A novel k-out-of-n Oblivious Transfer Protocols Based on Bilinear Pairings

Yalin Chen[1], *Jue-Sam Chou[2], Xian-Wu Hou[3]
[1]Institute of Information Systems and Applications, National Tsing Hua University, Taiwan, R.O.C
d949702@oz.nthu.edu.tw
Tel: 886+3+5738997, Fax: 886+3+5723694
[2] Department of Information Management, Nanhua University, Taiwan, R.O.C
jschou@mail.nhu.edu.tw
[3] Department of Information Management, Nanhua University, Taiwan, R.O.C
g4161509@mail2.nhu.edu.tw

*: corresponding author

Abstract

Low bandwidth consumption is an important issue in a busy commercial network whereas time may not be so crucial, for example, the end-of-day financial settlement for commercial transactions in a day. In this paper, we construct a secure and low bandwidth-consumption k-out-of-n oblivious transfer scheme based on bilinear pairings. We analyze the security and efficiency of our scheme and conclude that our scheme is more secure and efficient in communication bandwidth consumption than most of the other existing oblivious transfer schemes that we know.

1. Introduction

Since Oblivious transfer (OT) has an important feature that the sender cannot know which part of the transmitted messages the receiver will obtain and the receiver cannot learn extra messages other than the ones he chosen in advance, it has become an important primitive for designing secure protocol to provide privacy protection. The original OT was proposed by Rabin [20] in 1981. In the scheme, Alice sends a bit to Bob and Bob only has 1/2 probability to obtain the bit. Subsequently, many flavors of OT schemes were proposed such as, 1-out-of -2 OT (OT_2^1) [1,2,17,21,22], 1-out-of-n OT(OT_n^1)[13,24,25], k-out-of-n OT (OT_n^k) [5,8,9,11,12,18], adaptive

OT_n^k [10,15], and non-interactive OT [23,26,27]. In 1985, Even et al.[22] first proposed a general 1-out-of-2 OT (OT_2^1) scheme, in which the sender sends two messages to the receiver, and the receiver can receive only one of them. In 1987, Crepeau [3] proved that Rabin's OT [20] and Even et al.'s OT_2^1 [22] are computationally equivalent. The extension of OT_2^1 is 1-out-of-n OT (OT_n^1) in which the sender sends n messages to the receiver, and the receiver can learn only one of them. The more general form is k-out-of-n OT (OT_n^k), in which the sender sends n messages to the receiver, and the receiver can obtain k of them. Most previous OT_n^1 schemes cannot be used to construct an OT_n^k scheme easily. Hence, for constructing an OT_n^k scheme, an OT_n^1 scheme must be run k times. In an adaptive OT_n^k, the sender sends n messages to the receiver, and the receiver can learn k of them in an adaptive manner. Another form of OT is non-interactive OT. It is a variation of interactive OT scheme. In it, the receiver doesn't need to communicate with the sender since he had chosen the message wished in advance in the setup phase.

During 1999 to 2001, Naor et al. proposed some related OT works such as, adaptive OT_k^n [18], proxy OT_1^2 [31], distributed OT_k^n [14], efficient OT_1^n [32], and efficient OT_k^n [339]. In 2000, Naor et al. [14] proposed two efficient distributed OT_1^2 schemes in which the sender Alice's task is to distribute his messages among a set of servers and the chooser's task is to make contact with k (k<n) servers to get one of these messages. They claimed that their scheme can protect both parties in an information theoretic sense. However in 2007, Ghodosi [8] showed that their schemes fails since they don't protect the chooser/sender in the information theoretic sense. In 2002, Mu et al. [26] proposed three m-out-of n OT schemes. Two of them are interactive and the other can be used to construt either interactive or non-interactive. They claimed that their schemes are complete, robust, and flexible. However in 2006, Ghodosi et al. [29] showed that their schemes fail to satisfy the requirement of the oblivious transfer. In 2004, Wang et al.[5], presented an efficient OT_n^k scheme which can conceal all sender's secrets and greatly reduce the sender's communication cost.

