Journal of Theoretical and Applied Information Technology
20th April 2013. Vol. 50 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN EFFICIENT PROTOCOL FOR RESTRICTED ADAPTIVE OBLIVIOUS TRANSFER

RUAN OU[1,2], ZHOU JING[2,*],FU CAI[1], WANG CHUNZHI[2]

[1]College of Computer Science & Technology,

Huazhong University of Science & Technology, Wuhan, China, 430074

[2]College of Computer Science & Technology,

Hubei University of Technology, Wuhan, China, 430068

*Corresponding author: Zhou Jing, 12695133@qq.com

ABSTRACT

Restricted adaptive oblivious transfer was introduced by Herranz in 2011, which is the main approach to protect user privacy in e-transactions involving operations on digital confidential data or sensitive information. There are many practical applications for restricted adaptive oblivious transfer, such as medical or financial data access, pay-per-view TV, and so on. However, so far as we know, there are only two protocols for restricted adaptive oblivious transfers which were both proposed by Herranz [8]. Furthermore, these two protocols are very expensive. In this paper, we propose a new protocol for restricted adaptive oblivious transfer by using fully homomorphic encryption. Compared with Herranz's constructions, our protocol is more efficient in the cost of communication and computation.

Keywords: *Oblivious Transfer, Restricted Adaptive Oblivious Transfer, Fully Homomorphic Encryption*

1. INTRODUCTION

With the growth of modern Internet and mobile communication networks,more and more transactions in our daily life are performed electronically. Many of these e-transactions involve operations on digital confidential data or sensitive information. Thus, the demand for providing privacy to users is growing. The cryptographic primitive of standard oblivious transfer [1, 2] provides an approach to protect user privacy, which is an interactive protocol between a server and a client: the client retrieves an item db_i, and nothing else, from a database $DB = \{db_1, \ldots, db_N\}$ of secret items maintained by the server, who does not obtain any information about the index i (chosen by the client) of the retrieved item. So far, plenty of OT protocols have been proposed to provide user privacy, such as [3-7]. As we know, in traditional OT, a client can arbitrarily retrieve messages of his choices from a server without any restrictions, while this rules out many practical applications, such as medical or financial data access, pay-per-view TV. In these cases, on the one hand, the database server wants to enforce access control policies on the database, and prohibit the clients from retrieving messages of their choices without any restrictions. On the other hand, the clients do not want to reveal which messages they are retrieving. Summing up, there are situations which both the server and the clients want to preserve some kind of privacy. The server wants to restrict the access of each client to his data, by means of some policy; these restrictions can be defined by (decreasingly) monotone families, containing the subsets of items that are allowed to be retrieved. The clients can ask for retrieval of different items, in a sequential and adaptive (*i.e.*, possibly depending on the previously retrieved items) way, and should obtain these items, as long as they form a subset of allowed items, without letting the server know which items have been retrieved. This problem was called restricted adaptive oblivious transfer by Herranz [8]. There are many applications for restricted adaptive oblivious transfer. One real-life example where such a protocol is important is pay-per-view TV system: a TV channel over the Internet broadcasts different programs (films, sport events, MVs) which can be watched only by those clients who have paid for them. For example, a client may pay a registration fee which gives him the right of watching five films or ten football matches or twenty MVs.

However, traditional OT protocol does not solve it by itself, the problem of restricted adaptive oblivious transfer: since the server does not know the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

index of the currently queried item, he cannot decide if the client has (still) the right to obtain this item. So far as we know, there are only two protocols for restricted adaptive oblivious transfers that were both proposed by Herranz [8]. Furthermore, these two protocols are very expensive. In this paper, we propose a new protocol for restricted adaptive oblivious transfer by using fully homomorphic encryption. Compared whith Herranz's constructions, our protocol is more efficient in the cost of communication and computation.

The rest of the paper is arranged as follows. In Section 2, the related works are introduced. Then, fully homomorphic encryption is recalled in Section 3. Section 4 proposes our new protocol for restricted adaptive oblivious transfer and analyzes its efficiency. Finally, conclusions are drawn and future work is presented in Section 5.

