Journal of Universal Computer Science, vol. 14, no. 3 (2008), 397-415
submitted: 2/6/07, accepted: 1/11/07, appeared: 1/2/08 © J.UCS

Efficient k-out-of-n Oblivious Transfer Schemes

Cheng-Kang Chu
(National Chiao Tung University, Taiwan
ckchu@cs.nctu.edu.tw)

Wen-Guey Tzeng
(National Chiao Tung University, Taiwan
wgtzeng @cs.nctu.edu.tw)

Abstract: Oblivious transfer is an important cryptographic protocol in various security applications. For example, in on-line transactions, a k-out-of-n oblivious transfer scheme allows a buyer to *privately* choose k out of n digital goods from a merchant without learning information about other $n-k$ goods. In this paper, we propose several efficient two-round k-out-of-n oblivious transfer schemes, in which the receiver R sends $O(k)$ messages to the sender S, and S sends $O(n)$ messages back to R. The schemes provide unconditional security for either sender or receiver. The computational security for the other side is based on the Decisional Diffie-Hellman (DDH) or Chosen-Target Computational Diffie-Hellman (CT-CDH) problems. Our schemes have the nice property of universal parameters, that is, each pair of R and S need not hold any secret before performing the protocol. The system parameters can be used by all senders and receivers without any trapdoor specification. In some cases, our OT_n^k schemes are the most efficient ones in terms of the communication cost, either in rounds or the number of messages. Moreover, one of our schemes is extended to an adaptive oblivious transfer scheme. In that 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. The preliminary version of this paper was published at PKC '05 [Chu and Tzeng 2005].
Key Words: oblivious transfer, privacy protection, electronic commerce
Category: E.3, D.4.6, K.6.5

1 Introduction

Assume that an on-line store sells digital goods, such as music, articles, etc. The buyer wants to get some of them without revealing his/her choices. That is, the buyer can only get the paid goods, and the merchant doesn't know which ones are chosen. Oblivious transfer (OT) is a cryptographic protocol designed for such requirement. The other applications of OT in computer security are secret exchange [Rabin 1981], contract singing [Even et al. 1985], etc. Moreover, OT is also an important primitive used in many other cryptographic protocols [Goldreich and Vainish 1987, Kilian 1988]. For example, Yao [Yao 1986] proposed the notion of secure circuit computation by using oblivious transfer.

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 notion of oblivious transfer was first introduced by Rabin [Rabin 1981]. Then it was developed in the following four types:

– Rabin's OT: S sends a message to R, and R gets the message with probability $\frac{1}{2}$. On the other hand, S does not know whether R gets the message or not.

– 1-out-of-2 OT (OT_2^1): 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.

– 1-out-of-n OT (OT_n^1): An extension of OT_2^1 for the case that S has n messages.

– k-out-of-n OT (OT_n^k): The scheme similar to OT_n^1 except that R obtains k out of n messages from S.

We are concerned about the most general case - OT_n^k in this work. 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 security of OT is also an interesting consideration. Since it is impossible to provide unconditional security for both the sender and the receiver, we consider the case that only one of them has perfect (unconditional) security, and the security of the other side is computational. We can choose appropriate schemes in the different applications.

Oblivious transfer with adaptive queries (Adpt-OT) allows R to query messages one by one adaptively [Naor and Pinkas 1999b, Ogata and Kurosawa 2004]. For this setting, S first commits messages to R in the commitment phase. In the transfer phase, R makes queries of messages one by one. It seems that the adaptive case implies the non-adaptive case. But, the non-adaptive one converted from an adaptive one usually needs one more round to send the public parameters from S to R. Since our scheme needs no trapdoors, there is no entailed cost due to conversion. Adaptive OT is natural and has many applications, such as oblivious search, oblivious database queries, private information retrieval, etc.

In this paper we propose several 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 schemes provide perfect security for either sender or receiver. The computational security for the other side is based on the Decisional Diffie-Hellman (DDH) or Chosen-Target Computational Diffie-Hellman (CT-CDH) problems. When $k = 1$, our scheme is as efficient as the one in [Tzeng 2004]. Our schemes have the nice property of universal parameters, that is, each pair of R and S need not hold any secret before performing the protocol. The system parameters can be used by all senders and receivers without any trapdoor specification. In some cases, our OT_n^k schemes are the most efficient ones in terms of the communication cost, either in rounds or the number of messages[1].

Moreover, one of our schemes is extended to an adaptive OT scheme. In that 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.

1.1 Previous work and comparison

Rabin [Rabin 1981] 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 [Even et al. 1985] proposed an extension of bit-OT_2^1, in which the sender's two messages m_1 and m_2 are only one-bit. Brassard, Crépeau and Robert [Brassard et al. 1986a] 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 [Brassard et al. 1986b, Brassard et al. 1996, Naor and Pinkas 1999a], some are constructed directly from cryptographic techniques [Salomaa and Santean 1990, Niemi and Renvall 1994, Stern 1998, Naor and Pinkas 2001, Tzeng 2004, Boneh et al. 2005], and the others derived from computational private information retrieval (CPIR) have polylogarithmic communication cost [Lipmaa 2005]. However, the scheme achieves only computational receiver's privacy and unconditional sender's security. Besides, there are various oblivious transfer schemes developed in different models and applications, such as OT in the bounded storage model [Cachin et al. 1998, Ding 2001], distributed OT [Naor and Pinkas 2000, Blundo et al. 2002], Quantum OT [Bennett et al. 1991, Chen and Zhu 2003], and so on. Lipmaa [Lipmaa] provided a good collection of these works.

For OT_n^k, Bellare and Micali [Bellare and Micali 1989] proposed an OT_n^{n-1} scheme. Naor and Pinkas [Naor and Pinkas 1999a] 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 $k \leq n^{1/4}$. Moreover, they took notice of adaptive queries and provided some Adaptive OT_n^k schemes [Naor and Pinkas 1999b]. 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 [Mu et al. 2002] presented some efficient OT_n^k schemes. These schemes are designed from cryptographic functions directly. The most efficient one is a non-interactive one. To

[1] For the scheme with perfect sender's security, one may perform the schemes of Lipmaa [Lipmaa 2005] k times independently to get better efficiency in some cases of k and n.