In 2005, Huang et al.[9], proposed an efficient t-out-of-n OT. They claimed that their scheme is efficient than all existing OT schemes. However, their scheme has three rounds. This means their scheme is less efficient in the number of passes. In the same year, Zhang et al.s'[12], proposed two efficient t-out-of-n OT schemes. Both are based on DDH assumption. They claimed that both of their schemes are provably secure under the Decisional Diffie–Hellman (DDH) assumption. However, we found that $C_{k-1} \neq (-\delta_1 - \delta_2, \ldots, -\delta_k)$ in their first scheme. Also, in 2005, Chu, et al [4] proposed two efficient k-out-of-n oblivious transfer schemes with adaptive and non-adaptive, respectively. Their schemes are mainly based on the discrete logarithm problem. They claimed that their schemes are more efficient than all the previous proposed. In 2006, Parakh [1] proposed an OT_2^1 scheme based on Elliptic Curve Cryptography (ECC). But we found that A can decide whether B can obtain his secret n_A by first assuming that $P_A=P_B$. Under this assumption, he can obtain R in step2 and compute n_AR. Then, he can compute K=Q since n_B (n_AP_A)= n_A (n_BP_B) in step 5a. That is, although A doesn't know n_B, he can compute K, and n_BK (in step 5b)= n_B n_AR= n_A(n_B R), as B does, where (n_B R) is trasferred in step2 by B. Therefore, if A can obtain Z_B = Pn_A after the result of step 5b, A knows that $P_A=P_B$ and n_A can be obtained by B. This violates B's secrecy. In the same year, Kim, et al.[23] proposed a new secure verifiable non-interactive oblivious transfer protocol using RSA. They claimed their scheme has the function of authenticating the sender and anyone can't deny the message he sent. But we found their protocol is vulnerable to the impersonation attack. Since if an adversary E intercepts the messages sent from Alice, modifies X_A to X'_A ($\equiv(X'_0, X'_1)$), and then sends (X'_A,M_A,C_A) to Bob. Bob will verify him as authentic by using his private key d_B and the sender's public key e_A to decrypt C_A. Since C_A is the signature of M_A encrypted by Bob's public key, it has no relationship with X_A'. Hence, E can therefore successfully impersonate Alice. Moreover, in their scheme, there are two modulus, n_A and n_B. If they are not properly used, for example, if $n_A>n_B$, it will incur the re-blocking problem [30]. Also, in 2006, Zhang et al.[11] proposed two efficient t-out-of-n oblivious transfer schemes. They claimed that both of their schemes are efficient. However, it needs three rounds in the first scheme. In 2009, Jing et al. proposed two non-interactive OT_1^n schemes [34]. However in their protocols, when R wants to select one of the n messages sent from S every time, he has to interact with the third party T to obtain the choice-related secret key x_i. This makes their scheme somewhat inconvenient and inconsistent with the meaning of non-interactive protocols as indicated in the title. (This phenomenon can be found in other proposed non-interactive OT schemes as well.) Also in 2009, Chang [28] presented a robust OT_k^n scheme using both the RSA blind signature and Chinese

Remainder Theorem. However, we found that their scheme fails since the sender Alice is able to decide which part of the sent messages were chosen by the chooser Bob. We will describe this in Section 3.2.

Although, there are so many OT schemes proposed. However, due to lack of considering possible attacks that maybe encounter in an open network, all of them need run under a secure channel. This incurs extra communication overhead. Hence, for efficiency consideration in communicational bandwidth consumption, in this paper we propose a novel bilinear pairing based OT_n^k scheme which not only is secure but also possesses the property of low bandwidth consumption.

The rest of this paper is organized as follows. In Section 2, we show the relational work. In Section 3, we review Chang et al.'s protocol [28] then show their weakness. In Section 4, we present our protocol. And show the security analysis and the performance comparisons with other proposed works in Section 5. Finally, a conclusion is given in Section 6.

2 Preliminary

In 2001, bilinear pairings, namely the Weil pairing and the Tate pairing, defined on elliptic curves were proved and applied to cryptography by Boneh and Franklin in 2001 [7]. Since then, many protocols have been designed based on the Weil pairing [6,7,16] for easier key distribution consideration. In this section, we will briefly describe the basic definitions and properties of bilinear pairings.

2.1 Bilinear Pairings

Let P be a generator of G_1 that is a cyclic group whose order is a prime q, and G_2 be a cyclic multiplicative group of the same order q. It is assumed that the discrete logarithm problem (DLP) in both G_1 and G_2 is difficult. The security level of bilinear pairing is equal to the discrete logarithm problem [7] and a bilinear pairings is a map e:

$G_1 \times G_1 \rightarrow G_2$ with the following conditions.

