - u \geq L$. Then

$$L \leq t - u = t - \lceil t/2 \rceil = \lfloor t/2 \rfloor \leq t/2.$$

Hence $t \geq 2L$.

Q.E.D.

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] R. Canetti, Y. Dodis, S. Halevi, E. Kushilevitz and A. Sahai: Exposure-resilient functions and all-or-nothing transforms. In, B. Preneel (ed.), *Advances in Cryptology — EUROCRYPT 2000*, Lecture Notes in Computer Science 1807, Springer, pp.453–469 (2000)

[4] C. Crépeau: Equivalence between two flavours of oblivious transfers. In, C. Pomerance (ed.), *Advances in Cryptology — CRYPTO 1987*, Lecture Notes in Computer Science 293, Springer, pp.350–354 (1988)

[5] C. Crépeau: Efficient cryptographic protocols based on noisy channels. In, W. Fumy (ed.), *Advances in Cryptology — EUROCRYPT 1997*, Lecture Notes in Computer Science 1233, Springer, pp.306–317 (1997)

[6] A. Gabizon, R. Raz and R. Shaltiel: Deterministic extractors for bit-fixing sources by obtaining an independent seed. *Proc. 45th IEEE Symposium on Foundations of Computer Science*, pp.394–403 (2004)

[7] W. Hoeffding: Probability inequalities for sum of bounded random variables. Journal of the American Statistical Association, Vol.58, pp.13–30 (1963)

[8] H. Imai, K. Morozov, A. Nascimento: On the oblivious transfer capacity of the erasure channel. *Proc. 2006 IEEE Symposium on Information Theory*, pp.1428–1431 (2006)

[9] J. Kamp and D. Zuckerman: Deterministic extractors for bit-fixing sources and exposure-resilient cryptography. *Proc. 44th IEEE Symposium on Foundations of Computer Science*, pp.92–101 (2003)

[10] K. Kurosawa, T. Johansson, D. Stinson: Almost k-Wise Independent Sample Spaces and Their Cryptologic Applications. J. Cryptology 14(4): 231-253 (2001)