Efficient k-out-of-n oblivious transfer protocol

Wang QingLong[1,2]

[1] *School of Information Engineering, Chang'an University, Xi'an 710064, Shaanxi province, P. R. China;*
[2] *Department of Mathematic, University of Cincinnati, Cincinnati 45220, Ohio, USA;*

Abstract: A new k-out-of-n oblivious transfer protocol is presented in this paper. The communication cost of our scheme are n+1 messages of sender to receiver and k messages from the receiver to sender. To the best knowledge of the authors, the communication complexity of our scheme is the least. Also, our scheme has a lower computation cost with (k+1)n modular exponentiations for sender and 3k modular exponentiations for the receiver. The security of our scheme is only based on the Decision Diffie-Hellman assumption. Further, we proved the sender's computational security and the receiver's unconditional security under standard model.

Keywords: two party computation, oblivious transfer, DDH assumption

1 Introduction

Nowadays, cryptography has been used to implement schemes for varies purposes in digital world and many cryptographic theories and technologies have been proposed. Oblivious transfer （OT）protocol is one of the most important cryptographic technologies which is designed for varies application such as secret exchange, contract signing, private information retrieval, oblivious search, oblivious database queries and secure function evaluation[1-4], etc. Also, OT is an important foundation in cryptography used in many other cryptography protocols [3,5,6,10,11].

OT is such a two-party protocol that includes a sender, S, and a receiver, R. Rabin firstly introduced an OT protocol[7] in which S sends a message to R and would like R get it with probability $1/2$. Different with [7], 1-out-of-n OT (OT_2^1)[8, 9, 10] is such a protocol in which S sends two messages to R and wants he exactly obtains one of them at his choice, meanwhile S remains oblivious to R's choice. Shortly after, Brassard, Crépeau and Robert proposed the 1-out-of-n OT (OT_n^1)[11, 12, 23, 24] which is an extension of OT_2^1. The k-out-of-n OT (OT_n^k) is the most general case and was firstly presented by Bellare and Micali[13]. Since then OT_n^k became the hot research field and many paper were published [14-22, 25-28].

A trivial solution for OT_n^k is running OT_n^1 k times. Naor and Pinkas firstly presented an non-trivial OT_n^k which is constructed by invoking a basic OT_2^1 several times. Mu et.al proposed three OT_n^k schemes[14] which have been showed unsatisfying the privacy of OT[27]. In 2009, Chang and Lee presented another OT_n^k scheme[20] based on RSA and Chinese Remainder Theorem which also has been found to violate the receiver's privacy[19]. Zhang and Wang presented two provably secure 2-pass OT_n^k schemes[26]. However, we found that their second scheme is totally insecure because receiver can get all encryption keys by the same way as the sender produces them, because the sender do not use any secret information when he produces the encryption keys. Chu and Tzeng also presented two 2-passes OT_n^k schemes[17, 28]. Chou pointed out that their second scheme $\mathrm{OT}_n^k - \mathrm{II}$ was the most efficient one[19]. But the security of $\mathrm{OT}_n^k - \mathrm{II}$ was based on random oracle model and built on the assumptions not only DDH problem but also collision resistant hash function. The first scheme $\mathrm{OT}_n^k - \mathrm{I}$ was only built on the DDH assumption and was secure under standard model. However, it has a higher communication cost than $\mathrm{OT}_n^k - \mathrm{II}$. In [19, 24, 25], the authors proposed several OT_n^k schemes based on bilinear pairings. Other than the computational complexity of bilinear pairings, [19,24] also involved the third party which made them less practical.

In this paper, we present a new OT_n^k scheme which has the most efficient communication cost to date. The security of our scheme is built only on the assumption of DDH problem and proved under standard model. Although our scheme is constructed based on the $\mathrm{OT}_n^k - \mathrm{I}$ scheme of [17], it greatly improves the efficiency of both communication cost and computation complexity.

The rest of this paper is organized as follows: Section 2 introduces the related primitives used later. Section 3 proposes our k-out-of-n protocol. The efficiency of our scheme is given in section 4. Section 5 concludes this paper.