(1) Bilinear: $e(aP,bQ) = e(P,Q)^{ab}$, for any $a,b \in Z_q^*$ and $P,Q \in G_1$.

(2) Computable: There is an efficient algorithm to compute (P, Q) for all, $P,Q \in G_1$.

(3) Non - degenerate: there exists $P \in G_1$ and $Q \in G_1$ such that $e(P,Q) \neq 1$ in G_2.

After showing what is a bilinear map, we first introduce the following problems in G_1:

– **Discrete Logarithm Problem (DLP):** Given two group elements P and Q, find an integer n, such that $Q = nP$ whenever such an integer exists.

– **Decision Diffie-Hellman Problem (DDHP):** For $a, b, c \in Z_q^*$, given P, aP, bP, cP, decide whether $c \equiv ab \bmod q$.

– **Computational Diffie-Hellman Problem (CDHP):** For $a, b \in Z_q^*$, given $P, aP, bP,$ compute abP.

– **Decisional Bilinear Diffie–Hellman Problem (DBDHP)**: Given P, aP, bP, cP for a, b, $c \in Z_q^*$ and $z \in G_2$, decide whether $z = e(P,P)^{abc}$.

3. Review of Chang et al.'s protocol

In 2009, Chang et al. proposed a robust OT_k^n scheme based on CRT, hoping that their scheme can achieve the requirements of general OT_k^n schemes. However, we found that their scheme can not satisfy the chooser's privacy. In the following, we first review the scheme in Section 3.1 then show the weakness in Section 3.2.

3.1 Review

We roughly list the steps of the protocol in following (see [28] for more details).

Step 1: After receiving the request sent by Bob for all messages $a_1, a_2, \ldots, a_n$, Alice selects n relatively prime integers, $d_1, d_2, \ldots, d_n$, and computes $D= d_1*d_2* \ldots *d_n$. He then constructs the congruence system

$C \equiv a_1 \bmod d_1$, $C \equiv a_2 \bmod d_2$,…, $C \equiv a_n \bmod d_n$

Furthermore, Alice computes the following values:

$T_1 = d_1^e \bmod N$, $T_2 = d_2^e \bmod N$, ..., $T_n = d_n^e \bmod N$,
using the public key e.

Finally, Alice publishes C and the pairs of (ID_i, T_i), for i=1 to n, in the public board.

Step 2: If Bob wants to learn the information possessed by Alice, then Bob must select t pairs of (ID'_j, T'_j), for j = 1 to t, from the public board and generate t corresponding random numbers $r_1, r_2, \ldots, r_t$, for each pair of (ID'_j, T'_j) first. Bob subsequently computes the following:

$\alpha_1 = r_1^e * T'_1 \bmod N$, $\alpha_2 = r_2^e * T'_2 \bmod N$,..., $\alpha_t = r_t^e * T'_t \bmod N$,
using Alice's public key e and then sends $\{\alpha_1, \alpha_2, \ldots, \alpha_t\}$ back to Alice.

Step 3: Upon receiving the messages sent by Bob, Alice employs the private key d to compute $\beta_1 = \alpha_1^d \bmod N$, $\beta_2 = \alpha_2^d \bmod N$, …, $\beta_t = \alpha_t^d \bmod N$, and then sends the results $\{\beta_1, \beta_2, \ldots, \beta_t\}$ to Bob.

Step 4: After receiving the messages sent by Alice, Bob computes the following values:

$d_1' = r_1^{-1} * \beta_1 \bmod N$, $d_2' = r_2^{-1} * \beta_2 \bmod N$, …, $d_t' = r_t^{-1} * \beta_t \bmod N$

Consequently, Bob learns the demanded messages successfully by computing $b_1 = C \bmod d_1'$, $b_2 = C \bmod d_2'$, …, $b_t = C \bmod d_t'$.