2. RELATED WORKS

Oblivious transfer (OT) is a two-party computation protocol between a sender and a receiver where the sender transfers some information to the receiver while remaining oblivious as to which information the receiver obtains [1]. This scheme was first introduced by Rabin [3]. In 1985, Even *et al.* [4] presented a more generalized form of OT, naming *1*-out-of-*2* OT which can let a sender send two encrypted messages to a receiver, whereas the receiver can decrypt only one of them that he had chosen in advance. In 1986, Brassard et al. [2] further extended *1*-out-of-*2* to *1*-out-of-*n* OT, the case of sending *n* messages to a receiver with only one of them can be obtained by the receiver. Here, *k*-out-of-*n* scheme is the final form of OT scheme [5-7].

In its basic form, oblivious transfer puts no restrictions on which records a particular user can access, *i.e.*, all users can access all records. In many practical applications, such as medical or financial data access, pay-per-view TV, the server wants to enforce access control policies on messages, and prohibit users retrieving messages of their choices without any restrictions. In 2001, Aiello *et al.* [9] present priced oblivious transfer, in which each record has attached a (possibly different) price, the client holds a (homomorphically) encrypted balance which is reduced with each transfer and her can only retrieve records as long as her balance is positive. In 2011, Herranz [8] proposes a more general scheme called restricted oblivious transfer, which protects each record with an access control policy. In his case the policy consists of several different lists, the client can access to items if and only if the serial accessing items form a subset of one of the lists. In his paper, he also showed that priced oblivious transfer is a particular case of restricted adaptive oblivious transfer.

Other works [10-14] focused on providing access control policy with user anonymity for OT protocols, where each item of the database is associated with a policy, and only clients whose attributes satisfy this policy are allowed to obtain this item in a private and anonymous way. In their schemes, in order to guarantee user anonymity they introduced a trusted third party, called the issuer external which is assigning attributes to users for the server database.

3. PRELIMINARIES

In this section we recall fully homomorphic encryption which will appear in the construction of our new restricted adaptive oblivious transfer protocol.

3.1 Fully Homomorphic Encryption

Fully homomorphic encryption is one of the holy grails of modern cryptography. Such scheme is well known to be useful for constructing privacy-preserving protocols, for example as required in 'cloud computing' applications: a user can store encrypted data on a server, and allow the server to process the encrypted data without revealing the data to the server. At a high-level, the essence of fully homomorphic encryption is simple: given ciphertexts that encrypt $\pi_1, \pi_2, \ldots, \pi_t$, fully homomorphic encryption should allow anyone to output a ciphertext that encrypts $f(\pi_1, \pi_2, \ldots, \pi_t)$ for any desired function *f*, as long as that function can be efficiently computed. No information about $\pi_1, \pi_2, \ldots, \pi_t$ or $f(\pi_1, \pi_2, \ldots, \pi_t)$, or any intermediate plaintext values, should leak; the inputs, output and intermediate values are always encrypted. The problem was suggested by Rivest, Adleman and Dertouzos [15] back in 1978, yet the first plausible candidate came thirty years later with Gentry's breakthrough work in 2009 [16,17].

Dijk *et al.* [18] and Brakerski *et al.* [19] introduced the *somewhat homomorphic* scheme, which can achieve homomorphism under addition and multiplication. Brakerski *et al.* [20] show that *somewhat homomorphic* encryption can be based on standard, well-studied cryptographic assumptions, and constructed a very efficient *somewhat homomorphic* encryption protocol.

In the construction of our restricted adaptive oblivious transfer protocol, the *somewhat homo-*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

morphic scheme will be used. A public key cryptosystem is additively homomorphic if there exists an operation $\oplus$ defined on the set of ciphertexts, such message that encrypted in $c_1 \oplus c_2$ is $m_1 + m_2$, where m_i is the message encrypted in c_i, for $i = 1, 2$. Formally, this property is written as $D_{sk}(\varepsilon_{pk}(m_1) \oplus \varepsilon_{pk}(m_2)) = m_1 + m_2$. Analogously, a cryptosystem is multiplicatively homomorphic if there exists an operation $\otimes$ which is defined on the set of ciphertexts, such that $D_{sk}(\varepsilon_{pk}(m_1) \otimes \varepsilon_{pk}(m_2)) = m_1 \cdot m_2$, for any pair of plaintexts (m_1, m_2).

