1Y-2

弱い仮定に基づく紛失通信

山田 章央* 安永 憲司* 田中 圭介*

1 Background

Oblivious transfer (OT) is one of the fundamental cryptographic primitives. OT was first introduced by Rabin [15] and some variations have been studied in several works. OT can be used to implement a wide variety of protocols [11][7]. Particularly, secure multi party computation can be based on the security of OT. Nevertheless, constructions of OT protocol need unproven computational assumptions: the difficulty of factoring large numbers, computing discrete logarithms, the existence of enhanced trapdoor permutations [15][14][6]. These problems may be solved efficiently, and strong assumptions may be turn out to be false. Thus, constructions of OT protocol from "weak" assumptions is important.

Minimal assumption commonly used in cryptography is the existence of one-way functions [9]. However OT can not be reduced to the existence of one-way permutations with black-box construction [10]. It is unlikely that a provable construction of OT based on one-way functions is found. Therefore we study a weaker variant of OT from one-way functions.

We study the case in which there exists a quadratic gap between the computational resources of the honest party and the adversary. In the standard form of OT, computational resource's gap must be super-polynomial. Considering such a weaker form of OT is general and reasonable, because it is the natural setting that a ratio between the computational resources of an adversary and that of honest parties grows linearly.

Other cryptographic primitive which has quadratic security also has been studied in [2]. A protocol of key exchange, that is also one of fundamental cryptographic primitives, with quadratic security based on strong one-way functions was suggested in [2]. It is shown that key exchange protocol in the random oracle model with quadratic security is optimal [1].

In this paper we consider the 1-out-of-2 variant of OT proposed by Even, Goldreich, and Lempel [6], which is shown to be equivalent to Rabin's OT by Crépeau [4] and more useful. The 1-out-of-2 OT is a protocol between two players: a sender (Alice) and a receiver (Bob). Alice has two secrets s_0 and s_1, Bob has a choice bit c. Bob wishes to receive one of the secrets which he chooses (i.e., s_c) without Alice learning c, while Alice wants to ensure that Bob receives only one of the two secrets.

Constructions of weak OT which has quadratic security relates strongly with OT in Maurer's bounded storage model (BSM) [12][5]. In the BSM, it is assumed that the adversary has bounded space (memory size) rather than running time. In a typical setting of the BSM a large random string $\mathcal{R}$ of length N is initially transmitted to the honest parties and the adversary, both of the honest parties and the adversary can store only a limited portion of $\mathcal{R}$. It is shown that there exists a OT protocol in the BSM which can have unconditional security [3]. It is shown that a protocol in the BSM with unconditional security can be transformed into a computational secure protocol based on strong one-way functions [2].

In [16] it is proved that the paradigm of transforming unconditionally secure protocols in Maurer's bounded storage model into computational secure protocols based on random oracles can be applied to OT protocols and constructed weak OT protocols, that is with quadratic security, from random oracles and proved that random oracle can be repaced into strong one-way permutations.

2 Our contribution

We present weak oblivious transfer protocol from strong one-way functions. Our OT protocol can send multi-bit secret bounded $O(\log \log k)$, where k is security parameter. We prove that our protocol has quadratic security against dishonest adversaries. Our protocol is based on Merkle's puzzles [13], the OT protocol in the BSM [5], standard error-correct coding techniques, and the paradigm of transforming unconditionally secure protocols in Maurer's bounded storage model into computational secure protocol based on one-way functions.

Similar transforming was presented for the key exchange protocol [2]. However in OT protocol, Alice or Bob may be adversary. In addition adversary can be dishonest rather than semi-honest. dishonest adversary mcan run protocol ignoring his input. Therefore we cannot directly use standard techniques which are used in key exchange protocol. The techniques which are combining several copies of the basic protocol can amplify correctness

*Department of Mathematical and Computing Sciences, Tokyo Institute of Technology. W8-55, 2-12-1 Ookayama, Meguro-ku, Tokyo, 152-8552, Japan. {yamada9, keisuke, yasunaga}@is.titech.ac.jp. This research was supported in part by NTT Information Sharing Platform Laboratories and JSPS Global COE program "Computationism as Foundation for the Sciences".

and security of protocol. We carefully use these techniques combining several copies and integrate error-correcting technique into our protocol. We can achieve our OT protocol correctness and security as well as key exchange protocol's [2].