2 Definition

2.1 Primitive

Computationally indistinguishablity: Two probability ensembles $\{X_i\}$ and $\{Y_i\}$, indexed by i, are computationally

email: ql_wang@outlook.com

indistinguishable if for any polynomial-time-bounded probabilistic Turing machines (PPTM D), polynomial p(n) and sufficiently large i, it holds that $|\Pr[\mathrm{D}(X_i=1)]-\Pr[\mathrm{D}(Y_i=1)]|\le 1/\mathrm{p}(i)$.

Diffie-Hellman assumptions: Let p,q be two big primes and satisfy $p=2q+1$ and G_q be a subgroup of Z_p^* with order q. We shorten $g^x \bmod p$ as g^x. Then the Decisional Diffie--Hellman (DDH) assumption is that the following two distribution ensembles are computationally indistinguishable, for any $g \in G_q \setminus \{1\}$ and any $a,b,c \in_R Z_q$:

$$Y_1 = \left(g, g^a, g^b, g^{ab}\right)$$

$$Y_2 = \left(g, g^a, g^b, g^c\right)$$

2.2 K-out-of-n OT protocol

OT_n^k is a two party protocol. The sender S has n messages $m_1,...,m_n$ and willing to leak arbitrary k messages to receiver while the receiver R has some choices $\{\sigma_1,...,\sigma_k\} \subset \{1,...,n\}$. At the end of the protocol k-out-of-n, R obtains the k messages $m_{\sigma_1},...,m_{\sigma_k}$.

The secure requirements of OT_n^k can be described as:

- Receiver's privacy: Alice should not be able to learn any about which k messages Bob has selected.
- Sender's privacy: Bob should not be able to learn any about the remaining $n-k$ messages that he did not select.

In an oblivious transfer scheme, a party's behavior might be semi-honest or malicious. By a semi-honest party, it means that the party will follow the OT protocol honestly, but tries to get extra information from received messages. By a malicious party it means that the party can arbitrarily deviate from the protocol. There are several different secure definitions for oblivious transfer protocol such as semi-honest (also called honest but curious) model[17], hasf-simulation model[16] and fully-simulation model[8,29]. In this paper, we only consider the semi-honest model same as the first scheme of [17].

3 Proposed k-out-of-n protocol

The proposed k-out-of-n protocol is as follow:

- System parameters: $\left(g,h,G_q,p\right)$, where p,q are two large primes and satisfy $p=2q+1$. g and h are two different generators of group G_q. It is assumed that the DDH problem is difficult in G_q.
- S has n messages: $m_1,m_2,...,m_n$ where $m_i \in G_q$, $i=[1,n]$.
- $R's$ choices: $\{\sigma_1,\sigma_2,...,\sigma_k\} \subset \{1,2,...,n\}$.

step1. R chooses two polynomials $f(x)=a_0+a_1x+a_2x^2+...+a_{k-1}x^{k-1}+x^k$ where $a_0,a_1,...,a_{k-1} \in_R Z_q$ and $f'(x)=(x-\sigma_1)(x-\sigma_2)...(x-\sigma_k) \bmod q = b_0+b_1x+...+b_{k-1}x^{k-1}+x^k$.

step2. $R \to S$: $A_0 = g^{a_0}h^{b_0} \bmod p, ..., A_{k-1} = g^{a_{k-1}}h^{b_{k-1}} \bmod p$

step3. S randomly selects $r \in \mathbb{Z}_q$ and computes $c_i = m_i B_i \bmod p$ where

$B_i = g^{rf(i)}h^{rf'(i)} = \left(A_0A_1^iA_2^{i^2}...A_{k-1}^{i^{k-1}}(gh)^{i^k}\right)^r \bmod p$ for $i=1,2,...,n$.

step4. $S \to R$: $g^r, c_1, c_2, ..., c_n$

step5. R computes $m_{\sigma_i} = c_{\sigma_i}\left(\left(g^r\right)^{f(\sigma_i)}\right)^{-1} \bmod p$ for each $\sigma_i, 1 \le i \le k$, where $\left(\left(g^r\right)^{f(\sigma_i)}\right)^{-1}\left(\left(g^r\right)^{f(\sigma_i)}\right) = 1 \bmod p$.

