Efficient k-out-of-n Oblivious Transfer Schemes with Adaptive and Non-Adaptive Queries

Cheng-Kang Chu and Wen-Guey Tzeng
Department of Computer and Information Science
National Chiao Tung University
Hsinchu, Taiwan 30050
Email:{ckchu,tzeng}@cis.nctu.edu.tw

Abstract. In this paper we propose efficient two-round k-out-of-n oblivious transfer schemes, in which R sends $O(k)$ messages to S, and S sends $O(n)$ messages back to R. The computation cost of R and S is reasonable. The choices of R are unconditionally secure. For the basic scheme, the secrecy of unchosen messages is guaranteed if the Decisional Diffie-Hellman problem is hard. When $k = 1$, our basic scheme is as efficient as the most efficient 1-out-of-n oblivious transfer scheme. Our schemes have the nice property of *universal parameters*, that is each pair of R and S need neither hold any secret key nor perform any prior setup (initialization). The system parameters can be used by all senders and receivers without any trapdoor specification. Our k-out-of-n oblivious transfer schemes are the most efficient ones in terms of the communication cost, in both rounds and the number of messages.
Moreover, one of our schemes can be extended in a straightforward way to an *adaptive* k-out-of-n oblivious transfer scheme, which allows the receiver R to choose the messages one by one adaptively. In our adaptive-query scheme, S sends $O(n)$ messages to R in one round in the commitment phase. For each query of R, only $O(1)$ messages are exchanged and $O(1)$ operations are performed. In fact, the number k of queries need not be pre-fixed or known beforehand. This makes our scheme highly flexible.

Keywords: k-out-of-n Oblivious Transfer, Adaptive Oblivious Transfer

1 Introduction

Oblivious transfer (OT) is an important primitive used in many cryptographic protocols [GV87,Kil88]. An oblivious transfer protocol involves two parties, the sender S and the receiver R. S has some messages and R wants to obtain some of them via interaction with S. The security requirement is that S wants R to obtain the message of his choice only and R does not want S to know what he chooses. The original OT was proposed by Rabin [Rab81], in which S sends a message to R, and R gets the message with probability 0.5. On the other hand, S does not know whether R gets the message or not. Even, et al. [EGL85] suggested a more general scheme, called 1-out-of-2 OT (OT_2^1). In this scheme, S has two messages m_1 and m_2, and would like R to obtain exactly one of them. In addition,

S remains oblivious to R's choice. Brassard, et al. [BCR86] further extended OT_2^1 to 1-out-of-n OT (OT_n^1) for the case of n messages.

Oblivious transfer has been studied extensively and in many flavors. Most of them consider the case that R chooses one message. In this paper we are concerned about the case that R chooses many messages at the same time. A k-out-of-n OT (OT_n^k) scheme is an OT scheme in which R chooses k messages at the same time, where $k < n$. A straightforward solution for OT_n^k is to run OT_n^1 k times independently. However, this needs k times the cost of OT_n^1. The communication cost is two-round, $O(k)$ messages from R to S, and $O(kn)$ messages from S to R even using the most efficient OT_n^1 schemes [NP01,Tze02].

Oblivious transfer with adaptive queries (Adpt-OT) allows R to query the messages one by one adaptively [NP99a]. For the setting, S first commits the messages to R in the commitment phase. Then, in the transfer phase, R makes queries of the messages one by one. The cost is considered for the commitment and transfer phases, respectively. It seems that the adaptive case implies the non-adaptive case. But, the non-adaptive one converted from an adaptive one usually needs more rounds (combining the commitment and transfer phases), for example, the scheme in [OK04]. Since our scheme needs no trapdoors, there is no entailed cost due to conversion. Adaptive OT_n^k is natural and has many applications, such as oblivious search, oblivious database queries, private information retrieval, etc.

In this paper we propose efficient two-round OT_n^k schemes, in which R sends $O(k)$ messages to S, and S sends $O(n)$ messages back to R. The computation cost of R and S is reasonable. The choices of R are unconditionally secure. For the basic scheme, the secrecy of unchosen messages is guaranteed if the Decisional Diffie-Hellman (DDH) problem is hard. When $k = 1$, our scheme is as efficient as the one in [Tze02]. Our schemes have the nice property of universal parameters, that is, each pair of R and S need neither hold any secret key nor perform any prior setup (initialization). The system parameters can be used by all senders and receivers without any trapdoor specification. Our OT_n^k schemes are the most efficient one in terms of the communication cost, either in rounds or the number of messages.

Moreover, one of our schemes can be extended in a straightforward way to an Adpt-OT_n^k scheme. In our adaptive-query scheme, S sends $O(n)$ messages to R in one round in the commitment phase. For each query of R, only $O(1)$ messages are exchanged and $O(1)$ operations are performed. In fact, the number k of queries need not be fixed or known beforehand. This makes our scheme highly flexible.