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 $O(n)$ 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. Wu, Zhang, and Wang [Wu et al. 2003] also provided a three-round OT_n^k based on the two-lock cryptosystem. Recently, Ogata and Kurosawa [Ogata and Kurosawa 2004] 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 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 [Ishai et al. 2003] proposed some efficient protocols for extending a small number of OT's to a large number of OT's. Chen and Zhu [Chen and Zhu 2003] provided an OT_n^k in the quantum computation model. We won't compare these schemes with ours since they are in different categories.

1.2 Our Results

We propose three k-out-of-n OT schemes and one adaptive OT scheme, named OT_n^k-I, OT_n^k-II, OT_n^k-III, and Adpt-OT_n. OT_n^k-I and OT_n^k-II have perfect security for the receiver, where OT_n^k-I assumes a semi-honest receiver in the standard model and OT_n^k-II is secure against any malicious receiver in the random oracle model. OT_n^k-III provides perfect security for the sender in the standard model. Finally, we extend OT_n^k-II to Adpt-OT_n directly.

In [Tab. 1] we summarize the comparison of ours, Mu, Zheng, and Varadharajan's [Mu et al. 2002], Wu, Zhang, and Wang's [Wu et al. 2003], and Naor and Pinkas's [Naor and Pinkas 1999a] OT_n^k schemes. In [Tab. 2] we summarize the comparison of ours, Naor and Pinkas's [Naor and Pinkas 1999b], and Ogata and Kurosawa's [Ogata and Kurosawa 2004] Adpt-OT_n^k schemes. Note that the works of [Naor and Pinkas 1999a] and [Naor and Pinkas 1999b] invoke other OT schemes, therefore we use asymptotical orders for them in the comparison.

2 Preliminaries

Involved parties. An OT scheme has two involved parties: the sender and receiver. Both are polynomial-time-bounded probabilistic Turing machines (PPTM). A party is semi-honest (or passive, honest-but-curious) 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.

	OT_n^k-I	OT_n^k-II	OT_n^k-III	MZV	WZW	NP
rounds	2	2	2	2	3	$O(wk \log n)$
messages† $(R \to S)$	k	k	$2k+2$	$2n$	k	$O(wk \log n)$
messages† $(S \to R)$	$2n$	$n+k$	$2n$	$2n$	$n+k$	$O(n + wk \log n)$
universal parameters	Yes	Yes	Yes	Yes	Yes	No (need setup)
made to adaptiveness	No	Yes	No	No	Yes	Yes

† The number of group elements.

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

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

† The number of group elements.
* 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.

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. For the scheme OT_n^k-I and OT_n^k-III, we have the following security 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. If the ciphertexts of unchosen messages are uniformly distributed for R, the security of S is unconditional.

Scheme OT_n^k-II and scheme Adpt-OT_n should meet the following security 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 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 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 $\mathbb{G}_q$ be a subgroup of $\mathbb{Z}_p^*$ with prime order q, and $p = 2q+1$ is also prime. Let g be a generator of $\mathbb{G}_q$. We usually denote $g^x \bmod p$ as g^x, where $x \in \mathbb{Z}_q$. Let $x \in_R X$ denote that x is chosen uniformly and independently from the set X.

Security assumptions. For the schemes OT_n^k-I and OT_n^k-III, we assume hardness of the Decisional Diffie-Hellman (DDH) problem. For OT_n^k-II and Adpt-OT_n, we assume hardness of the Chosen-Target Computational Diffie-Hellman (CT-CDH) problem.

Assumption 1 (Decisional Diffie-Hellman (DDH)) *Let $p = 2q + 1$ where p, q are two primes, and $\mathbb{G}_q$ be the subgroup of $\mathbb{Z}_p^*$ with order q. The following two distribution ensembles are computationally indistinguishable:*

– $Y_1 = \{(g, g^a, g^b, g^{ab})\}_{\mathbb{G}_q}$, *where g is a generator of $\mathbb{G}_q$, and $a, b \in_R \mathbb{Z}_q$.*

- System parameters: $(g, h, \mathbb{G}_q)$;
- 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 $f(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1} + x^k$ and $f'(x) = b_0 + b_1x + \cdots + b_{k-1}x^{k-1} + x^k$ where $a_0, a_1, \ldots, a_{k-1} \in_R \mathbb{Z}_q$ and $b_0 + b_1x + \cdots + b_{k-1}x^{k-1} + x^k \equiv (x - \sigma_1)(x - \sigma_2) \cdots (x - \sigma_k) \bmod q$.
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 $c_i = (g^{k_i}, m_iB_i^{k_i})$ where $k_i \in_R \mathbb{Z}_q$ and $B_i = g^{f(i)}h^{f'(i)} = A_0A_1^i \cdots A_{k-1}^{i^{k-1}}(gh)^{i^k} \bmod p$, 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.

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

– $Y_2 = \{(g, g^a, g^b, g^c)\}_{\mathbb{G}_q}$, *where g is a generator of $\mathbb{G}_q$, and $a, b, c \in_R \mathbb{Z}_q$.*

The variations used in our proofs are easily shown to be equivalent to the DDH assumption.

The CT-CDH assumption, introduced by Boldyreva [Boldyreva 2003], is analogous to the chosen-target RSA inversion assumption defined by Bellare, et al. [Bellare et al. 2001]

Assumption 2 (Chosen-Target Computational Diffie-Hellman (CT-CDH)) *Let $\mathbb{G}_q$ be a group of prime order q, g be a generator of $\mathbb{G}_q$, $x \in_R \mathbb{Z}_q^*$. Let $H_1 : \{0,1\}^* \to \mathbb{G}_q$ 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 $w_i \in \mathbb{G}_q$ 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 $i \in \{1, 2, \ldots, k\}$, $q_H < k \leq q_T$, is negligible.*

3 k-out-of-n OT schemes with perfect security of receiver

We present OT_n^k schemes with perfect security for the receiver in this section.

