IEICE TRANS. FUNDAMENTALS, VOL.E87–A, NO.1 JANUARY 2004

LETTER

An Approximate Scheme of Oblivious Transfer with Probabilistic Receipt

Shoichi HIROSE[†a)] ***and*** **Susumu YOSHIDA**[†], ***Members***

SUMMARY An efficient scheme is proposed which achieves the oblivious transfer with probabilistic receipt, α-OT, approximately for $0 < \alpha < 1$. The proposed scheme approximates α-OT with 2^{-i}-OT for $i = 1, 2, \ldots, k$. It implements γ-OT for some γ such that $(\alpha - 2^{-k})/(1 - 2^{-k}) < \gamma \leq \alpha$ with $\lfloor -\log(1-\alpha) \rfloor$ invocations of 2^{-1}-OT and at most 2 invocations of 2^{-i}-OT for each $i = 2, \ldots, k$. These invocations can be executed in parallel.
key words: *oblivious transfer, approximation*

1. Introduction

The notion of oblivious transfer (OT) was first introduced by Halpern and Rabin [4]. Oblivious transfer is a protocol between two parties; a sender Alice and a receiver Bob. There are two types of oblivious transfer. The one is usually called α-OT. By α-OT, Alice sends a message to Bob, and he receives it with probability α. Furthermore, she cannot know whether he received the message successfully or not. The other one is usually called k-out-of-n-OT. By k-out-of-n-OT, Alice sends n messages to Bob and he receives only k of them. Furthermore, she cannot know which k messages he received. The two types of oblivious transfer are equivalent [1], [2]. Many papers have been published on k-out-of-n-OT, while α-OT has not been studied very much.

(1) Our Result.

In this manuscript, a simple and efficient scheme is proposed which achieves α-OT approximately for $0 < \alpha < 1$. The proposed scheme approximates α-OT for $0 < \alpha < 1$ with 2^{-i}-OT for $i = 1, 2, \ldots, k$. It implements γ-OT for some γ such that $(\alpha - 2^{-k})/(1 - 2^{-k}) < \gamma \leq \alpha$ with $\lfloor -\log(1-\alpha) \rfloor$ invocations of 2^{-1}-OT and at most 2 invocations of 2^{-i}-OT for each $i = 2, \ldots, k$. This approximation does not increase the number of moves because all of the invocations can be executed in parallel.

(2) Related Work.

Rabin presented a scheme of 1/2-OT based on factoring [4]. Kuwakado and Tanaka [3] showed a scheme which achieves α-OT approximately with 1/2-OT. They also proposed 1/2-OT and $1/n$-OT schemes based on a public key encryption scheme. Their approximate α-OT scheme is based on the binomial distribution and the approximation is guaranteed by the central limit theorem in Bernoulli trials. Thus, in general, their scheme is not so efficient as our scheme.

(3) Organization of the Manuscript.

In Sect. 2, the definition of α-OT and that of its security are provided. The proposed scheme of approximate α-OT is presented in Sect. 3. Section 4 concludes this manuscript.

2. Preliminaries

A function δ from the set of non-negative integers to the set of non-negative reals is *negligible* if, for any constant $d > 0$ and for all large n, $\delta(n) < n^{-d}$.

2.1 α-OT

α-OT is a two-party message transmission protocol. Let us call the sender Alice and the receiver Bob. By α-OT, Alice sends a message to Bob, and Bob receives it with probability α. Furthermore, Alice cannot know whether Bob received the message successfully or not.

A secure scheme of α-OT is defined to be a scheme which satisfies the three properties: correctness, sender security, and receiver security. Let ℓ be the security parameter. Correctness means that, if both Alice and Bob are honest, then Bob succeeds in receiving the message from Alice with probability α. Sender security means that the probability that any malicious Bob succeeds in receiving the message from Alice is at most $\alpha + \varepsilon(\ell)$, where ε is a negligible function. Receiver security means that the probability that any honest but curious Alice succeeds in guessing whether Bob receives the message or not is at most $\max\{\alpha, 1-\alpha\} + \varepsilon(\ell)$, where ε is a negligible function. For receiver security, we only consider honest but curious Alice because any malicious Alice is able to know that Bob fails to receive the message only if she does not send the message honestly to him.

3. Approximate α-OT for $0 < \alpha < 1$

In this section, it is shown that, for $0 < \alpha < 1$, α-

Manuscript received February 28, 2003.
Final manuscript received September 30, 2003.
[†]The authors are with the Graduate School of Informatics, Kyoto University, Kyoto-shi, 606–8501 Japan.
a) E-mail: hirose@i.kyoto-u.ac.jp

OT can be approximated efficiently with 2^{-i}-OT for $i = 1, 2, \ldots, k$.

First, a simple procedure `approx` is presented which gives an approximation of β such that $0 < \beta < 1$. With input β and a positive integer k, `approx` outputs integers $c_1, c_2, \ldots, c_k$ such that $\prod_{i=1}^{k}(1-2^{-i})^{c_i}$ is a good approximation of β. In the description below, $\leftarrow$ represents substitution.

The procedure `approx`(β, k)

0. $j \leftarrow 1$; $\beta_1 \leftarrow \beta$.
1. while $j \leq k$, do the following steps;
   a. $c_j \leftarrow c$, where $(1-2^{-j})^{c+1} < \beta_j \leq (1-2^{-j})^c$;
   b. $\beta_{j+1} \leftarrow \beta_j/(1-2^{-j})^{c_j}$;
   c. $j \leftarrow j+1$.
2. output $c_1, c_2, \ldots, c_k$.

The following lemma shows that the procedure `approx` gives a good approximation for $0 < \beta < 1$. This lemma shows that rather small k, for example, $k \leq 20$, would be sufficient, because it gives an approximation up to about 10^{-6}.