3.1 proof of correctness

Proof: from step3, we have

$c_i = m_iB_i = m_ig^{rf(i)}h^{rf'(i)} = \bmod p$, $i=1,2,...,n$.

from step5, we have

$$c_{\sigma_i}\left(\left(g^r\right)^{f(\sigma_i)}\right)^{-1} = m_{\sigma_i}g^{rf(\sigma_i)}h^{rf'(\sigma_i)}\left(\left(g^r\right)^{f(\sigma_i)}\right)^{-1} = m_{\sigma_i}g^{rf(\sigma_i)}\left(\left(g^r\right)^{f(\sigma_i)}\right)^{-1} = m_{\sigma_i}g^{rf(\sigma_i)}\left(g^{rf(\sigma_i)}\right)^{-1} = m_{\sigma_i} \bmod p$$

3.2 Proof of Security

Theorem1. R's choices are unconditionally secure.

Proof: it can be easily seen that for every choices $\left(\sigma_1^{'},\sigma_2^{'},...,\sigma_k^{'}\right)$, which determines a k degree function, $f_1^{'}(x)=\left(x-\sigma_1^{'}\right)\left(x-\sigma_2^{'}\right)...\left(x-\sigma_k^{'}\right)=b_0^{'}+b_1^{'}x+...+b_{k-1}^{'}x^{k-1}+x^k \bmod q$, exists a k degree function $f_1(x)=a_0^{'}+a_1^{'}x+a_2^{'}x^2+...+a_{k-1}^{'}x^{k-1}+x^k$ satisfying $A_i=g^{a_i^{'}}h^{b_i^{'}} \bmod q, 0\le i\le k-1$. So, the Receiver's secure is unconditional.

Theorem 2. If the assumption of DDH is true and the receiver is semi-honest, then the advantage of receiver getting m_i where $i\notin\{\sigma_1,...,\sigma_k\}$ is negligible.

Proof: if receiver can get any other message with non-negligible advantage ε then we can distinguish DDH with the same advantage ε.

Assume the algorithm that receiver used to get other message is $\mathcal{A}$, then we have an algorithm $\mathcal{B}$ to distinguish DDH by using $\mathcal{A}$ as a subroutine.

Let the input of $\mathcal{B}$ is (g,u,v,w) from either Y_1 or Y_2. $\mathcal{B}$ constructs a modified system parameters as $\left(g_1,g_2,h_1,h_2,G_q,p\right)$ where $g_1=g,\ g_2=u,\ h_1=v,h_2=w$. Then $\mathcal{B}$ runs the OT protocol with receiver as follows:

step1. R chooses two polynomials $f(x)=a_0+a_1x+a_2x^2+...+a_{k-1}x^{k-1}+x^k$ where $a_0,a_1,...,a_{k-1}\in_R Z_q$ and $f^{'}(x)=(x-\sigma_1)(x-\sigma_2)...(x-\sigma_k)\bmod q=b_0+b_1x+...+b_{k-1}x^{k-1}+x^k$.

step2. $R\to\mathcal{B}$: $A_0=g_2^{a_0}h_2^{b_0}, A_1=g_2^{a_1}h_2^{b_1},..., A_{k-1}=g_2^{a_{k-1}}h_2^{b_{k-1}}$

step3. $\mathcal{B}$ randomly selects $r\in\mathbb{Z}_q$ and computes $c_i=m_iB_i \bmod p$ where

$B_i=g_2^{rf(i)}h_2^{rf^{'}(i)}=\left(A_0A_1^iA_2^{i^2}...A_{k-1}^{i^{k-1}}g_2^{i^k}h_2^{i^k}\right)^r \bmod p$, for $i=1,2,...,n$

step4. $\mathcal{B}\to R$: $g_2^r=g_1^{ar}$ (we can see ar as a random number $r^{'}\in Z_q$), $c_1,c_2,...,c_n$.

step5. $R\to\mathcal{B}$: any $k+1$ messages $\left\{m_{\beta_1},...,m_{\beta_{k+1}}\right\}\subseteq\{m_1,...,m_n\}$.

If $k+1$ messages are all correct, $\mathcal{B}$ outputs 1 else outputs 0. (it is obliviously that $\mathcal{B}$ will output 1 with probability $1/q$ if R gets other messages only through guess).