4. AN EFFICIENT PROTOCOL FOR RESTRICTED ADAPTIVE OBLIVIOUS TRANSFER

In this section, we will propose our protocol for restricted adaptive oblivious transfer, and analyze its efficiency by comparing it with Herranz's construction [8].

4.1 The General Functionality of Restricted Adaptive Oblivious Transfer

In this section we review definitions related to the general functionality of restricted adaptive oblivious transfer, where a server S maintains a secret database $DB = \{db_1, \ldots, db_N\}$ with N items and a policy defining which subsets of entries of the database can be available to the different clients, and wants to be sure that a client C will not obtain any information about items of the database which are not allowed to C; and a client ask for retrieval of different items in a sequential and adaptive way without letting the server know which items have been retrieved. In general, a protocol fulfilling this functionality will consist of two phases: the setup phase - defining rights and the request & retrieval phase.

The setup phase: defining rights. This phase should be run offline. Let $\rho = \{1, \ldots, N\}$ denote the set of indices of the items in the database. For a particular client C, the server S specifies the family $\mathrm{B}_C = \{B_1, \ldots, B_s\} \subset 2^{\rho}$ of subsets of items that client C is allowed to obtain. Of course, B_C must be a decreasingly monotone family: if $B_1 \in B_C$ is allowed, and $B' \subset B_1$, then $B' \in B_C$ is allowed, as well. The family B_C is known by both S and C. The server S stores an information info_C related to C, which initially contains B_C. Possibly, the client C receives some additional information α_c from S, to be used in the future requests.

Request & retrieval phase. The input for the client C includes α_c and the index i_t corresponding to the item db_{i_t} he wants to retrieve from the database. The input for the server consists of the database DB and info_C. At the end of the protocol, C obtains a value out_{i_t}. Assume that this is the t-th time that C executes this protocol with S, and that previous executions had inputs $i_1, \ldots, i_{t-1}$. Let us define the subset of indices $B = \{i_1, \ldots, i_{t-1}, i_t\}$. Then C obtains the desired value, *i.e.* $out_{i_t} = db_{i_t}$, if and only if $B \in B_C$.

A protocol for this functionality of restricted adaptive oblivious transfer will be considered secure if it satisfies the following three properties.

- **Correctness**. Assume that the t-th execution of the protocol has input (i_t, α_c) for C, where $i_t \in \{1, \ldots, N\}$. The first requirement is a typical correct one: if the client and the server behave honestly during the t-th execution and if $\{i_1, \ldots, i_t\} \in B_C$, then $out_{i_t} = db_{i_t}$ is the secret output of C.

- **Privacy for the client**. In any execution of the protocol for request & retrieval of an item, the server S does not obtain any information about the index i_t.

- **Privacy for the server**. In the t-th execution of the 'request & retrieval' phase, with input (i_t, α_c), the client C does not obtain any information about items db_ℓ, for $\ell \neq i_t$; and does not obtain any information about item db_{i_t}, if $\{i_1, \ldots, i_t\} \notin B_C$.

Just as we can see, a malicious server can always refuse to execute his part of the protocol or run the request & retrieval phase with entries db_j' different than the correct ones db_j. The first case almost exists in all protocols, which we can't do anything about it. The second case, to avoid this problem, the server can be required to publish a cryptographic commitment of each entry in the database, in the setup phase of the system. Later, in case of dispute, a judge can forge the server to open the corresponding commitments and take a decision.

In the construction of our protocol for restricted adaptive oblivious transfer, for simplicity, we will assume that the server behaves honestly, *i.e.* he does not refuse any query of a client, and he uses

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the correct values db_j of the items as the inputs of the corresponding protocols.

4.2 The New Protocol for Restricted Adaptive Oblivious Transfer

We now describe our protocol in details. The two phases of the protocol that we propose work as follows.

1. The setup phase: defining rights

Let $\rho = \{1,\ldots,N\}$ denote the set of indices of the items in the server's database and $\mathrm{B}_C = \{B_1,\ldots,B_s\} \subset 2^\rho$ be the family of subsets of indices expressing the collections of items that client C is allowed to query. In general, we will have $B_j = \{i_{j,1},\ldots,i_{j,n_j}\} \subset \rho$.