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 $\mathbb{G}_q$, that is, all messages are in $\mathbb{G}_q$. The receiver R wants to get $m_{\sigma_1}, m_{\sigma_2}, \ldots, m_{\sigma_k}$ without revealing any information about $\sigma_1, \sigma_2, \ldots, \sigma_k$. The protocol OT_n^k-I is depicted in [Fig. 1].

For system parameters, let g, h be two generators of $\mathbb{G}_q$ where $\log_g h$ is unknown to all, and $\mathbb{G}_q$ be the group with some description. These parameters can be used repeatedly by all possible senders and receivers as long as the value $\log_g h$ is not revealed. Therefore, $(g, h, \mathbb{G}_q)$ 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. If the DDH assumption holds and R is semi-honest, R 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. Assume that there is a polynomial-time distinguisher $\mathcal{D} = (\mathcal{D}_1, \mathcal{D}_2)$ where $\mathcal{D}_1$ takes k choices as inputs and outputs $f^*(x), f'^*(x)$ (Since $\mathcal{D}$ is semi-honest, $\mathcal{D}_1$ follows the protocol and chooses the correct values), and $\mathcal{D}_2$ distinguishes the following two distributions:

– $C = (g^*, h^*, f^*(x), f'^*(x), ((g^*)^{k^*_{i_1}}, (B^*_{i_1})^{k^*_{i_1}}), \ldots, ((g^*)^{k^*_{i_{n-k}}}, (B^*_{i_{n-k}})^{k^*_{i_{n-k}}}))$, where $g^*, h^* \in \mathbb{G}_q \backslash \{1\}, k^*_i \in_R \mathbb{Z}_q, B^*_i = (g^*)^{f^*(i)}(h^*)^{f'^*(i)}$

– $X = (g^*, h^*, f^*(x), f'^*(x), ((g^*)^{k^*_{i_1}}, X_1), \ldots, ((g^*)^{k^*_{i_{n-k}}}, X_{n-k}))$, where $g^*, h^* \in \mathbb{G}_q \backslash \{1\}, k^*_i \in_R \mathbb{Z}_q, X_i \in_R \mathbb{G}_q$.

Then we can construct another PPTM $\mathcal{D}'$, which takes $\mathcal{D}$ as a sub-routine, to distinguish the following two distributions:

– $\tilde{Y}_1 = \{(g, h, g^a, h^a)\}_{\mathbb{G}_q}$, where g, h are generators of $\mathbb{G}_q$, and $a \in_R \mathbb{Z}_q$.

– $\tilde{Y}_2 = \{(g, h, g^a, g^b)\}_{\mathbb{G}_q}$, where g, h are generators of $\mathbb{G}_q$, and $a, b \in_R \mathbb{Z}_q$.

The difference between $(\tilde{Y}_1, \tilde{Y}_2)$ and (Y_1, Y_2) is that h can't be 1 in $\tilde{Y}_1$ and $\tilde{Y}_2$.
<u>Machine $\mathcal{D}'$</u>
Input: (g, u, v, w) (either from $\tilde{Y}_1$ or $\tilde{Y}_2$)

1. Let $g^* = g, h^* = u$ be the system parameters of OT^k_n-I.
2. Randomly select $\sigma_1, \ldots, \sigma_k \in \{1, \ldots, n\}$, and let $\mathcal{I} = \{i_1, \ldots, i_{n-k}\}$ $= \{1, \ldots, n\} \backslash \{\sigma_1, \ldots, \sigma_k\}$.
3. Perform $\mathcal{D}_1(\sigma_1, \ldots, \sigma_k) = (f^*(x), f'^*(x))$.
4. Randomly select $l \in \mathcal{I}$.
5. Output $\mathcal{D}_2(g^*, h^*, f^*(x), f'^*(x), (U^*_i, V^*_i))$ for all $i \in \mathcal{I}$, where
$$(U^*_i, V^*_i) = \begin{cases} ((g^*)^{k^*_i}, (B^*_i)^{k^*_i}) & \text{if } i \in \{i_1, \ldots, i_{l-1}\} \\ (v, v^{f^*(i)} w^{f'^*(i)}) & \text{if } i = i_l \\ ((g^*)^{k^*_i}, X_i) & \text{if } i \in \{i_{l+1}, \ldots, i_{n-k}\} \end{cases},$$
and $k^*_i \in_R \mathbb{Z}_q, B^*_i = (g^*)^{f^*(i)}(h^*)^{f'^*(i)}, X_i \in_R \mathbb{G}_q$.

Assume that $\mathcal{D}$ distinguishes C and X with non-negligible advantage ε. Let $\alpha = (g, u, v, w)$ and $\vec{C}_l = (g^*, h^*, f^*(x), f'^*(x), (U^*_i, V^*_i)), i = 1, 2, \ldots, n-k$ where
$$(U^*_i, V^*_i) = \begin{cases} ((g^*)^{k^*_i}, (B^*_i)^{k^*_i}) & \text{if } i \in \{1, \ldots, l\} \\ ((g^*)^{k^*_i}, X_i) & \text{if } i \in \{l+1, \ldots, n-k\} \end{cases},$$
and $k^*_i \in_R \mathbb{Z}_q, B^*_i = (g^*)^{f^*(i)}(h^*)^{f'^*(i)}, X_i \in_R \mathbb{G}_q$. Note that $\vec{C}_{n-k} = C$ and $\vec{C}_0 = X$. If α is chosen from $\tilde{Y}_1$, then
$$\Pr_{\alpha \in \tilde{Y}_1}[\mathcal{D}'(\alpha) = 1] = \Pr[\mathcal{D}'(\tilde{Y}_1) = 1] = \frac{1}{n-k} \sum_{l=1}^{n-k} \Pr[\mathcal{D}(\vec{C}_l) = 1].$$