Here, if (g,u,v,w) is from Y_1, we have $B_i=g_2^{rf(i)}h_2^{rf^{'}(i)}=u^{rf(i)}w^{rf^{'}(i)}=g^{arf(i)}g^{abrf^{'}(i)}=\left(g_1^{f(i)}h_1^{f^{'}(i)}\right)^{ar}$ which are well-formed data for $i=1,2,...,n$. So, receiver can get k messages he selected as normal and the other message with advantage ε over $1/q$ by using $\mathcal{A}$. Else if (g,u,v,w) is from Y_2, we have $B_i=g_2^{rf(i)}h_2^{rf^{'}(i)}=u^{rf(i)}w^{rf^{'}(i)}=g^{arf(i)}g^{a^{'}brf^{'}(i)}\ne\left(g_1^{f(i)}h_1^{f^{'}(i)}\right)^{ar}$ which are not valid data. Since r is randomly selected B_i is uniformly distributed over G_p. Thus receiver will get the information of other message with probability $1/q$. It is noticed that receiver can still get the k messages he selected in this case.

Finally, if $\mathcal{B}$ output 1 with probability great than $\varepsilon+1/q$, then $\mathcal{B}$ will conclude that (g,u,v,w) is from Y_1. If $\mathcal{B}$ output 1 with probability less than $\varepsilon+1/q$, then $\mathcal{B}$ will conclude that (g,u,v,w) is from Y_2. Thus $\mathcal{B}$ can distinguish DDH with a non-negligible probability.

4 Efficiency

In an oblivious transfer scheme, the performance criteria involve sender's computational effort and receiver's computational effort as well as the communicational cost between the sender and the receiver. The communicational cost is measured mainly by three factors: (1) the number of passes (or rounds) between sender and receiver, (2) the number of transferred messages from sender to receiver, (3) the number of transferred messages from receiver to sender. The computation complexity is mainly determined by exponentiation operator in an oblivious transfer scheme. Our scheme has two passes. Receiver computes $3k$ modular exponentiations and sends k messages to sender in the first pass. Sender computes $(k+1)n$ modular exponentiations and comes back $n+1$ messages to receiver.

A comparison of communication cost and computational complexity between our scheme and other correct two pass OT_n^k protocols are given in Table 1. It is clearly that our scheme is most efficient on communication cost among them. While the $\mathrm{OT}_n^k - \mathrm{II}$ scheme of [17] has less computational complexity it depends on both DDH and collision resistant assumption and the security is proved under random oracle model. [19, 25] need to compute bilinear pairings besides the model exponentiations and scalar multiplying which has more computational complexity than ours.

Table 1 Our Scheme vs Other Two Passes Schemes

Protocol	Message S→R	Message R→S	Computational complexity S	Computational complexity R
Ours	n+1	k	(k+1)n	3k
[17]- I	2n	k	(k+2)n	3k+2
[17]- II	n+k	k	n+k	2k
[19]	n+k	k+2	n*	kn*
[25]	n+k	n+k+1	n*+n	k*+k
[26]-1	2n	k+3	(k+4)n+1	2k+3

*computation of bilinear pairing

5 Conlusion

In this paper, we proposed a new OT_n^k protocol. Although it is based on the work of [17], our scheme greatly improved the communication cost and computational complexity. As we know our scheme is the most efficient OT_n^k protocol as for communication cost. The security of our scheme is only based on the DDH assumption and security is proved under standard model. In future, we will focus on to design new two passes k-out-of-n protocol with less computational complexity.