1.1 Previous work and comparison

Rabin [Rab81] introduced the notion of OT and presented an implementation to obliviously transfer one-bit message, based on quadratic roots modulo a composite. Even, Goldreich and Lempel [EGL85] proposed an extension of bit-OT_2^1, in which m_1 and m_2 are only one-bit. Brassard, Crépeau and Robert [BCR86] proposed OT_n^1 soon after in the name "all-or-nothing disclosure of secrets" (ANDOS). After that, OT_n^1 has become an important research topic in cryptographic protocol design. Some OT_n^1 schemes are built by invoking basis OT_2^1 several times [BCR87,BCS96,NP99b], and the others are constructed directly from basic cryptographic techniques [SS90,NR94,Ste98,NP01,Tze02]. Some OT_n^1 schemes derived from computational private information retrieval (CPIR) have polylogarithmic communication cost [Lip04]. Nevertheless, the privacy of the receiver's choice is computationally secure. Besides, there are various oblivious transfer schemes developed in different models and applications, such as OT in the bounded storage model [CCM98,Din01], distributed OT [NP00,BDSS02], Quantum OT [BBCS91,CZ03], and so on. Lipmaa [Lip] provided a good collection of these works.

For OT_n^k, Bellare and Micali [BM89] proposed an OT_n^{n-1} scheme. Naor and Pinkas [NP99b] proposed a non-trivial OT_n^k scheme. The scheme invokes a basis OT_2^1 scheme $O(wk \log n)$ times, where $w > \log \delta / \log(k^4/\sqrt{n})$ and δ is the probability that R can obtain more than k messages. The scheme works only for $k \leq n^{1/4}$. After then, they also took notice of adaptive queries and provided some Adpt-OT_n^k schemes [NP99a]. In one scheme (the two-dimensional one), each query needs invoke the basis $\mathrm{OT}_{\sqrt{n}}^1$ scheme twice, in which each invocation of $\mathrm{OT}_{\sqrt{n}}^1$ needs $O(\sqrt{n})$ initialization work. In another scheme, each adaptive query of messages need invoke the basis OT_1^2 protocol $\log n$ times. Mu, Zhang, and Varadharajan [MZV02] presented some efficient OT_n^k schemes[1]. These schemes are designed from cryptographic functions directly. The most efficient one is a non-interactive one. To be compared fairly, the setup phase of establishing shared key pairs of a public-key cryptosystem should be included. Thus, the scheme is two-round and R and S send each other $\mathrm{O}(n)$ messages. However, the choices of R cannot be made adaptive since R's choices are sent to S first and the message commitments are dependent on the choices. Recently, Ogata and Kurosawa [OK04] proposed an efficient adaptive OT scheme based on the RSA cryptosystem. Each S needs a trapdoor (the RSA modulus) specific to him. The scheme is as efficient as our Adpt-OT_n^k scheme. But, if the adaptive OT scheme is converted to a non-adaptive one, it needs 3 rounds (In the first round, S sends the modulus N to R).

Ishai, Kilian, Nissim and Petrank [IKNP03] proposed some efficient protocols for extending a small number of OT's to a large number of OT's. Chen and Zhu [CZ03] provided an OT_n^k in the quantum computation model. We won't compare these schemes with ours since they are in different categories.

In Table 1 we summarize the comparison of our, Mu, Zheng, and Varadharajan's, and Naor and Pinkas's OT_n^k schemes. In Table 2 we summarize the comparison of our and Naor and Pinkas's Adpt-OT_n^k schemes.

[1] Yao, Bao, and Deng [YBD03] pointed out some security issues in [MZV02].

	Ours (this paper)	Mu, et al. [MZV02]	Naor, et al. [NP99b]
rounds	2	2	$O(wk \log n)$
messages ($R \to S$)	$O(k)$	$O(n)$	$O(wk \log n))$
messages ($S \to R$)	$O(n)$	$O(n)$	$O(n + wk \log n)$
universal parameters	Yes	Yes	No (need setup)
made to adaptiveness	Yes (OT_n^k-II)	No	Yes

Table 1. Comparison of OT_n^k schemes in communication cost.

		Ours (this paper)	2-dimensional one, Naor, et al. [NP99a]	OT_n^k, Ogata, et al.[OK04]
commitment phase	rounds	1	1	1
	messages	$O(n)$	$O(n)$	O(n)
transfer phase	rounds	2	3*	2
	messages	$O(1)$	$O(\sqrt{n})$**	O(1)

* Two invocations of $\mathrm{OT}^1_{\sqrt{n}}$ in parallel.

** Use the most round-efficient $\mathrm{OT}^1_{\sqrt{n}}$ scheme as the basis.

Table 2. Comparison of Adpt-OT_n^k schemes in communication cost.