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

1. R computes $h_{\sigma_j} = H_1(\sigma_j)$ and $A_j = (h_{\sigma_j})^{a_j}$, where $a_j \in_R \mathbb{Z}_q^*$ and $j = 1, 2, \ldots, k$.
2. $R \longrightarrow S$: $A_1, A_2, \ldots, A_k$.
3. S chooses a random $x \in \mathbb{Z}_q^*$ and computes $D_j = (A_j)^x$, $h_i = H_1(i)$, and $c_i = m_i \oplus H_2(h_i^x)$, where $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, k$.
4. $S \longrightarrow R$: $D_1, D_2, \ldots, D_k$, $c_1, c_2, \ldots, c_n$
5. R computes $K_j = (D_j)^{a_j^{-1}}$ and gets $m_{\sigma_j} = c_{\sigma_j} \oplus H_2(K_j)$ for $j = 1, 2, \ldots, k$.

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

If α is chosen from $\tilde{Y}_2$, then

$$\Pr_{\alpha \in \tilde{Y}_2}[\mathcal{D}'(\alpha) = 1] = \Pr[\mathcal{D}'(\tilde{Y}_2) = 1] = \frac{1}{n-k} \sum_{l=0}^{n-k-1} \Pr[\mathcal{D}(\vec{C}_l) = 1].$$

Therefore, we have

$$\begin{aligned} & \Pr[\mathcal{D}'(\tilde{Y}_1) = 1] - \Pr[\mathcal{D}'(\tilde{Y}_2) = 1] \\ &= \tfrac{1}{n-k}\left(\textstyle\sum_{l=1}^{n-k} \Pr[\mathcal{D}(\vec{C}_l) = 1] - \sum_{l^*=0}^{n-k-1} \Pr[\mathcal{D}(\vec{C}_l) = 1]\right) \\ &= \tfrac{1}{n-k}(\Pr[\mathcal{D}(\vec{C}_{n-k}) = 1] - \Pr[\mathcal{D}(\vec{C}_0) = 1]) \\ &= \tfrac{1}{n-k}(\Pr[\mathcal{D}(C) = 1] - \Pr[\mathcal{D}(X) = 1]) \\ &\geq \tfrac{\varepsilon}{n-k}. \end{aligned}$$

Moreover, since $dist(\tilde{Y}_1, Y_1) = 1/q$ and $dist(\tilde{Y}_2, Y_2) = 1/q$, we can solve the DDH problem with at least non-negligible advantage $\frac{\varepsilon}{n-k} - \frac{2}{q}$, which is a contradiction. □

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

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

A malicious player may not follow the protocol dutifully. For example, a malicious R might send random A_i's in step 2. So, we present another scheme OT_n^k-II that is provable secure against the malicious R in the random oracle model. The scheme is depicted in [Fig. 2].

The generator g and group $\mathbb{G}_q$ of system parameters are defined as that in OT_n^k-I. Let $H_1 : \{0,1\}^* \to \mathbb{G}_q, H_2 : \mathbb{G}_q \to \{0,1\}^l$ be two collision-resistant hash functions. Let messages be of l-bit length. Assume that CT-CDH is hard under $\mathbb{G}_q$.

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

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

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

Theorem 3. *In OT^k_n-II, R's choices are unconditionally secure.*

Proof. Since $\mathbb{G}_q$ is the group of prime order q, all elements except 1 in $\mathbb{G}_q$ are generators. So for any $A_j = h_j^{a_j}$ and any h_l, $l \neq j$, there is an a_l that satisfies $A_j = h_l^{a_l}$. That is, A_j can be a masked value of any index. Thus, the receiver's choices are unconditionally secure.

□

Theorem 4. *Even if R is malicious, the scheme OT^k_n-II meets the requirement for the sender's security in the random oracle model.*

Proof. Since we treat H_2 as a random oracle, the malicious R has to know $K_i = h_i^x$ in order to query the hash oracle to get $H_2(h_i^x)$. 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 h_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^*, $D_1^*, D_2^*, \ldots, D_k^*$.
3. R^* randomly chooses $c_1^*, c_2^*, \ldots, c_n^*$.
4. R^* simulates R on input $(D_1^*, D_2^*, \ldots, D_k^*, c_1^*, c_2^*, \ldots, c_n^*)$ and monitors the queries closely. If R queries H_2 on some $v_j = (h_j^*)^{x^*}$, R^* sends j to the TTP T to obtain m_j and returns $c_j^* \oplus m_j$ as the hash value $H_2((h_j^*)^{x^*})$, otherwise, returns a random value (consistent with previous queries).
5. Output $(A_1^*, A_2^*, \ldots, A_k^*, D_1^*, D_2^*, \ldots, D_k^*, c_1^*, c_2^* \ldots, c_n^*)$.

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

- System parameters: $(g, \mathbb{G}_q)$;
- S has messages: $m_1, m_2, \dots, m_n$;
- R's choices: $\sigma_1, \sigma_2, \dots, \sigma_k$;