The client generates a pair of keys $(pk, sk) \leftarrow Kg(1^k)$ for the homomorphic cryptosystem PKE, and publishes pk. The server computes an encryption of B_C, *i.e.*, he computes $\vec{\mathrm{c}}_j = (\varepsilon_{\mathrm{pk}}(i_{j,1}),\ldots,\varepsilon_{\mathrm{pk}}(i_{j,n_j}))$, for $j = 1,\ldots,s$. He also chooses a random value u_0 and encrypts it $c_u = \varepsilon_{\mathrm{pk}}(u_0)$. Initially, he sets $\mathrm{info}_C = (pk, c_u, \{\vec{\mathrm{c}}_j\}_{j=1,\ldots,s})$ and sends additional information c_u to the client, which will be used in the future requests.

2. Request & retrieval phase

The *t*-th execution of the "request and retrieval" protocol works as follows, for $t \geq 1$.

(1) To retrieve item db_{i_t}, the client decrypts c_u to get u_{t-1}, and computes $c_{i_t} = \varepsilon_{\mathrm{pk}}(i_t)$ and $c_{u,i_t} = \varepsilon_{\mathrm{pk}}(u_{t-1})$, then sends (c_{i_t}, c_{u,i_t}) to the server.

(2) After receiving (c_{i_t}, c_{u,i_t}) from the client, the server does:

(i) He computes $\vec{\mathrm{c}}_{s,t,j} = (c_{s,t,j,1},\ldots,c_{s,t,j,N})$, for $j = 1,\ldots,s$,

where $c_{s,t,j,k}$ =

$$\varepsilon_{\mathrm{pk}}(db_k + (u'_{t-1} - u_{t-1} + i_k - i_t)^{t_{j,k,0}} + (i_{j,1} - i_t)^{t_{j,k,1}} \cdot (i_{j,2} - i_t)^{t_{j,k,2}} \cdot \ldots \cdot (i_{j,n_j} - i_t)^{t_{j,k,n_j}})$$

for $k = 1,\ldots,N$, u'_{t-1} is the plaintext of c_{u,i_t},.

The server can compute $c_{s,t,j,k}$ as follows.

(a) $c_{db_k} = \varepsilon_{\mathrm{pk}}(db_k)$

(b) $c_{i_k} = \varepsilon_{\mathrm{pk}}(i_k)$

(c) $c_{s,t,j,k}$ =

$$c_{db_k} \oplus (c_{u,i_t} - c_u + c_{i_k} - c_{i_t})^{t_{j,k,0}} \oplus (c_{j,1} - c_{i_t})^{t_{j,k,1}} \otimes (c_{j,2} - c_{i_t})^{t_{j,k,2}} \otimes \ldots \otimes (c_{j,n_j} - c_{i_t})^{t_{j,k,n_j}}$$

(ii) Her chooses a random value u_t and encrypts it, *i.e.*, $c_{u_t} = \varepsilon_{\mathrm{pk}}(u_t)$.

(iii) He sends $(c_{u_t}, \{\vec{\mathrm{c}}_{s,t,j}\}_{j=1,\ldots,s})$ to the client.

(3) The server updates the values $\{\vec{\mathrm{c}}_j\}_{j=1,\ldots,s}$.

First, he computes

$$c'_{j,i} = \varepsilon_{\mathrm{pk}}(i_{j,i} + (i_{j,1} - i_t)^{t_{j,1}} \cdot (i_{j,2} - i_t)^{t_{j,2}} \cdot \ldots \cdot (i_{j,n_j} - i_t)^{t_{j,n_j}})$$

$$= c_{j,i} \oplus (c_{j,1} - c_{i_t})^{t_{j,1}} \otimes (c_{j,2} - c_{i_t})^{t_{j,2}} \otimes \ldots \otimes (c_{j,n_j} - c_{i_t})^{t_{j,n_j}}$$

for $j = 1,\ldots,s$ and $i = 1,\ldots,n_j$.