2 Preliminaries

Involved parties. The involved parties of an OT scheme is the sender and receiver. Both are polynomial-time-bounded probabilistic Turing machines (PPTM). A party is semi-honest (or passive) if it does not deviate from the steps defined in the protocol, but tries to compute extra information from received messages. A party is malicious (or active) if it can deviate from the specified steps in any way in order to get extra information.

A malicious sender may cheat in order or content of his possessed messages. To prevent the cheat, we can require the sender to commit the messages in a bulletin board. When the sender sends the encrypted messages to the receiver during execution of an OT scheme, he need tag a zero-knowledge proof of showing equality of committed messages and encrypted messages. However, in most applications, the sender just follows the protocol faithfully. Therefore, we consider the semi-honest sender only and the semi-honest/malicious receiver.

Indistinguishability. Two probability ensembles $\{X_i\}$ and $\{Y_i\}$, indexed by i, are (computationally) indistinguishable if for any PPTM D, polynomial $p(n)$ and sufficiently large i, it holds that

$$|\Pr[D(X_i) = 1] - \Pr[D(Y_i) = 1]| \leq 1/p(i).$$

Correctness of a protocol. An OT scheme is correct if the receiver obtains the messages of his choices when the sender with the messages and the receiver with the choices follow the steps of the scheme.

Security model. Assume that S holds n messages $m_1, m_2, \ldots, m_n$ and R's k choices are $\sigma_1, \sigma_2, \ldots, \sigma_k$. Note that only semi-honest sender is considered. We say that two sets C and C' are different if there is x in C, but not in C', or vice versa. An OT_n^k scheme with security against a semi-honest receiver should meet following requirements:

1. Receiver's privacy - indistinguishability: for any two different sets of choices $C = \{\sigma_1, \sigma_2, \ldots, \sigma_k\}$ and $C' = \{\sigma'_1, \sigma'_2, \ldots, \sigma'_k\}$, the transcripts, corresponding to C and C', received by the sender are indistinguishable. If the received messages of S for C and C' are identically distributed, the choices of R are unconditionally secure.
2. Sender's security - indistinguishability: for any choice set $C = \{\sigma_1, \sigma_2, \ldots, \sigma_k\}$, the unchosen messages should be indistinguishable from the random ones.

An OT_n^k scheme with security against a malicious receiver should meet following requirements:

1. Receiver's privacy - indistinguishability: the same as the case of the semi-honest receiver.
2. Sender's security - compared with the Ideal model: in the Ideal model, the sender sends all messages and the receiver sends his choices to the trusted third party (TTP). TTP then sends the chosen messages to the receiver. This is the securest way to implement the OT_n^k scheme. The receiver R cannot obtain extra information from the sender S in the Ideal model. We say that the sender's security is achieved if for any receiver R in the real OT_n^k scheme, there is another PPTM R' (called simulator) in the Ideal model such that the outputs of R and R' are indistinguishable.

Computational model. Let G_q be a subgroup of Z_p^* with prime order q, and $p = 2q+1$ is also prime. Let g be a generator of G_q. We usually denote $g^x \bmod p$ as g^x, where $x \in Z_q$. Let $x \in_R X$ denote that x is chosen uniformly and independently from the set X.

Security assumptions. For our OT_n^k schemes against semi-honest and malicious receiver, we assume the hardness of Decisional Diffie-Hellman (DDH) problem and Chosen-Target Computational Diffie-Hellman (CT-CDH) problem, respectively.

Assumption 1 (Decisional Diffie-Hellman (DDH)) *Let $p = 2q + 1$ where p, q are two primes, and G_q be the subgroup of Z_p^* with order q. The following two distribution ensembles are computationally indistinguishable:*

- $Y_1 = \{(g, g^a, g^b, g^{ab})\}_{G_q}$*, where g is a generator of G_q, and $a, b \in_R Z_q$.*
- $Y_2 = \{(g, g^a, g^b, g^c)\}_{G_q}$*, where g is a generator of G_q, and $a, b, c \in_R Z_q$.*

For the scheme against malicious receiver, we use the assumption introduced by Boldyreva [Bol03], which is analogous to the chosen-target RSA inversion assumption defined by Bellare, et al. [BNPS01]

- System parameters: (g, h, G_q);
- S has messages: $m_1, m_2, \ldots, m_n$;
- R's choices: $\sigma_1, \sigma_2, \ldots, \sigma_k$;