Lemma 1: Let $c_1, \ldots, c_k$ be the output of `approx` for input β and k, and let $\beta^* = \prod_{i=1}^{k}(1-2^{-i})^{c_i}$. Then, $1 - 2^{-k} < \beta/\beta^* \leq 1$.

(Proof) From the procedure `approx`, $\beta/\beta^* = \beta_{k+1}$, and $1 - 2^{-k} < \beta_{k+1} = \beta_k/(1-2^{-k})^{c_k} \leq 1$ since $(1-2^{-k})^{c_k+1} < \beta_k \leq (1-2^{-k})^{c_k}$. □

The following lemma gives upper bounds on $c_1, \ldots, c_k$ obtained by the procedure `approx`.

Lemma 2: $c_1 \leq \lfloor -\log\beta \rfloor$ and $c_i \in \{0, 1, 2\}$ for $i = 2, \ldots, k$.

(Proof) From the step 1 of `approx`, $(1/2)^{c_1+1} < \beta \leq (1/2)^{c_1}$. Thus, $c_1 \leq \lfloor -\log\beta \rfloor$.

For $j \geq 2$,

$$\begin{aligned}(1-2^{-j})^3 &= 1 - 3\cdot 2^{-j} + 3\cdot 2^{-2j} - 2^{-3j} \\ &< 1 - 2^{-(j-1)} - 2^{-2j}(2^j - 3) \\ &< 1 - 2^{-(j-1)}.\end{aligned}$$

On the other hand, $\beta_j > 1 - 2^{-(j-1)}$. Thus, $c_j \leq 2$ for $j \geq 2$. □

The approximation of α-OT can be achieved with 2^{-i}-OT's for $1 \leq i \leq k$ in the following way. Suppose that the message sent to Bob by Alice is m.

Let $c_1, c_2, \ldots, c_k$ be the output of `approx` with input $\beta = 1 - \alpha$ and k. Then, $1 - \alpha \approx \prod_{i=1}^{k}(1-2^{-i})^{c_i}$.

Alice transfers the message m to Bob by c_i invocations of 2^{-i}-OT for $i = 1, 2, \ldots, k$. Bob succeeds in receiving m if and only if he succeeds in at least one of c_i invocations of 2^{-i}-OT for $i = 1, 2, \ldots, k$. Thus, the probability that Bob successfully receives m is $1 - \prod_{i=1}^{k}(1-2^{-i})^{c_i} \approx \alpha$.

It is obvious that the above scheme is secure if the underlying 2^{-i}-OT schemes are secure.

Theorem 1: For every $0 < \alpha < 1$, there exists some γ such that $(\alpha - 2^{-k})/(1-2^{-k}) < \gamma \leq \alpha$ and γ-OT can be achieved by $\lfloor -\log(1-\alpha) \rfloor$ invocations of 2^{-1}-OT and at most 2 invocations of 2^{-i}-OT for each $i = 2, \ldots, k$.

(Proof) Let $c_1, c_2, \ldots, c_k$ be the output of `approx` with input $1-\alpha, k$, and let $\gamma = 1 - \prod_{i=1}^{k}(1-2^{-i})^{c_i}$. Then, from Lemma 1, since $1 - 2^{-k} < (1-\alpha)/(1-\gamma) \leq 1$, $(\alpha - 2^{-k})/(1-2^{-k}) < \gamma \leq \alpha$. Furthermore, from Lemma 2, $c_1 \leq \lfloor -\log(1-\alpha) \rfloor$ and $c_i \leq 2$ for each $i = 2, \ldots, k$. □

2^{-i}-OT can be constructed efficiently using the 1-out-of-n-OT scheme in [5], which is based on discrete logarithms.

2^{-i}-OT can also be achieved simply by i invocations of 1/2-OT. To send m, Alice first randomly selects $m_1, m_2, \ldots, m_i$ such that $m = m_1 \oplus m_2 \oplus \cdots \oplus m_i$. Then, Alice sends each m_i to Bob with 1/2-OT. Bob receives m if and only if he receives all of $m_1, m_2, \ldots, m_i$ successfully. Thus, the following corollary is lead from the above theorem.

Corollary 1: For every $0 < \alpha < 1$, there exists some γ such that $(\alpha - 2^{-k})/(1-2^{-k}) < \gamma \leq \alpha$ and γ-OT can be achieved by $\lfloor -\log(1-\alpha) \rfloor + k(k+1) - 2$ invocations of 2^{-1}-OT. □

4. Conclusion

In this manuscript, we have proposed an efficient scheme which achieves α-OT approximately for $0 < \alpha < 1$ with 2^{-i}-OT's for $i = 1, 2, \ldots, k$.

References

[1] G. Brassard, C. Crépeau, and J.-M. Robert, "Information theoretic reductions among disclosure problems," Proc. 27th IEEE Symposium on Foundations of Computer Science, pp.168–173, 1986.
[2] C. Crépeau, "Equivalence between two flavours of oblivious transfers," Proc. CRYPTO'87, pp.350–354, Lecture Notes in Computer Science 293, 1988.
[3] H. Kuwakado and H. Tanaka, "Rabin-type oblivious transfer based on public key cryptosystems," Proc. 2000 Symposium on Cryptography and Information Security, SCIS2000-B52, 2000.
[4] M.O. Rabin, "How to exchange secrets by oblivious transfer," Technical Memo TR-81, Aiken Computation Laboratory, Harvard University, 1981.
[5] W.-G. Tzeng, "Efficient 1-out-n oblivious transfer schemes," Proc. Public Key Cryptography 2002, pp.159–171, Lecture Notes in Computer Science 2274, 2002.