Then, he replaces the old values $\{\vec{\mathrm{c}}_j\}_{j=1,\ldots,s}$ of with the new ones, in info_C, where he also replaces c_u with c_{u_t}. From the above updating, we can see that $\vec{\mathrm{c}}_j$ become encryptions of a list of random values if the client has asked for an item which was not in B_j, which means the subset B_j must not be considered any more.

(4) After receiving $(c_{u_t}, \{\vec{\mathrm{c}}_{s,t,j}\}_{j=1,\ldots,s})$ from the server, the client can decrypt the ciphertext c_{s,t,m,i_t} with *sk*, obtaining the desired item db_{i_t}, if $\{i_1,\ldots,i_t\} \subseteq B_m \wedge B_m \in \mathrm{B}_C$.

Theorem 1: The above protocol securely realizes the general functionality of restricted adaptive oblivious transfer.

Proof: We will show that the above protocol satisfies the following 3 properties.

(i) Correctness:

$D_{sk}(c_{s,t,m,i_t})$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$= D_{sk}(\varepsilon_{\mathrm{pk}}(db_{i_t} + (u'_{t-1} - u_{t-1} + i_t - i_t)^{t_{m,k,0}} + (i_{m,1} - i_t)^{t_{m,i_t,1}} \cdot (i_{j,2} - i_t)^{t_{m,i_t,2}} \cdot \ldots (i_{m,n_m} - i_t)^{t_{m,i_t,n_m}}))$$

$$= D_{sk}(\varepsilon_{\mathrm{pk}}(db_{i_t} + 0 + (i_{m,1} - i_t)^{t_{m,i_t,1}} \cdot (i_{m,2} - i_t)^{t_{m,i_t,2}} \cdot \ldots \cdot (i_t - i_t)^{t_{m,i_t,i_t}} \cdot \ldots (i_{m,n_m} - i_t)^{t_{m,i_t,n_m}}))$$

$$= D_{sk}(\varepsilon_{\mathrm{pk}}(db_{i_t} + 0 + (i_{m,1} - i_t)^{t_{m,i_t,1}} \cdot (i_{m,2} - i_t)^{t_{m,i_t,2}} \cdot \ldots \cdot 0 \cdot \ldots (i_{m,n_m} - i_t)^{t_{m,i_t,n_m}}))$$

$$= D_{sk}(\varepsilon_{\mathrm{pk}}(db_{i_t}))$$

$$= db_{i_t}$$

(ii) Privacy for the client:

In the protocol, the client only sends the ciphertexts (c_{i_t}, c_{u,i_t}) to the server, which disclosed nothing to the server from the security of the encryption scheme.

(ii) Privacy for the server:

In the protocol, the server sends message $(u_t, \{\vec{c}_{s,t,j}\}_{j=1,\ldots,s})$ to the client.

(1)If $\{i_1,\ldots,i_t\} \subseteq B_m$ ($B_m \in \mathrm{B}_C$), from the correctness of the protocol, the client can get the desired item db_{i_t} , however, he learns nothing about the other item db_ℓ ($\ell \neq i_t$), because the ciphertext $c_{s,t,m,\ell}$ is an encryption of some random value.

$$c_{s,t,m,\ell} =$$

$$\varepsilon_{\mathrm{pk}}(db_\ell + (u'_{t-1} - u_{t-1} + i_\ell - i_t)^{t_{m,k,0}} + (i_{m,1} - i_t)^{t_{m,i_t,1}} \cdot (i_{m,2} - i_t)^{t_{m,i_t,2}} \cdot \ldots (i_{m,n_m} - i_t)^{t_{m,i_t,n_m}})$$

$$= \varepsilon_{\mathrm{pk}}(db_\ell + (i_\ell - i_t)^{t_{m,k,0}})$$

(2)If $\{i_1,\ldots,i_t\} \not\subset B_m$ ($B_m \in \mathrm{B}_C$), there exists some index $i_\ell \notin B_m$.