1. R chooses a generator h of $\mathbb{G}_q$, a random $b \in \mathbb{Z}_q$, and two polynomials $f(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1} + x^k$ and $f'(x) = a'_0 + a'_1 x + \cdots + a'_{k-1}x^{k-1} + x^k$ where $a_0, a_1, \dots, a_{k-1} \in_R \mathbb{Z}_q$ and $a'_0 + a'_1 x + \cdots + a'_{k-1}x^{k-1} + x^k \equiv (x-\sigma_1)(x-\sigma_2)\cdots(x-\sigma_k) \bmod q$. Let $(A_0, A_1, \dots, A_{k-1}) = (g^{a_0}, g^{a_1}, \dots, g^{a_{k-1}}), B = g^b, (C_0, C_1, \dots, C_{k-1}) = (g^{a_0 b}h^{a'_0}, g^{a_1 b}h^{a'_1}, \dots, g^{a_{k-1}b}h^{a'_{k-1}})$.
2. $R \longrightarrow S : (h, A_0, A_1, \dots, A_{k-1}, B, C_0, C_1, \dots, C_{k-1})$.
3. S chooses n random pairs $(r_1, s_1), (r_2, s_2), \cdots, (r_n, s_n)$ in $\mathbb{Z}_q$, and computes $c_i = (g^{f(i)r_i}g^{s_i}, (g^{f(i)b}h^{f'(i)})^{r_i}(g^b)^{s_i} \oplus m_i) = (X_i^{r_i}g^{s_i}, Z_i^{r_i}B^{s_i} \oplus m_i)$ for $i = 1, 2, \dots, n$, where $X_i = A_0 A_1^i \cdots A_{k-1}^{i^{k-1}} g^{i^k}, Z_i = C_0 C_1^i \cdots C_{k-1}^{i^{k-1}} (gh)^{i^k}$.
4. $S \longrightarrow R$: $c_1, c_2, \dots, c_n$.
5. Let $c_i = (U_i, V_i)$. R computes $m_{\sigma_i} = U_{\sigma_i}^b \oplus V_{\sigma_i}$ for each σ_i.

Figure 3: OT_n^k-III: k-out-of-n OT with perfect sender's security

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 $1 \le i \le k+1$, 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 $\sigma_1,\ \sigma_2, \dots, \sigma_k$ 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 $j = 1, 2, \dots, k$. Since no other $(h_l^*)^{x^*}$, $l \ne \sigma_1, \sigma_2, \dots, \sigma_k$, 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 $n+k$ messages. For computation, R computes $2k$, and S computes $n+k$ modular exponentiations.

4 k-out-of-n OT scheme with perfect security of sender

On the other hand, we propose another k-out-of-n OT with unconditional security for the sender and computational privacy for the receiver. The scheme is extended from the 1-out-of-n OT under the same security condition provided by Naor and Pinkas [Naor and Pinkas 2001]. We present the protocol in [Fig. 3].

The main idea of this scheme is the same as OT_n^k-I. R first chooses two polynomials $f(x), f'(x)$ and a random value b where $f'(x)$ represents the choices, and $f(x)$ and b are used to mask $f'(x)$. By the DDH assumption, $C_i = g^{a_i b}h^{a'_i}$ can't be distinguished from the random value when given g^{a_i} and g^b, for $i = 0, 1, \dots, k-1$. Therefore the choices of R are computationally secure.

Then S encrypts the messages by the similar technique of randomized reduction of DDH from [Naor and Reingold 1997, Stadler 1996]. The receiver R uses the value b to decrypt the chosen messages, and gets no information about other messages.

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

$$\begin{aligned} U_{\sigma_i}^b \oplus V_{\sigma_i} &= (g^{f(\sigma_i)r_{\sigma_i}} g^{s_{\sigma_i}})^b \oplus (g^{f(\sigma_i)b} h^{f'(\sigma_i)})^{r_{\sigma_i}} (g^b)^{s_{\sigma_i}} \oplus m_{\sigma_i} \\ &= g^{f(\sigma_i)br_{\sigma_i}+bs_{\sigma_i}} \oplus (g^{f(\sigma_i)b} \cdot 1)^{r_{\sigma_i}} g^{bs_{\sigma_i}} \oplus m_{\sigma_i} \\ &= g^{f(\sigma_i)br_{\sigma_i}+bs_{\sigma_i}} \oplus g^{f(\sigma_i)br_{\sigma_i}+bs_{\sigma_i}} \oplus m_{\sigma_i} \\ &= m_{\sigma_i}. \end{aligned}$$

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

Theorem 5. *For scheme OT_n^k-III, R's choices are secure under the DDH assumption.*

Proof. Since R's choices $(\sigma_1, \sigma_2, \ldots, \sigma_k)$ are concealed in $(C_0, C_1, \ldots, C_{k-1})$, we prove the receiver's privacy by showing that $(C_0, C_1, \ldots, C_{k-1})$ look random if the DDH assumption holds. Assume that there exists a distinguisher $\mathcal{D}$ distinguishes the following two distributions:

- $E = (g, g^{a_0}, g^{a_1}, \ldots, g^{a_{k-1}}, g^b, g^{a_0 b}, g^{a_1 b}, \ldots, g^{a_{k-1} b})$, where g is a generator of $\mathbb{G}_q, a_0, a_1, \ldots, a_{k-1}, b \in_R \mathbb{Z}_q$;
- $X = (g, g^{a_0}, g^{a_1}, \ldots, g^{a_{k-1}}, g^b, R_0, R_1, \ldots, R_{k-1})$, where g is a generator of $\mathbb{G}_q, a_0, a_1, \ldots, a_{k-1}, b \in_R \mathbb{Z}_q, R_0, R_1, \ldots, R_{k-1} \in_R \mathbb{G}_q$.

We can construct another PPTM $\mathcal{D}'$, which takes $\mathcal{D}$ as a sub-routine, to solve the DDH problem:
<u>Machine $\mathcal{D}'$</u>
Input: (g, u, v, w) (either from Y_1 or Y_2)

1. Let $g^* = g$ be the system parameters of OT_n^k-III.
2. Randomly select $l \in \{0, 1, \ldots, k-1\}$.
3. Output $\mathcal{D}(g^*, A_0^*, A_1^*, \ldots, A_{k-1}^*, v, C_0^*, C_1^*, \ldots, C_{k-1}^*)$ where

$$(A_i^*, C_i^*) = \begin{cases} ((g^*)^{a_i^*}, v^{a_i^*}), a_i^* \in_R \mathbb{Z}_q & \text{if } i \in \{0, \ldots, l-1\} \\ (u, w) & \text{if } i = l \\ ((g^*)^{a_i^*}, R_i), a_i^* \in_R \mathbb{Z}_q, R_i \in_R \mathbb{G}_q & \text{if } i \in \{l+1, \ldots, k-1\} \end{cases}.$$