3.2 Weaknesses

Although, Chang et al. claimed that their scheme can achieve the requirements of general OT_k^n schemes. However, we found that the privacy of Bob has been violated. Since Bob has committed his t choices to the t values of α and the n d_i values are selected by Alice. Hence, after computing the t values of β_j s, Alice can use each of the n d_i^{-1}s to compute $r_k = \beta_j * d_i^{-1}$, for k=1 to n∗t. And for each r_k, Alice computes the n

$\alpha_i = (r_j * d_i)^e$ values to compare with the t committed values, where $1 \leqq i \leqq n$ and $1 \leqq j \leqq t$. Hence, we can easily see that it needs $n*t$ multiplications to obtain r_k, n^2*t multiplications to obtain $(r_j * d_t)$, and n^2*t exponentiation operations to determine α_j values, e.g., $\alpha_j = (r_k * d_t)^e$. Therefore, totally with at most $n^2*t + n*t$ multiplications and n^2*t exponentiations, Alice can decide which t values Bob selected. This violates Bob's privacy.

4. The proposed k-out-of-n OT scheme

In this session, we present a k-out-of n OT scheme based on bilinear pairing. Our scheme consists of two phases: (1) setup phase, (2) data transfer phase. The details of our protocol are executed as follows and also illustrated in Figure 1.

(1) Setup phase

Initially, there is a public system parameter set, $\{G_1, G_2, q, P, e, H\}$, where G_1 be a cyclic additive group generated by P whose order is a prime q , G_2 be a cyclic multiplicative group of the same order q, e is a bilinear pairing mapping e: $G_1 \times G_1 \rightarrow G_2$,and H be a one-way hash function $H: \{0,1\}^* \rightarrow G_1$. R is the receiver and S is the sender.

(2) Data transfer phase.

(a). R randomly chooses integers t, w, and n s_i *s* (for i=1,2,…,n). He then computes $A_i = ws_iP$, $B_j = ts_{\sigma j}P$ (for j=1,2,…,k) and V=tP, where σ_j is the k indices to represent k of the n random integers S_i, i=1 to n, chosen by R. Then R sends $A_1, A_2, \ldots, A_n, B_1, B_2, \ldots, B_k$ and V to S.

(b). After receiving the above sent message form R, S randomly chooses an integer r, computes $C_i = m_i \oplus H(e(A_i, V)^r)$ and $D_j = rB_j$. Then he sends C_i, $C_2, \ldots, C_n$, D_1, $D_2, \ldots$, D_k to R.

(c). After receiving C_1, $C_2, \ldots$, C_n, D_1, $D_2, \ldots$, D_k , R computes $c_{\sigma j} \oplus H(e(D_j, P)^w)$ to obtain $m_{\sigma j}$.

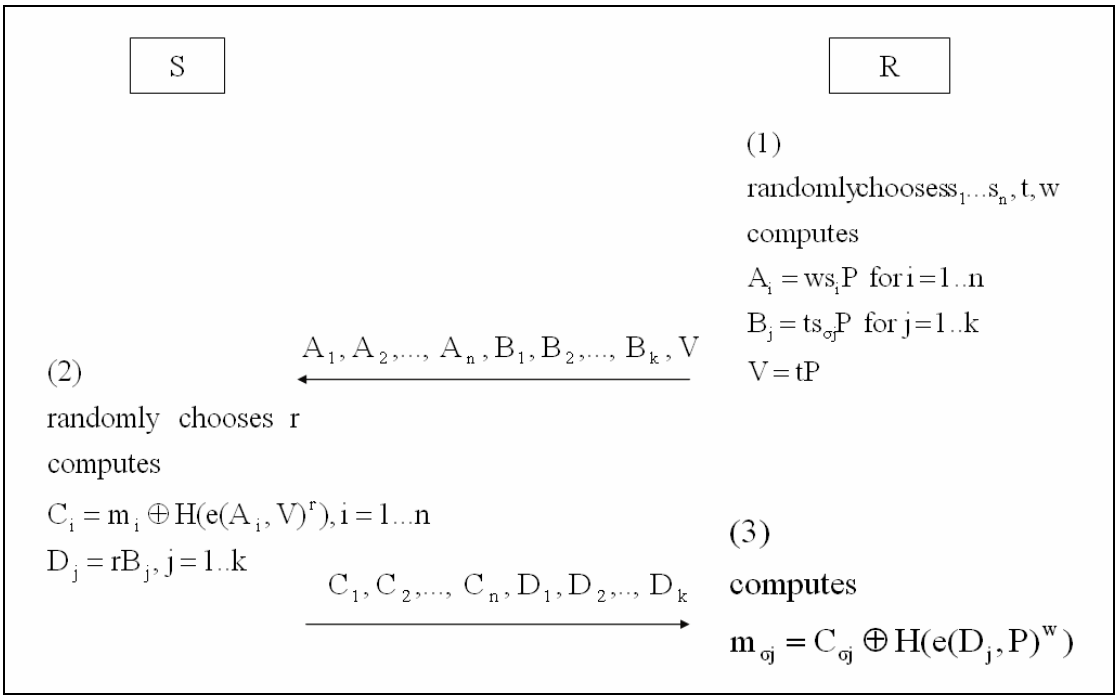

Figure 1 Our k-out-of-n OT scheme

5. Security and Performance analysis

In this session, we analyze the security of our scheme in Section 5.1 and also compare its communicational cost with other related work in Section 5.2.