(i)If $i_\ell = i_t$,

$$c_{s,t,m,k} =$$

$$\varepsilon_{\mathrm{pk}}(db_k + (u'_{t-1} - u_{t-1} + i_k - i_t)^{t_{j,k,0}} + (i_{m,1} - i_t)^{t_{m,i_t,1}} \cdot (i_{m,2} - i_t)^{t_{m,i_t,2}} \cdot \ldots (i_{m,n_m} - i_t)^{t_{m,i_t,n_m}})$$

is an encryption of some random value, because $(i_{m,1} - i_t)^{t_{m,i_t,1}} \cdot (i_{m,2} - i_t)^{t_{m,i_t,2}} \cdot \ldots (i_{m,n_m} - i_t)^{t_{m,i_t,n_m}}$ is a random value.

(ii)If $i_\ell < i_t$, in the ℓ -th execution of the "request & retrieval" phase, the server updates $\{\vec{c}_j\}_{j=1,\ldots,s}$, in which $c_{m,i} =$

$$\varepsilon_{\mathrm{pk}}(i_{m,i} + (i_{m,1} - i_\ell)^{t_{m,1}} \cdot (i_{m,2} - i_\ell)^{t_{m,2}} \cdot \ldots (i_{m,n_m} - i_\ell)^{t_{m,n_m}})$$

for $i = 1,\ldots,n_m$ is an encryption of some random value because $(i_{m,1} - i_\ell)^{t_{m,1}} \cdot (i_{m,2} - i_\ell)^{t_{m,2}} \cdot \ldots (i_{m,n_m} - i_\ell)^{t_{m,n_m}}$ is a random value. Thus, from the $\ell+1$ -th execution the $\vec{c}_m$ is the encryptions of some random values instead of the encryptions of B_m.

4.3 Efficiency Analyze

So far there are only two protocols for restricted adaptive oblivious transfer, which were both proposed by Herranz [8] and we denote as JH11-1 and JH11-2. Just as Herranz pointing out in [8], JH11-2 is less efficient than JH11-1. Thus, we only need to compare our protocol with JH11-1. In the construction of JH11-1, a complicated conditional disclosure of secrets protocol was used, which needs $2N^2 + 2s + 2$ encryptions and $2N^2 + 2s + 2$ group element exchange, where N is the size of the server's DB, s is the number of the client's subsets of items that he is allowed to obtain. However, we avoid using the conditional disclosure of secrets protocol. The efficiency results of the protocols JH11-1 and ours are shown in the table 1, where N, s are just the same as above, $n_1, n_2, \ldots, n_s$ are the number of each subset's items that the client is allowed to obtain, and $s \square N$, $n_i \square N$ for $i = 1,\ldots,s$ in the vast majority of practical applications. From table 1 we can see obviously that our protocol is more efficient than JH11-1, especially for bandwidth.

Table 1. Efficiency results of the protocols JH11-1 and Ours

Scheme		JH11-1	Ours
Defining rights	Encryptions	$s \cdot N$	$(n_1 + n_2 + \ldots + n_s)$
Request & retrieval	Client's Encryptions	$2N^2 + N + 2s + 4$	6
	Server's Encryptions	1	$2N + 1$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

	Group element Exchanges	$4N^2 + N$ $+4s+5$	$s \cdot N + 4$

5. CONCLUSION AND FUTURE WORK

In the paper, we propose a new protocol for restricted adaptive oblivious transfer by using public key cryptosystems which are additive at the same time and multiplicatively homomorphic, called fully homomorphic encryption. Our protocol avoids using the conditional disclosure of secrets protocol, and is more efficient in the cost of communication and computation than Herranz's constructions.

As future research related to this work, Herranz mentioned two possibilities: improving the efficiency of the solutions and providing anonymity for the clients. There has a third possibility: constructing secure protocols for restricted adaptive oblivious transfer according to the standard ideal/real simulation paradigm [21] and within UC framework [22].

ACKNOWLEDGEMENT

This work was partially funded by the National Natural Science Funds of China under Grant No.60903175 and 61170135.

REFRENCES:

[1] M. Rabin, "How to exchange secrets by oblivious transfer", *Technical report TR-81*, Harvard Aiken Computation Laboratory, 1981.

[2] G. Brassard, C. Crépeau and J.M. Robert, "All-or-nothing disclosure of secrets", *Proceedings of Crypto'86*, Santa Barbara, CA, Aug 11-15,1986, pp. 234 – 238.