1. R chooses two polynomials $f(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1} + x^k$ and $f'(x) = b_0 + b_1 x + \cdots + b_{k-1}x^{k-1} + x^k$ where $a_0, a_1, \ldots, a_{k-1} \in_R Z_q$ and $b_0 + b_1 x + \cdots + b_{k-1}x^{k-1} + x^k \equiv (x-\sigma_1)(x-\sigma_2)\cdots(x-\sigma_k) \bmod q$.
2. $R \longrightarrow S : A_0 = g^{a_0}h^{b_0}, A_1 = g^{a_1}h^{b_1}, \ldots, A_{k-1} = g^{a_{k-1}}h^{b_{k-1}}$.
3. S computes $c_i = (g^{k_i}, m_i B_i^{k_i})$ where $k_i \in_R Z_q^*$ and $B_i = g^{f(i)}h^{f'(i)} = A_0 A_1^i \cdots A_{k-1}^{i^{k-1}} (gh)^{i^k} \bmod p$, for $i = 1, 2, \ldots, n$.
4. $S \longrightarrow R$: $c_1, c_2, \ldots, c_n$.
5. Let $c_i = (U_i, V_i)$, R computes $m_{\sigma_i} = V_{\sigma_i}/U_{\sigma_i}^{f(\sigma_i)} \bmod p$ for each σ_i.

Fig. 1. OT_n^k-I: k-out-of-n OT against semi-honest receiver

Assumption 2 (Chosen-Target Computational Diffie-Hellman (CT-CDH)) *Let G_q be a group of prime order q, g be a generator of G_q, $x \in_R Z_q^*$. Let $H_1 : \{0,1\}^* \rightarrow G_q$ be a cryptographic hash function. The adversary A is given input (q, g, g^x, H_1) and two oracles: target oracle $T_G(\cdot)$ that returns a random element $w_i \in G_q$ at the i-th query and helper oracle $H_G(\cdot)$ that returns $(\cdot)^x$. Let q_T and q_H be the number of queries A made to the target oracle and helper oracle respectively. The probability that A outputs k pairs $((v_1, j_1), (v_2, j_2), \ldots, (v_k, j_k))$, where $v_i = (w_{j_i})^x$ for $i \in \{1, 2, \ldots, k\}$, $q_H < k \le q_T$, is negligible.*

3 k-out-of-n OT schemes

We first present a basic OT_n^k scheme for the semi-honest receiver in the standard model. Then, we modify the scheme to be secure against the malicious receiver in the random oracle model. Due to the random oracle model, the second scheme is more efficient in computation.

3.1 k-out-of-n OT against semi-honest receiver

The sender S has n secret messages $m_1, m_2, \ldots, m_n$. Without loss of generality, we assume that the message space is G_q, that is, all messages are in G_q. The semi-honest receiver R wants to get $m_{\sigma_1}, m_{\sigma_2}, \ldots, m_{\sigma_k}$. The protocol OT_n^k-I with security against the semi-honest receiver is depicted in Figure 1.

For system parameters, let g, h be two generators of G_q where $\log_g h$ is unknown to all, and G_q be the group with some descriptions. These parameters can be used repeatedly by all possible senders and receivers as long as the value $\log_g h$ is not revealed. Therefore, (g, h, G_q) are universal parameters.

The receiver R first constructs a k-degree polynomial $f'(x)$ such that $f'(i) = 0$ if and only if $i \in \{\sigma_1, \ldots, \sigma_k\}$. Then R chooses another random k-degree polynomial $f(x)$ to mask the chosen polynomial $f'(x)$. The masked choices $A_0, A_1, \ldots, A_{k-1}$ are sent to the sender S.

When S receives these queries, he first computes $B_i = g^{f(i)}h^{f'(i)}$ by computing $A_0 A_1^i \cdots A_{k-1}^{i^{k-1}} (gh)^{i^k} \bmod p$. Because of the random polynomial $f(x)$, S does not know which $f'(i)$ is equal to zero, for $i = 1, 2, \ldots, n$. Then S treats B_i as the public key and encrypts each message m_i by the ElGamal cryptosystem. The encrypted messages $c_1, c_2, \ldots, c_n$ are sent to R.

For each $c_i, i \in \{\sigma_1, \sigma_2, \ldots, \sigma_k\}$, since $B_i = g^{f(i)}h^{f'(i)} = g^{f(i)}h^0 = g^{f(i)}$, R can get these messages by the decryption of ElGamal cryptosystem with secret key $f(i)$. If $i \notin \{\sigma_1, \sigma_2, \ldots, \sigma_k\}$, since R can not compute $(g^{f(i)}h^{f'(i)})^{k_i}$ with the knowledge of g^{k_i} and $f(i), f'(i)$ only, the message m_i is unknown to R.