5.1 Security Analysis

In this section, we examine the security of our scheme by considering the following properties.

(1). Correctness: After receiving messages, $C_1,C_2,\ldots,C_n,D_1,D_2,\ldots,D_k$, by using these received k D_j s to decrypt the n C_i s, R can correctly obtain the k messages $m_{\sigma 1}$, $m_{\sigma 2},\ldots,m_{\sigma k}$, which he had chosen by computing

$m_{\sigma j}=C_{\sigma j}\oplus H(e(D_j,P)^w) = C_{\sigma j}\oplus H(e(rB_j,P)^w) = C_{\sigma j}\oplus H(e(rts_{\sigma j}P,P)^w) =$

$C_{\sigma j}\oplus H(e(ws_{\sigma j}P,tP)^r) = C_{\sigma j}\oplus H(e(A_{\sigma j},V)^r)$.

(2). Assurance of the sender's privacy: The sender sends message m_i which is

protected by XORing $H(e(A_i,tP)^r)$. If R wants to obtain extra messages which he didn't choose, he need to know the number r. However, solving the random number r from D_j, j=1..k is computationally infeasible due to the ECDLP assumption.

(3). Assurance of the receiver privacy: The receiver's k choices in the n S_i random numbers, s_i,(i=1 to n), $s_{\sigma 1}$, $s_{\sigma 2}$,…, $s_{\sigma k}$, are enciphered in B_j (=$ts_{\sigma j}P$). After receiving $A_1,A_2,\ldots,A_n,B_1,B_2,\ldots,B_k$ and V(= tP) from R, S can not compute $s_{\sigma 1}$, $s_{\sigma 2}$,…, $s_{\sigma j}$ from B_j in polynomial time due to the ECDLP assumption. Therefore, the sender can not know which k messages, $m_{\sigma j}$, for j=1 to k, the receiver chose.

(4). Against dishonest receiver: In our k-out-of-n OT scheme, if R is dishonest in computing B_j(=$ts_{\sigma j}P$, for i=1,…,k) or V=(tP), R will not be able to obtain the correct $m_{\sigma j}$ by computing $m_{\sigma j} = C_{\sigma j} \oplus H(e(D_j,P)^w) = C_{\sigma j} \oplus H(e(rB_j,P)^w) \neq C_{\sigma j} \oplus H(e(A_j,V)^r) = C_{\sigma j} \oplus H(e(ws_{\sigma j}P,tP)^r) = C_{\sigma j} \oplus H(e(rts_{\sigma j}P,P)^w)$, where t and $s_{\sigma j}$ are committed in V and A_i by R, respectively.

5.2 Performance Analysis

In this section, we first compare the efficiency in bandwidth consumption and then the computation cost of our scheme with Chu et al.s' [4], Zhang et al.s'[12], and Mu et al.s' [26] in Table 1 and Table 2, respectively.

If the computation in discrete log problem needs 1024 bits, the bilinear pairings only needs 160 bits to achieve the same security level. Based on this fact, we compare the communicational cost of our scheme with the others by considering three factors, (1) the number of needed rounds between S and R, (2) the number of bits transfered from R to S, and (3) the number of bits from S to R. We show the result in Table 1.

Table 1: comparisons of needed rounds and transferred bits among proposed OT_k^n protocols

	Our scheme	Chu et al.s'[4]	Zhang et al.s'[12]	Mu et al.s'[26]
Needed Rounds	2	2	3	2
Bits needed from R to S	(n+k+1)*160 bits	k*1024 bits	(K+3)*1024 bits	2n*1024 bits
Bits needed from S to R	(n+k)*160 bits	(n+k+1)*1024 bits	2n*1024 bits	n*1024 bits

From table 1, we can see that if we wish our scheme to be more efficient than the others such as [4], (n+k+1)*160 must be less than k*1024. That is (n+k+1)*160 $\leqq$ 1024k. In other words, our scheme has the best performance in bandwidth consumption when n $\leqq$ 5.4k-1. Now, we compare the computational cost with the other three by using two factors: (1) the number of operations S performs, and (2) the number of operations R performs. We first show the definition of used notations in the following then show the result in Table 2. We first list the definitions of used notation.