Assume that $\mathcal{D}$ distinguishes E and X with non-negligible advantage ε. Let $\alpha = (g, u, v, w)$ and $\vec{E}_l = (g^*, A_1^*, A_2^*, \ldots, A_k^*, g^{b^*}, C_1^*, C_2^*, \ldots, C_k^*)$ where $b^* \in_R \mathbb{Z}_q$ and

$$(A_i^*, C_i^*) = \begin{cases} ((g^*)^{a_i^*}, v^{a_i^*}), a_i^* \in_R \mathbb{Z}_q & \text{if } i \in \{1, \ldots, l\} \\ ((g^*)^{a_i^*}, R_i), a_i^* \in_R \mathbb{Z}_q, R_i \in_R \mathbb{G}_q & \text{if } i \in \{l+1, \ldots, k\} \end{cases}.$$

Note that $\vec{E}_k = E$ and $\vec{E}_0 = X$. If α is chosen from Y_1, then

$$\Pr_{\alpha \in Y_1}[\mathcal{D}'(\alpha) = 1] = \Pr[\mathcal{D}'(Y_1) = 1] = \frac{1}{k} \sum_{l=1}^{k} \Pr[\mathcal{D}(\vec{E}_l) = 1].$$

If α is chosen from Y_2, then

$$\Pr_{\alpha \in Y_2}[\mathcal{D}'(\alpha) = 1] = \Pr[\mathcal{D}'(Y_2) = 1] = \frac{1}{k} \sum_{l=0}^{k-1} \Pr[\mathcal{D}(\vec{E}_l) = 1].$$

Therefore, we have

$$\begin{aligned} \Pr[\mathcal{D}'(Y_1) = 1] - \Pr[\mathcal{D}'(Y_2) = 1] &= \frac{1}{k}(\sum_{l=1}^{k} \Pr[\mathcal{D}(\vec{E}_l) = 1] - \sum_{l=0}^{k-1} \Pr[\mathcal{D}(\vec{E}_l) = 1]) \\ &= \frac{1}{k}(\Pr[\mathcal{D}(\vec{E}_k) = 1] - \Pr[\mathcal{D}(\vec{E}_0) = 1]) \\ &= \frac{1}{k}(\Pr[\mathcal{D}(E) = 1] - \Pr[\mathcal{D}(X) = 1]) \\ &\geq \frac{\varepsilon}{k}. \end{aligned}$$

So we can solve the DDH problem with at least non-negligible advantage $\frac{\varepsilon}{k}$, which is a contradiction.

□

Theorem 6. *The sender's security of Scheme OT_n^k-III is unconditionally-secure. That is, for $i \notin \{\sigma_1, \sigma_2, \ldots, \sigma_k\}$, no receiver R can get information about messages m_i.*

Proof. Since $Z_i = C_0 C_1^i \cdots C_{k-1}^{i^{k-1}} (gh)^{i^k} = g^{f^*(i)b^*} h^{f'^*(i)}$, the degree of $f'^*(x)$ is k. That is, there are at most k $f'^*(i)$'s equal to 0. Then for any other $f'^*(i) \neq 0$, we prove that $Z_i^{r_i} B^{s_i}$ is uniformly distributed in $\mathbb{G}_q$.

Let $\mathcal{I} = \{i \in \{1, 2, \ldots, n\} | f'^*(i) \neq 0\}$. For any $i \in \mathcal{I}$, we let $\tilde{a}_i = f^*(i) r_i + s_i$, and $e_i = \log_g h^{f'^*(i)}$. Then

$$\begin{aligned} Z_i^{r_i} B^{s_i} &= (g^{f^*(i)b} h^{f'^*(i)})^{r_i} g^{bs_i} \\ &= g^{(f^*(i)r_i + s_i)b} (h^{f'^*(i)})^{r_i} \\ &= g^{\tilde{a}_i b + e_i r_i}. \end{aligned}$$

- System parameters: $(g, H_1, H_2, \mathbb{G}_q)$;
- 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 $c_i = m_i \oplus H_2(h_i^x)$ for $i = 1, 2, \ldots, n$, where $h_i = H_1(i)$, and $x \in_R \mathbb{Z}_q^*$.
2. $S \longrightarrow R : c_1, c_2, \ldots, c_n$.

Transfer Phase

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

1. R chooses a random $a_j \in \mathbb{Z}_q^*$ and computes $h_{\sigma_j} = H_1(\sigma_j), A_j = (h_{\sigma_j})^{a_j}$.
2. $R \longrightarrow S : A_j$.
3. $S \longrightarrow R : D_j = (A_j)^x$.
4. R computes $K_j = (D_j)^{a_j^{-1}}$ and gets $m_{\sigma_j} = c_{\sigma_j} \oplus H_2(K_j)$.

Figure 4: Adpt-OT$_n^k$: Adaptive OT$_n^k$

Therefore, $Z_i^{r_i} B^{s_i}$ is uniformly distributed in $\mathbb{G}_q$ because $e_i \neq 0$ and r_i is uniformly distributed in $\mathbb{Z}_q$.

□

Complexity. OT$_n^k$-III has two rounds. The first round sends $2k+2$ messages and the second round sends n messages. For computation, R computes $4k+1$, and S computes $(2k+6)n$ modular exponentiations.

5 OT with adaptive queries

The queries of R in OT$_n^k$-II can be adaptive. In OT$_n^k$-II, the commitments c_i's of the messages m_i's of S to R are independent of the key masking. Therefore, our scheme OT$_n^k$-II is adaptive in nature and the number k of queries need not be prefixed. Our Adpt-OT$_n$ scheme is depicted in [Fig. 4].

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.