Correctness. Let $c_i = (U_i, V_i)$, we can check that the chosen messages m_{σ_i}, $i = 1, 2, \ldots, k$, are computed as

$$\begin{aligned} V_{\sigma_i}/U_{\sigma_i}^{f(\sigma_i)} &= m_{\sigma_i} \cdot (g^{f(\sigma_i)}h^{f'(\sigma_i)})^{k_{\sigma_i}}/g^{k_{\sigma_i}f(\sigma_i)} \\ &= m_{\sigma_i} \cdot (g^{f(\sigma_i)} \cdot 1)^{k_{\sigma_i}}/g^{k_{\sigma_i}f(\sigma_i)} \\ &= m_{\sigma_i}. \end{aligned}$$

Security analysis. We now prove the security of OT_n^k-I.

Theorem 1. *For scheme OT_n^k-I, R's choices are unconditionally secure.*

Proof. For every tuple $(b_0', b_1', \ldots, b_{k-1}')$ representing the choices $\sigma_1', \sigma_2', \ldots, \sigma_k'$, there is a tuple $(a_0', a_1', \ldots, a_{k-1}')$ that satisfies $A_i = g^{a_i'}h^{b_i'}$ for $i = 0, 1, \ldots, k-1$. Thus, the receiver R's choices are unconditionally secure.

□

Theorem 2. *Scheme OT_n^k-I meets the sender's security requirement. That is, by the DDH assumption, if R is semi-honest, he gets no information about messages m_i, $i \notin \{\sigma_1, \sigma_2, \ldots, \sigma_k\}$.*

Proof. We show that for all $i \notin \{\sigma_1, \sigma_2, \ldots, \sigma_k\}$, c_i's look random if the DDH assumption holds. First, we define the random variable for the unchosen messages

$$C = (g, h, (g^{k_{i_1}}, m_{i_1}(g^{f(i_1)}h^{f'(i_1)})^{k_{i_1}}), \ldots, (g^{k_{i_{n-k}}}, m_{i_{n-k}}(g^{f(i_{n-k})}h^{f'(i_{n-k})})^{k_{i_{n-k}}})),$$

where $k_{i_1}, k_{i_2}, \ldots, k_{i_{n-k}} \in_R Z_q^*$. Since the polynomial $f(x)$ and $f'(x)$ are chosen by the receiver, and $f'(i_1), \ldots, f'(i_{n-k}) \neq 0$, we can simplify C as

$$C' = (g, h, (g^{k_{i_1}}, h^{k_{i_1}}), \ldots, (g^{k_{i_{n-k}}}, h^{k_{i_{n-k}}}))$$

Since the indistinguishability is preserved under multiple samples, we just need to show that if the following two distributions

– $\tilde{C} = (g, h, g^r, h^r)$, where $h \neq 1, r \in_R Z_q^*$

– $\tilde{X} = (g, h, x_1, x_2)$, where $h \neq 1, x_1, x_2 \in_R G_q$

are distinguishable by a polynomial-time distinguisher $\mathcal{D}$, we can construct another polynomial-time machine $\mathcal{D}'$, which takes $\mathcal{D}$ as a sub-routine, to solve the DDH problem:

Machine $\mathcal{D}'$

Input: (g, u, v, w) (either from Y_1 or Y_2 in DDH)
Output: $\mathcal{D}(g, u, v, w)$

If $\mathcal{D}$ distinguishes $\tilde{C}$ and $\tilde{X}$ with non-negligible advantage ε (Should be $\epsilon(n,t)$, we omit the security parameter n and t here for simplicity, where t is the security parameter.), $\mathcal{D}'$ distinguishes Y_1, Y_2 in the DDH problem with at least non-negligible advantage $\varepsilon - 2/q$, where $dist(\tilde{C}, Y_1) = 1/q$ and $dist(\tilde{X}, Y_2) = 1/q$. □

Complexity. The scheme uses two rounds (steps 2 and 4), the first round sends $k+1$ messages and the second round sends $2n$ messages. For computation, R computes $3k+2$ and S computes $(k+2)n$ modular exponentiations.

3.2 k-out-of-n OT against malicious receiver

A malicious player may not follow the protocol dutifully. For example, in scheme OT_n^k-I, a malicious R might send some special form of A_i's in step 2 such that he is able to get extra information, such as the linear combination of two messages (even though we don't know how to do such attack). So, we present another scheme OT_n^k-II that is provable secure against the malicious R. The scheme is depicted in Figure 2.

Let G_q be the subgroup of Z_p^* with prime order q, g be a generator of G_q, and $p = 2q+1$ is also prime. Let $H_1 : \{0,1\}^* \to G_q, H_2 : G_q \to \{0,1\}^l$ be two collision-resistant hash functions. Let messages be of l-bit length. Assume that CT-CDH is hard under G_q.

Correctness. We can check that the chosen messages m_{σ_j}, $j = 1, 2, \ldots, k$, are computed as

$$\begin{aligned} c_{\sigma_j} \oplus H_2(K_j) &= m_{\sigma_j} \oplus H_2(w_{\sigma_j}^x) \oplus H_2(w_{\sigma_j}^x) \\ &= m_{\sigma_j}. \end{aligned}$$

Security analysis. We need the random oracle model in this security analysis.