T_{Exp}: the time needed by a modular exponentiation,1 ($T_{Exp} \cong 240\ T_{Mul}$)[19]

T_{Mul}: the time needed by a modular multiplication

T_{XOR}: the time needed by a modular bit-XOR

T_{EC_Mul}: the time needed by a scalar multipling a point on an elliptic curve(1 $T_{EC\_Mul} \cong 29\ T_{Mul}$)[19]

T_{bp} : the computation time of a bilinear pairing

T_{hash}: the computation time of a hash function

T_{enc}: the computation time of an encryption under DLP assumption

T_{dec}: the computation time of a decryption under DLP assumption

Table 2: comparisons of computational cost

	Our scheme	Chu et al.s'[4]	Zhang et al.s'[12]	Mu et al.s'[26]
Sender	$n(T_{bp}+T_{XOR})+ k T_{EC\_Mul}+n T_{hash}$	$(n+k+1)T_{Exp} +nT_{XOR}+(n+k) T_{hash}$	$3n T_{Exp} +3nT_{Mul}$	$2nT_{Exp}+nT_{Mul}+ nT_{enc}$ or $3nT_{Exp}+nT_{Mul}$
Receiver	$(2n+2k+1) T_{EC\_Mul}+k(T_{bp}+ T_{XOR}) +kT_{hash}$	$2kT_{Mul}+2kT_{Exp} +kT_{XOR}+2kT_{hash}$	$2k+3 T_{Exp} +kT_{Mul}$	$kT_{Exp}+2kT_{Mul}+ kT_{dec}$ or $2kT_{Exp}+2kT_{Mul}$

From Table 1 and Table 2, we can see that our scheme maybe less efficient in computation time. However, it is more efficient in bandwidth consumption than the other proposed schemes.

6. Conclusion

In this paper, we propose a secure efficient k-out-of-n oblivious transfer scheme based on pairings to reduce the bandwidth consumption for both of the sender and the receiver. After our analysis, we conclude that our scheme is not only secure but also more efficient than all other existing OT_k^n schemes in bandwidth consumption which plays an important role for end-of-day settlement in a busy financial network.

Reference

[1] Abhishek Parakh, “Oblivious Transfer Using Elliptic Curves, ”Proceedings of Proceedings of the 15th International Conference on Computing, Page(s):323 - 328 , IEEE , 2006.

[2] Abhishek Parakh, “Oblivious Transfer based on Key Exchange, ”eprint arXiv: 0705.0178, 2007 - arxiv.org

[3] C.Crepeau, “Equivalence between two flavors of oblivious transfer, ”EUROCRYPTO 87, pp.350-354, 1987.

[4] Cheng-Kang Chu, Wen-Guey Tzeng, “efficient k-out-of-n oblivious transfer Schemes with adaptive and non-adptive queries, ”PKC 2005 LNCS, pages 172-183, 2005

[5] Chih-Hung Wang and Chi-Shin Lin. ”A New Efficient k-out-of-n Transfer Scheme by means of Common Cipher, ”Int. Computer Symposium, Dec. 15-17, 2004, Taipei, Taiwan

[6] Chih-Yin Lin, Tzong-Chen Wu, Fangguo Zhang and Jing-Jang Hwang, “New identity-based society oriented signature schemes from pairings on elliptic curves, ”Applied Mathematics and Computation, Volume 160, Pages 245-260, 2005.

[7] D.Boneh and M.Franklin, “Identity-based encryption from the Weil pairings, ”Advances in Cryptology-Crypto 2001,LNCS 2139,pp.213-229,Springer-Verlag,2001.

[8] Hossein Ghodosi, “On insecurity of Naor-Pinkas’ distributed oblivious transfer, ”Information Processing Letters, Volume 104,2007

[9] Hui-Feng Huang, Chin-Chen Chang, “A New Design for Efficient t-out-n Oblivious Transfer Scheme, ”Proceedings of Advanced Information Networking and Application, Volume 2, 28-30, IEEE, 2005.