Reference

[1] Shimon E, Oded G, Abraham L. A Randomized Protocol for Signing Contracts. Communication, 1985, 28(6): 637–647.
[2] Wakaha O, Kaoru K. Oblivious Keyword Search. Journal of Complexity, 2004, 20(2-3): 356–371.
[3] Oded G, Ronen V. How To Solve Any Protocol Problem-extended abstract. CRYPTO ’87. California, Santa Barbara, USA: Springer press, 1988: 73 - 86.
[4] Aiello B, Ishai Y, Reingold O. Priced Oblivious Transfer: How To Sell Digital Goods. EUROCRYPT 2001. Innsbruck, Austria: Springer press, 2001: 119–135.
[5] Kilian J. Founding Cryptography on Oblivious Transfer. STOC ’88. Chicago, Illinois, USA: ACM press, 1988: 20-31.
[6] Mummoorthy M, WEI Jiang, Ahmet E, Serkan U. Homomorphic Encryption Based k-out-of-n Oblivious Transfer Protocols. http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=2721&context=cstech
[7] Michael O. How To Exchange Secrets by Oblivious Transfer. Technical Report TR-81, Aiken Computation Laboratory, Harvard University, 1981.
[8] Andrew Y. Efficient Fully-simulatable Oblivious Transfer. CT-RSA 2008. San Francisco, California, USA: Springer press, 2008: 52-70.
[9] M Naor, B Pinkas. Efficient Oblivious Transfer Protocols. SODA ’01. Washington DC, USA: ACM press, 2001: 448-457.
[10] Peikert C, Vaikuntanathan V, Waters B. A Framework for Efficient and Composable Oblivious Transfer. CRYPTO 2008. Santa Barbara, California, USA: Springer press, 2008: 554-571.
[11] Ishai Y, Prabhakaran M, Sahai A: Founding Cryptography on Oblivious Transfer - Efficiently. CRYPTO 2008. Santa Barbara, California, USA: Springer press, 2008: 572-591
[12] Brassard G, Cr´epeau C, S´antha M. Oblivious Transfers and Intersecting Codes. IEEE Transactions on Information Theory, 1996, 42(6): 1769-1780, IEEE.
[13] Bellare M, Micali S. Non-interactive Oblivious Transfer and Applications. CRYPTO ’89. California, Santa Barbara, USA: Springer press, 1989: 547-557.
[14] MU Yi, ZHANG Junqi, Varadharajan V. m out of n Oblivious Transfer. ACISP ’02. Melbourne, Victoria, Austrialia: Springer press, 2002: 395-405.
[15] WU Qianhong, ZHANG Jianhong, WANG Yumin. Practical t-out-n oblivious transfer and its applications. ICICS’03. Singapore: Springer press, 2003: 226-237.
[16] M Naor, B Pinkas. Computationally Secure Oblivious Transfer. Journal of Cryptology , 2005, 18(1): 1-35.
[17] Cheng-kang C, Wen-guey T. Efficient k-out-of-n Oblivious Transfer Schemes. Journal of Universal Computer Science, 2008, 14(3): 397–415.
[18] Mummoorthy M, WEI Jiang, Ahmet E, Serkan U. k-out-of-n Oblivious Transfer Based on Homomorphic Encryption and Solvability of Linear Equations. CODASPY '11. San Antonio, Texas, USA: ACM press, 2011: 169-178.
[19] Jue-sam C, A Novel k-out-of-n Oblivious Transfer Protocol from Bilinear Pairing. Advances in Multimedia, 2012,2012 (2012):1- 9.

[20] Chin-chen C, Jung-san L. Robust t-out-of-n Oblivious Transfer Mechanism Based on CRT. Journal of Network and Computer Applications, 2009, 32(1): 226–235.
[21] MA Xu; XU Lingling; ZHANG, Fangguo. Oblivious Transfer with Timed Release Receiver's Privacy. Journal of Systems and oftware, 2001, 84(3): 460–464.
[22] Jain A, Hari C. A New Efficient Protocol for k-out-of-n Oblivious Transfer. Cryptologia, 2010, 34(4): 282-290.
[23] Parakh A. Oblivious Transfer Based on Key Exchange. Cryptologia, 2008, 32(1):37–44.
[24] QIN Jing. k out of n Oblivious Transfer Protocols from Bilinear Pairings. Journal Of Software, 2009, 5(1), 65-71.
[25] Ya-lin C, Jue-sam C, Xian-wu H. A Novel k-out-of-n Oblivious Transfer Protocols Based on Bilinear Pairings. e-print IACR archive, 2010, http://eprint.iacr.org/2010/027.pdf
[26] ZHANG Jianhong, WANG Yumin. Two Provably Secure k-out-of-n Oblivious Transfer Schemes. Applied Mathematics and Computation, 2005, 169(2): 1211-1220.
[27] Ghodosi H and Zaare-Nahandi R. Comments on The 'm out of n oblivious transfer'. Information Processing Letters, 2006, 97(4): 153–155.
[28] Cheng-kang C, Wen-guey T. Efficient k-out-of-n Oblivious Transfer Schemes with Adaptive and Non-adaptive Queries. PKC '05. "Les Diablerets" Switzerland: Springer press, 2005: 172–183.
[29] Jan Camenisch, Gregory Neven, Abhi Shelat Simulatable Adaptive Oblivious Transfer. EUROCRYPT 2007. Barcelona, Spain, Springer-verlag, 2007, vol.4514: 573-590