Theorem 3. *In OT_n^k-II, R's choice meets the receiver's privacy.*

Proof. For any $A_j = w_j g^{a_j}$ and w_l, $l \neq j$, there is an a_l' that satisfies $A_j = w_l g^{a_l'}$. For S, A_j can be a masked value of any index. Thus, the receiver's choices are unconditionally secure. □

– System parameters: (g, H_1, H_2, G_q);
– S has messages: $m_1, m_2, \ldots, m_n$;
– R's choices: $\sigma_1, \sigma_2, \ldots, \sigma_k$;

1. R computes $w_{\sigma_j} = H_1(\sigma_j)$ and $A_j = w_{\sigma_j} g^{a_j}$, where $a_j \in_R Z_q^*$ and $j = 1, 2, \ldots, k$.
2. $R \longrightarrow S$: $A_1, A_2, \ldots, A_k$.
3. S computes $y = g^x$, $D_j = (A_j)^x$, $w_i = H_1(i)$, and $c_i = m_i \oplus H_2(w_i^x)$, where $x \in_R Z_q^*, i = 1, 2, \ldots, n$, and $j = 1, 2, \ldots, k$.
4. $S \longrightarrow R$: y, $D_1, D_2, \ldots, D_k$, $c_1, c_2, \ldots, c_n$
5. R computes $K_j = D_j / y^{a_j}$ and gets $m_{\sigma_j} = c_{\sigma_j} \oplus H_2(K_j)$ for $j = 1, 2, \ldots, k$.

Fig. 2. OT_n^k-II: k-out-of-n OT against malicious receiver

Theorem 4. *Even if R is malicious, the scheme OT_n^k-II meets the requirement for the sender's security assuming hardness of the CT-CDH problem the random oracle model.*

Proof. Since we treat H_2 as a random oracle, the malicious R has to know $K_i = w_i^x$ in order to query the hash oracle to get $H_2(w_i^x)$. For each possible malicious R, we construct a simulator R^* in the Ideal model such that the outputs of R and R^* are indistinguishable.

R^* works as follows:

1. R^* simulates R to obtain $A_1^*, A_2^*, \ldots, A_k^*$. When R queries H_1 on index i, we return a random w_i^* (consistent with the previous queries.)
2. R^* simulates S (externally without knowing m_i's) on inputs A_1^*, $A_2^*, \ldots,$ A_k^* to obtain x^*, y^*, $D_1^*, D_2^*, \ldots, D_k^*$.
3. R^* randomly chooses $c_1^*, c_2^*, \ldots, c_n^*$.
4. R^* simulates R on input $(y^*, D_1^*, D_2^*, \ldots, D_k^*, c_1^*, c_2^*, \ldots, c_n^*)$ and monitors the queries closely. If R queries H_2 on some $v_j = (w_j^*)^{x^*}$, R^* sends j to the TTP T to obtain m_j and returns $c_j^* \oplus m_j$ as the hash value $H_2((w_j^*)^{x^*})$, otherwise, returns a random value (consistent with previous queries).
5. Output $(A_1^*, A_2^*, \ldots, A_k^*, y^*, D_1^*, D_2^*, \ldots, D_k^*, c_1^*, c_2^* \ldots, c_n^*)$.

If R obtains $k+1$ decryption keys, R^* does not know which k indices are really chosen by R. The simulation would fail. Therefore we show that R can obtain at most k decryption keys by assuming the hardness of chosen-target CDH problem: In the above simulation, if R queries H_1, we return a random value output by the target oracle. When R^* simulates S on input $A_1^*, A_2^*, \ldots, A_k^*$, we forward these queries to the helper oracle, and return the corresponding outputs. Finally, if R queries H_2 on legal v_{j_i} for all $1 \leq i \leq k+1$, we can output $k+1$ pairs (v_{j_i}, j_i), which contradicts to the CT-CDH assumption. Thus, R obtains at most k decryption keys.

Let $\sigma_1, \sigma_2, \ldots, \sigma_k$ be the k choices of R. For the queried legal v_{σ_j}'s, c_{σ_j} is consistent with the returned hash values, for $j = 1, 2, \ldots, k$. Since no other $(w_l^*)^{x^*}$,

– System parameters: (g, H_1, H_2, G_q);
– S has messages: $m_1, m_2, \ldots, m_n$;
– R's choices: $\sigma_1, \sigma_2, \ldots, \sigma_k$;

Commitment Phase

1. S computes $c_i = m_i \oplus H_2(w_i^x)$ for $i = 1, 2, \ldots, n$, and $y = g^x$ where $w_i = H_1(i)$, and $x \in_R Z_q^*$.
2. $S \longrightarrow R : y, c_1, c_2, \ldots, c_n$.