[10] Jan Camenish, Gregory Neven, abhi shelat, “Simulatable adaptive oblivious transfer, ”EUROCRYPT 2007, LNCS, page 573-590, 2007

[11] Jianhong Zhang, Wei Zou. “Two t-out-of-n oblivious transfer schemes with designated receiver, ”wuhan university journal of natural sciences, Vol.11, 2006.

[12] Jianhong Zhang, Yumin Wang, “Two provably secure k-out-of-n oblivious transfer schemes, ”Applied Mathematics and Computation, Volume 169, 2005.

[13] Kun Peng, Colin Boyd and Ed Dawson, “Batch verification of validity of bids in homomorphic e-auction, ”Computer Communications, Volume 29, 2006.

[14] M. Naor, B. PInkas, “Distributed oblivious transfer, ”Advances in Cryptology-Processings of ASIACRYPT’00, in: Lecture Notes in Computer Science, vol. 1976, Springer-Verlag, 2000

[15] Matthew Green, Susan Hohenberger. “Blind Identity-Based Encryption and Simulatable Oblivious Transfer, ”Cryptology ePrint Archive, Report 2007/235, 2007

[16] Manik Lal Das, Ashutosh Saxena, Ved P. Gulati and Deepak B. Phatak. “A novel remote user authentication scheme using bilinear pairings, ”Computers & Security, Volume 25, Pages 184-189, 2006

[17] Minh-Dung Dang, “More Extensions of Weak Oblivious Transfer, ”Innovation and Vision for the future, 2006-ieeexploreieee.org

[18] Moni Naor and Benny Pinkas. “Oblivious Transferwith Adaptive Queries”,In Proceedings of Advances in Cryptology-CRYPTO 99,volume 1666 of LNCS, pages 573-590, Springer-Verlag, 1999

[19] Narn-Yih Lee, Chien-Nan Wu, Chien-Chih Wang, “Authenticated multiple key exchange protocols based on elliptic curves and bilinear pairings, ”Computers and Electrical Engineering, 34 (2008) 12-20

[20] Rabin, “Exchange secrets by oblivious transfer, ”Computer Science Lab,

HarvardUniversity, Cambridge, MA, TR-81,1981

[21] Shai Halevi . “Yael Tauman Kalai. “Smooth projective hashing and two-message oblivious transfer, ”Cryptology ePrint Archive, Report 2007/118, 2007.

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

[23] Soongohn Kim, Seoksoo Kim, Geuk Lee, “Secure verifiable non-interactive oblivious transfer protocol using RSA and Bit commitment on distributed environment, ”Future Generation Computer Systems, 25 (2009) 352-357

[24] U SHINMYO, M KURIBAYASHI, M MORII, H TANAKA, “Fingerprinting Protocol Based on Distributed provider Using oblivious transfer, ”IEICE TRANS. FUNDAMENTALS,VOL.E89-A, NO.10 OCTOBER, 2006.

[25] 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.

[26] Yi Mu, Junqi Zhang, 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

[27] Yi Mu, Junqi Zhang, Vijay Varadharajan, Yan-Xia Lin, “Robust Non-Interactive Oblivious Transfer, ” IEEE COMMUNICATION LETTERS, VOL. 7,NO. 4,APRIL 2003

[28] Chin-Chen Chang, Jung-San Lee, “Robust t-out-of-n oblivious transfer mechanism based on CRT, “Journal of Network and Computer Applications, 32 (2009) 226– 235

[29] Hossein Ghodosi, Rahim Zaare-Nahandi, “Comments on the ‘m out of n oblivious transfer, “Information Processing Letters, Volume 97, Issue 4, 28

February 2006, Pages 153-155

[30] L.M. Kohnfelder, "On the signature reblocking problem in public-key cryptography," *Communications of the ACM, vol. 21(2)179*, 1978.

[31] M. Naor, B. Pinkas and R. Sumner, "Privacy preserving auctions and mechanism design, " *Proc. of the 1st ACM Conference on Electronic Commerce*, 1999.

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

[33] M. Naor and B. Pinkas, "Efficient oblivious transfer protocols," *SODA'01*, pp.448-457, 2001.

[34] Qin Jin, Zhao Hua-wei, and Wang Ming-Qiang, "Non-interactive oblivious transfer protocols," IFITA, IEEE, pp.120-124, 2009.