Theorem 7. *In Adpt-OT$_n^k$, R's choice are unconditionally secure.*

Proof. Since $\mathbb{G}_q$ is the group of prime order q, all elements except 1 in $\mathbb{G}_q$ are generators. So for any $A_j = h_j^{a_j}$ and any h_l, $l \neq j$, there is an a_l that satisfies $A_j = h_l^{a_l}$. That is, A_j can be a masked value of any index. Thus, the receiver's choices are unconditionally secure.

□

Theorem 8. *In the Adpt-OT_n^k, let $m_1, m_2, \ldots, m_n$ be messages committed in the commitment phase. For any receiver R, the number of messages which R can get is less than or equal to the number of R's queries in the transfer phase in the random oracle model.*

Proof. For any possible R, we construct a simulator R^* in the ideal model such that the outputs of R and R^* are indistinguishable:

1. In the commitment phase, R^* randomly chooses $c_1^*, c_2^*, \ldots, c_n^* \in \mathbb{G}_q$ and $x^* \in \mathbb{Z}_q^*$.
2. In the transfer phase, R^* simulates R on input $(c_1^*, c_2^*, \ldots, c_n^*)$, and gets message queries. For each query A_j, R^* returns $(A_j)^x$ to R. If R queries H_1 on index i, R^* returns a random $h_i^* \in \mathbb{G}_q$. If R queries H_2 on some K_i where
   - $K_i = (h_i^*)^x$ for some i, R^* sends i to the TTP T to obtain m_i and returns $c_i^* \oplus m_i$.
   - $K_i \neq (h_i^*)^x$ for all h_i^* have been queried to H_1, R^* returns a random value, and put $(K_i)^{x^{-1}}$ to the revocation list of H_1.

   Note that R^* uses a table for maintaining consistency of queries for each oracle. Moreover, R^* will not choose the values in the revocation list of H_1 as the answer of H_1 queries.
3. Output $(c_1^*, c_2^* \ldots, c_n^*, A_1^*, A_2^*, \ldots, A_k^*, D_1^*, D_2^*, \ldots, D_k^*)$. (We assume R makes k queries in the transfer phase: $A_1^*, A_2^*, \ldots, A_k^*$.)

Since R makes k queries in the transfer phase, we show that R gets k messages at most. Therefore we show that R obtains at most k decryption keys. In the above simulation, if R queries H_1, we return a random value output by the target oracle. When R queries A_i^*'s adaptively, we forward these queries to the helper oracle, and return the corresponding outputs. Finally, if R queries H_2 on legal $(h_i^*)^x$ for all $1 \leq i \leq k+1$, we can output $k+1$ pairs $((h_i^*)^x, i)$, 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 legal query $(h_{\sigma_j}^*)^x$, c_{σ_j} is consistent with the returned hash values, for $j = 1, 2, \ldots, k$. Since no other $(h_l^*)^{x^*}$, $l \neq \sigma_1, \sigma_2, \ldots, \sigma_k$, 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 R's output.

□

Complexity. In the commitment phase, S needs n modular exponentiations for computing the commitments c_i's. 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.

6 Conclusion

We have presented three very efficient OT_n^k schemes with perfect security of either receiver or sender. The first two OT_n^k schemes with perfect security of receiver are secure 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 for adaptive queries where the number of queries is unbounded. The essential technique is to reverse the order 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.

Acknowledgement

Research supported in part by Taiwan Information Security Center at NCTU (TWISC@NCTU), and National Science Council project NSC 95-2213-E-009-030 and NSC 96-2221-E-009-022.

References

[Bellare and Micali 1989] Bellare, M., Micali, S.: "Non-interactive oblivious transfer and applications"; in Proceedings of Advances in Cryptology - CRYPTO '89, volume 435 of LNCS, pp. 547-557, Springer-Verlag, 1989.

[Bellare et al. 2001] Bellare, M., Namprempre, C., Pointcheval, D., Semanko, M.: "Power of rsa inversion oracles and the security of Chaum's RSA-based blind signature scheme"; in Proceedings of Financial Cryptography (FC '01), volume 2339 of LNCS, pp. 319-338, Springer-Verlag, 2001.

[Bennett et al. 1991] Bennett, C. H., Brassard, G., Crépeau, C., Skubiszewska, M.-H.: "Practical quantum oblivious transfer"; in Proceedings of Advances in Cryptology - CRYPTO '91, volume 576 of LNCS, pp. 351-366, Springer-Verlag, 1991.

[Blundo et al. 2002] Blundo, C., D'Arco, P., Santis, A. D., Stinson, D.: "New results on unconditionally secure distributed oblivious transfer"; in Proceedings of Selected Areas in Cryptography - SAC '02, volume 2595 of LNCS, pp. 291-309, Springer-Verlag, 2002.

[Boldyreva 2003] Boldyreva, A.: "Threshold signatures, multisignatures and blind signatures based on the gap-die-hellman-group signature scheme"; in Proceedings of the Public Key Cryptography (PKC '03), volume 2567 of LNCS, pp. 31-46, Springer-Verlag, 2003.

[Boneh et al. 2005] Boneh, D., Goh, E.-J., Nissim, K.: "Evaluating 2-DNF formulas on ciphertexts"; in Proceedings of the 2nd Theory of Cryptography Conference (TCC 2005), volume 3378 of LNCS, pp. 325-341, Springer-Verlag, 2005.

[Brassard et al. 1986a] Brassard, G., Crépeau, C., Robert, J.-M.: "All-or-nothing disclosure of secrets"; in Proceedings of Advances in Cryptology - CRYPTO '86, volume 263 of LNCS, pp. 234-238, Springer-Verlag, 1986.

[Brassard et al. 1986b] Brassard, G., Crépeau, C., Robert, J.-M.: "Information theoretic reductions among disclosure problems"; in Proceedings of 27th Annual Symposium on Foundations of Computer Science (FOCS '86), pp. 427-437, IEEE, 1986.

[Brassard et al. 1996] Brassard, G., Crépeau, C., Sántha, M.: "Oblivious transfers and intersecting codes"; IEEE Transactions on Information Theory, 42(6):1769-1780, IEEE, 1996.