Transfer Phase

For each σ_j, $j = 1, 2, \ldots, k$, R and S execute the following steps:

1. R chooses a random $a_j \in Z_q^*$ and computes $w_{\sigma_j} = H_1(\sigma_j), A_j = w_{\sigma_j} g^{a_j}$.
2. $R \longrightarrow S : A_j$.
3. $S \longrightarrow R : D_j = (A_j)^x$.
4. R computes $K_j = D_j / y^{a_j}$ and gets $m_{\sigma_j} = c_{\sigma_j} \oplus H_2(K_j)$.

Fig. 3. Adpt-OT$_n^k$: Adaptive OT$_n^k$

$l \neq \sigma_1, \sigma_2, \ldots, \sigma_k$, can be queried to the H_2 hash oracle, c_l has the right distribution (due to the random oracle model). Thus, the output distribution is indistinguishable from that of R.

□

Complexity. OT$_n^k$-II has two rounds. The first round sends k messages and the second round sends $n + k + 1$ messages. For computation, R computes $2k$, and S computes $n + k + 1$ modular exponentiations.

4 k-out-of-n OT with adaptive queries

The queries of R in our schemes can be adaptive. In our schemes, the commitments c_i's of the messages m_i's of S to R are independent of the key masking. Therefore, our scheme is adaptive in nature. Our Adpt-OT$_n^k$ scheme, which rephrases the OT$_n^k$-II scheme, is depicted in Figure 3.

The protocol consists of two phases: the commitment phase and the transfer phase. The sender S first commits the messages in the commitment phase. In the transfer phase, for each query, R sends the query A_j to S and obtains the corresponding key to decrypt the commitment c_j.

Correctness of the scheme follows that of OT$_n^k$-II.

Security analysis. The security proofs are almost the same as those for OT$_n^k$-II. We omit them here.

Complexity. In the commitment phase, S needs $n+1$ modular exponentiations for computing the commitments c_i's and y. In the transfer phase, R needs 2 modular exponentiations for computing the query and the chosen message. S

needs one modular exponentiation for answering each R's query. The commitment phase is one-round and the transfer phase is two-round for each adaptive query.

5 Conclusion

We have presented two very efficient OT_n^k schemes against semi-honest receivers in the standard model and malicious receivers in the random oracle model. Our schemes possess other interesting features, such as, it can be non-interactive and needs no prior setup or trapdoor. We also proposed an efficient Adpt-OT_n^k for adaptive queries. The essential feature allowing this is the reversal of the orders of key commitment and message commitment. In most previous schemes (including OT_n^k-I), the key commitments (for encrypting the chosen messages) are sent to S first. The message commitments are dependent on the key commitments. Nevertheless, in our scheme OT_n^k-II the message commitments are independent of the key commitment. Thus, the message commitments can be sent to R first.

References

[BBCS91] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Marie-Hélène Skubiszewska. Practical quantum oblivious transfer. In *Proceedings of Advances in Cryptology - CRYPTO '91*, volume 576 of *LNCS*, pages 351–366. Springer-Verlag, 1991.

[BCR86] Gilles Brassard, Claude Crépeau, and Jean-Marc Robert. All-or-nothing disclosure of secrets. In *Proceedings of Advances in Cryptology - CRYPTO '86*, volume 263 of *LNCS*, pages 234–238. Springer-Verlag, 1986.

[BCR87] Gilles Brassard, Claude Crépeau, and Jean-Marc Robert. Information theoretic reductions among disclosure problems. In *Proceedings of 28th Annual Symposium on Foundations of Computer Science (FOCS '87)*, pages 427–437. IEEE, 1987.

[BCS96] Gilles Brassard, Claude Crépeau, and Miklós Sántha. Oblivious transfers and intersecting codes. *IEEE Transactions on Information Theory*, 42(6):1769–1780, 1996.

[BDSS02] Carlo Blundo, Paolo D'Arco, Alfredo De Santis, and Douglas R. Stinson. New results on unconditionally secure distributed oblivious transfer. In *Proceedings of Selected Areas in Cryptography - SAC '02*, volume 2595 of *LNCS*, pages 291–309. Springer-Verlag, 2002.

[BM89] Mihir Bellare and Silvio Micali. Non-interactive oblivious transfer and applications. In *Proceedings of Advances in Cryptology - CRYPTO '89*, volume 435 of *LNCS*, pages 547–557. Springer-Verlag, 1989.

[BNPS01] Mihir Bellare, Chanathip Namprempre, David Pointcheval, and Michael Semanko. Power of rsa inversion oracles and the security of Chaum's RSA-based blind signature scheme. In *Proceedings of Financial Cryptography (FC '01)*, pages 319–338. Springer-Verlag, 2001.