The OT Protocol from Strong One-Way Functions

The protocol uses the following tools: a collection of restricted strong one-way functions, an interactive hashing protocol, a strong extractor, and an error-correct code.

In our OT protocol, Alice first randomly chooses secret strings s'_0, s'_1. these strings are independent of her input secrets s_0, s_1. Alice encodes secrets made by herself. Alice and Bob run the basic protocol several times. In the one basic protocol, Alice and Bob run setup stage several times. Bob's output of the j'th basic protocol is the j'th bit of encoded strings.

If Bob collects almost of all outputs of the basic protocols, then Bob can decode the strings to secret which Alice made and by using it, get Alice's input which Bob wants.

Theorem 2.1. *If there exists a $2^{n(1-\delta)}$ one-way functions for any $\delta < 1/2$, then there exists (d, ϵ)-secure oblivious transfer protocol for $d = 2-2\delta-2\tau$, $\epsilon = k^{-\tau}$ for any $\tau < 1-\delta$.*

3 Conclusion and Open Problems

We construct an OT protocol with quadratic security from strong one-way functions. We show that our OT protocol comes through with $(1 - negl(k))$ probability and achieves $1/poly(k)$ advantage.

We do not know the way of closing this advantage to $negl(k)$. However we believe that there exist cleverer OT protocols by carefully analyzing and bringing other techniques: other error-correcting codes, extractors, a dream version XOR lemma [8]. Thus These techniques may improve advantage and remains hardness.

In addition the possibility of replacing strong one-way function to standard one-way function remains open problem. In [1] it is shown that the key exchange protocol with quadratic security is optimal in random oracle model, therefore it may be able to prove that an OT protocol with quadratic security is optimal in random oracle model.

References

[1] B. Barak and Mahmoody-Ghidary M. Merkle puzzles are optimal − an O(n^2)-query attack on any key exchange from a random oracle. *Proceedings of* CRYPTO 2009, pages 374–390, 2009.

[2] E. Biham, Y.J. Goren, and Y. Ishai. Basing weak public-key cryptography on strong one-way functions. *Proceedings of* TCC 2008, pages 55–72, 2008.

[3] C. Cachin and U. Maurer. Unconditional security against memory-bounded adversaries. *Proceedings of* CRYPTO 1997, pages 292–306, 1997.

[4] C. Crépeaut. Equivalence between two flavours of oblivious transfers. *Proceedings of* CRYPTO 1987, pages 350–354, 1987.

[5] Y.Z. Ding, D. Harnik, A. Rosen, and R. Shaltiel. Constant-round oblivious transfer in the bounded storage model. *Proceedings of* TCC 2004, pages 446–472, 2004.

[6] S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. *Communications of the ACM*, pages 637–647, 1985.

[7] Y. Gertner, S. Kannan, and T. Malkin. The relationship between public key encryption and oblivious transfer. *Proceedings of* FCCS 2000, pages 325–335, 2000.

[8] O. Goldreich, N. Nisan, and A. Wigderson. On yao's xor lemma. *Technical Report TR95-50*, 1995.

[9] R. Impagliazzo and M. Ruby. One-way functions are essential for complexity-based cryptography. *Proceedings of* FOCS 1989, pages 230–235, 1989.

[10] R. Impagliazzo and S. Rudich. Limits on the provable consequences of one-way permutations. *Proceedings of* STOC 1989, pages 44–61, 1989.

[11] J. Kilian. Founding cryptography on oblivious transfer. *In 20th ACM Symposium on the Theory of Computing*, pages 20–31, 1988.

[12] U.M. Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *Journal of Cryptology*, pages 53–66, 1992.

[13] R.C. Merkle. Secure communications over insecure channels. *Communications of the ACM*, pages 294–299, 1978.

[14] M. Naor and B. Pinkas. Efficient oblivious transfer protocols. *Proceedings of* SODA 2001, pages 448–457, 2001.

[15] M. Rabin. How to exchange secrets by oblivious transfer. *Technical Report TR-81*, 1981.

[16] A. Yamada, K. Yasunaga, and K. Tanaka. Weak oblivious transfer from strong one-way permutations. *Proceedings of* SCIS 2010, 2010.