[3] M. Naor and B. Pinkas, "Computationally secure oblivious transfer", *Journal of Cryptology*.Vol. 18, No.1, 2005, pp.1-35.

[4] S. Even and O. Goldreich, "A. Lempel. A randomized protocol for signing contracts", *Communications of the ACM*, Vol. 28, No. 6, 1985, pp. 637-647.

[5] W. Ogata and K. Kurosawa, "Oblivious keyword search", *Journal of Complexity*, Vol. 20, No. 2-3, 2004, pp. 356-371.

[6] J. Zhang and Y. Wang, "Two provably secure k-out-of-n oblivious transfer schemes", *Applied Mathematics and Computation*, Vol. 169, No. 2, 2005, pp.1211-1220.

[7] Zeng B. , Tartary C. , Xu P. , Jing, J. and Tang X, "A Practical Framework for t-Out-of-n Oblivious Transfer With Security Against Covert Adversaries", *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 2, 2012, pp.465-479.

[8] Javier Herranz, "Restricted adaptive oblivious transfer", *Journal Theoretical Computer Science*, Vol. 412, No. 46, October, 2011, pp.6498-6506.

[9] B. Aiello, Y. Ishai and O. Reingold, "Priced oblivious transfer: How to sell digital goods", *Proceedings of Eurocrypt 2001*, Innsbruck (Tyrol), Austria, May 6 -- 10, 2001, pp. 119 – 135.

[10] J. Camenisch, M. Dubovitskaya and G. Neven, "Oblivious transfer with access control", *Proceedings of CCS ' 09*, August 12 -- 17, 2009, pp. 131 – 140.

[11] J. Camenisch, M. Dubovitskaya, G. Neven and G.M. Zaverucha, "Oblivious transfer with hidden access control policies", *Proceedings of PKC'11*, Taormina, Italy, March 6-9, , 2011, pp. 192 – 209.

[12] A. Rial and B. Preneel, "Blind Attribute-Based Encryption and Oblivious Transfer with Fine-Gramed Access Control", *2010th Benelux Workshop on Information and System Security (WISSec 2010)*, Nijmegen, the Netherlands, November 29-30, 2010.

[13] Jan Camenisch, Maria Dubovitskaya, Robert R. Enderlein and Gregory Neven, "Oblivious Transfer with Hidden Access Control from Attribute-Based Encryption", *Security and Cryptography for Networks*, Lecture Notes in Computer Science Vol. 7485, 2012, pp. 559-579

[14] L. Xu and F. Zhang, "Oblivious Transfer with Threshold Access Control", *Journal of Information Science and Engineering*, Vol. 28, No. 3, May 2012, pp.555-570.

[15] R. Rivest, L. Adleman, and M. Dertouzos, "On data banks and privacy homomorphisms", *Foundations of Secure Computation*, Academic Press, 1978, pp. 169 – 177.

[16] Craig Gentry, "Fully homomorphic encryption using ideal lattices", STOC 2009, Maryland, USA, May 31 - June 2 2009, pp.169-178.

[18] Craig Gentry, "Toward basing fully homomorphic encryption on worst-case hardness", *CRYPTO 2010*, Santa Barbara, California, USA. August 15-19, 2010, pp. 116 – 137.

[19] M. Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan,"Fully homomorphic encryption over the integers", *EUROCRYPT 2010*, French Riviera, May 30 - June 3 2010, pp. 24 – 43.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[20] Z. Brakerski and V. Vaikuntanathan, "Fully homomorphic encryption from ring-LWE and security for key dependent messages", *CRYPTO 2011*, Santa Barbara, August 14-18 2011, p.501-520

[21] Zvika Brakerski and Vinod Vaikuntanathan. "Efficient Fully Homomorphic Encryption from (Standard) LWE", *Ost11*, Ostrovsky, 2011, pp.97-106.

[22] O. Goldreich, Foundations of Cryptography: Volume II—Basic Applications, 2004, Cambridge, U.K.: Cambridge Univ. Press.

[23] R. Canetti, "Universally composable security: A new paradigm for cryptographic protocols", *Proc. of 42nd Annual Symposium on Foundations of Computer Science (FOCS)*, Las Vegas, Nevada, USA, 14-17 October 2001, pp.136-145.