[Bol03] Alexandra Boldyreva. Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme. In *Proceedings of the Public-Key Cryptography (PKC '03)*, pages 31–46. Springer-Verlag, 2003.

[CCM98] Christian Cachin, Claude Crepeau, and Julien Marcil. Oblivious transfer with a memory-bounded receiver. In *Proceedings of 39th Annual Symposium on Foundations of Computer Science (FOCS '98)*, pages 493–502. IEEE, 1998.

[CZ03] Zhide Chen and Hong Zhu. Quantum m-out-of-n oblivious transfer. Technical report, arXiv:cs.CR/0311039, 2003.

[Din01] Yan Zong Ding. Oblivious transfer in the bounded storage model. In *Proceedings of Advances in Cryptology - CRYPTO '01*, volume 2139 of *LNCS*, pages 155–170. Springer-Verlag, 2001.

[EGL85] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. *Communications of the ACM*, 28(6):637–647, 1985.

[GV87] Oded Goldreich and Ronen Vainish. How to solve any protocol problem - an efficiency improvement. In *Proceedings of Advances in Cryptology - CRYPTO '87*, volume 293 of *LNCS*, pages 73–86. Springer-Verlag, 1987.

[IKNP03] Yuval Ishai, Joe Kilian, Kobbi Nissim, and Erez Petrank. Extending oblivious transfers efficiently. In *Proceedings of Advances in Cryptology - CRYPTO '03*, volume 2729 of *LNCS*, pages 145–161. Springer-Verlag, 2003.

[Kil88] Joe Kilian. Founding cryptography on oblivious transfer. In *Proceedings of the 20th Annual ACM Symposium on the Theory of Computing (STOC '88)*, pages 20–31. ACM, 1988.

[Lip] Helger Lipmaa. Oblivious transfer. http://www.tcs.hut.fi/ helger/crypto/link/protocols/oblivious.html.

[Lip04] Helger Lipmaa. An oblivious transfer protocol with log-squared communication. Technical report, Cryptology ePrint Archive: Report 2004/063, 2004.

[MZV02] Yi Mu, Junqi Zhang, and Vijay Varadharajan. m out of n oblivious transfer. In *Proceedings of the 7th Australasian Conference on Information Security and Privacy (ACISP '02)*, volume 2384 of *LNCS*, pages 395–405. Springer-Verlag, 2002.

[NP99a] Moni Naor and Benny Pinkas. Oblivious transfer and polynomial evaluation. In *Proceedings of the 31th Annual ACM Symposium on the Theory of Computing (STOC '99)*, pages 245–254. ACM, 1999.

[NP99b] Moni Naor and Benny Pinkas. Oblivious transfer with adaptive queries. In *Proceedings of Advances in Cryptology - CRYPTO '99*, volume 1666 of *LNCS*, pages 573–590. Springer-Verlag, 1999.

[NP00] Moni Naor and Benny Pinkas. Distributed oblivious transfer. In *Proceedings of Advances in Cryptology - ASIACRYPT '00*, volume 1976 of *LNCS*, pages 200–219. Springer-Verlag, 2000.

[NP01] Moni Naor and Benny Pinkas. Efficient oblivious transfer protocols. In *Proceedings of the 12th Annual Symposium on Discrete Algorithms (SODA '01)*, pages 448–457. ACM/SIAM, 2001.

[NR94] Valtteri Niemi and Ari Renvall. Cryptographic protocols and voting. In *Results and Trends in Theoretical Computer Science*, volume 812 of *LNCS*, pages 307–317. Springer-Verlag, 1994.

[OK04] Wakaha Ogata and Kaoru Kurosawa. Oblivious keyword search. *Journal of Complexity*, 20(2-3):356–371, 2004.

[Rab81] Michael O. Rabin. How to exchange secrets by oblivious transfer. Technical Report TR-81, Aiken Computation Laboratory, Harvard University, 1981.

[SS90] Arto Salomaa and Lila Santean. Secret selling of secrets with several buyers. *Bulletin of the European Association for Theoretical Computer Science (EATCS)*, 42:178–186, 1990.

[Ste98] Julien P. Stern. A new and efficient all or nothing disclosure of secrets protocol. In *Proceedings of Advances in Cryptology - ASIACRYPT '98*, volume 1514 of *LNCS*, pages 357–371. Springer-Verlag, 1998.

[Tze02] Wen-Guey Tzeng. Efficient 1-out-n oblivious transfer schemes. In *Proceedings of the Public-Key Cryptography (PKC '02)*, pages 159–171. Springer-Verlag, 2002.

[YBD03] Gang Yao, Feng Bao, and Robert Deng. Security analysis of three oblivious transfer protocols. Workshop on Coding, Cryptography and Combinatorics, Huangshan City, China, 2003.