[Cachin et al. 1998] Cachin, C., Crepeau, C., Marcil, J.: "Oblivious transfer with a memory-bounded receiver"; in Proceedings of 39th Annual Symposium on Foundations of Computer Science (FOCS '98), pp. 493-502, IEEE, 1998.

[Chen and Zhu 2003] Chen, Z., Zhu, H.: "Quantum m-out-of-n oblivious transfer"; Technical report, arXiv:cs.CR/0311039, 2003.

[Chu and Tzeng 2005] Chu, C.-K., Tzeng, W.-G.: "Efficient k-out-of-n oblivious transfer schemes with adaptive and non-adaptive queries"; in Proceedings of the Public Key Cryptography (PKC '05), volume 3386 of LNCS, pp. 172-183, Springer-Verlag, 2005.

[Ding 2001] Ding, Y. Z.: "Oblivious transfer in the bounded storage model"; in Proceedings of Advances in Cryptology - CRYPTO '01, volume 2139 of LNCS, pp. 155-170, Springer-Verlag, 2001.

[Even et al. 1985] Even, S., Goldreich, O., Lempel, A.: "A randomized protocol for signing contracts"; Communications of the ACM, 28(6):637-647, ACM, 1985.

[Goldreich and Vainish 1987] Goldreich, O., Vainish, R.: "How to solve any protocol problem - an efficiency improvement"; in Proceedings of Advances in Cryptology - CRYPTO '87, volume 293 of LNCS, pp. 73-86, Springer-Verlag, 1987.

[Ishai et al. 2003] Ishai, Y., Kilian, J., Nissim, K., Petrank, E.: "Extending oblivious transfers efficiently"; in Proceedings of Advances in Cryptology - CRYPTO '03, volume 2729 of LNCS, pp. 145-161, Springer-Verlag, 2003.

[Kilian 1988] Kilian, J.: "Founding cryptography on oblivious transfer"; in Proceedings of the 20th Annual ACM Symposium on the Theory of Computing (STOC '88), pp. 20-31, ACM, 1988.

[Lipmaa] Lipmaa, H.: "Oblivious transfer or private information retrieval"; `http://www.tcs.hut.fi/helger/crypto/link/protocols/oblivious.html`.

[Lipmaa 2005] Lipmaa, H.: "An oblivious transfer protocol with log-squared communication"; in Proceedings of 8th Information Security Conference (ISC '05), volume 3650 of LNCS, pp. 314-328, Springer-Verlag, 2005.

[Mu et al. 2002] Mu, Y., Zhang, J., Varadharajan, V.: "m out of n oblivious transfer"; in Proceedings of the 7th Australasian Conference on Information Security and Privacy (ACISP '02), volume 2384 of LNCS, pp. 395-405, Springer-Verlag, 2002.

[Naor and Pinkas 1999a] Naor, M., Pinkas, B.: "Oblivious transfer and polynomial evaluation"; in Proceedings of the 31th Annual ACM Symposium on the Theory of Computing (STOC '99), pp. 245-254, ACM, 1999.

[Naor and Pinkas 1999b] Naor, M., Pinkas, B.: "Oblivious transfer with adaptive queries"; in Proceedings of Advances in Cryptology - CRYPTO '99, volume 1666 of LNCS, pp. 573-590, Springer-Verlag, 1999.

[Naor and Pinkas 2000] Naor, M., Pinkas, B.: "Distributed oblivious transfer"; in Proceedings of Advances in Cryptology - ASIACRYPT '00, volume 1976 of LNCS, pp. 200-219, Springer-Verlag, 2000.

[Naor and Pinkas 2001] Naor, M., Pinkas, B.: "Efficient oblivious transfer protocols"; in Proceedings of the 12th Annual Symposium on Discrete Algorithms (SODA '01), pp. 448-457, ACM/SIAM, 2001.

[Naor and Reingold 1997] Naor, M., Reingold, O.: "Number-theoretic constructions of efficient pseudo-random functions"; in Proceedings of 38th Annual Symposium on Foundations of Computer Science (FOCS '97), pp. 458-467, IEEE, 1997.

[Niemi and Renvall 1994] Niemi, V., Renvall, A.: "Cryptographic protocols and voting"; in Results and Trends in Theoretical Computer Science, volume 812 of LNCS, pp. 307-317, Springer-Verlag, 1994.

[Ogata and Kurosawa 2004] Ogata, W., Kurosawa, K.: "Oblivious keyword search"; Journal of Complexity, 20(2-3):356-371, 2004.

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

[Salomaa and Santean 1990] Salomaa, A., Santean, L.: "Secret selling of secrets with several buyers"; Bulletin of the European Association for Theoretical Computer Science (EATCS), 42:178-186, 1990.

[Stadler 1996] Stadler, M.: "Publicly verifiable secret sharing"; in Proceedings of Advances in Cryptology - EUROCRYPT '96, volume 1070 of LNCS, pp. 190-199, Springer-Verlag, 1996.

[Stern 1998] Stern, J. P.: "A new and ecient all or nothing disclosure of secrets protocol"; in Proceedings of Advances in Cryptology - ASIACRYPT '98, volume 1514 of LNCS, pp. 357-371, Springer-Verlag, 1998.

[Tzeng 2004] Tzeng, W.-G.: "Efficient 1-out-of-n oblivious transfer schemes with universally reusable parameters"; IEEE Transactions on Computers, 53(2):232-240, IEEE, 2004.

[Wu et al. 2003] Wu, Q.-H., Zhang, J.-H., Wang, Y.-M.: "Practical t-out-n oblivious transfer and its applications"; in Proceedings of 5th International Conference on Information and Communications Security (ICICS'03), volume 2836 of LNCS, pp. 226-237, Springer-Verlag, 2003.

[Yao 1986] Yao, A. C.-C.: "How to generate and exchange secrets"; in Proceedings of 27th Annual Symposium on Foundations of Computer Science (FOCS '86), pp. 162-167, IEEE, 1986.