University of Wollongong
Research Online

Faculty of Informatics - Papers (Archive)

Faculty of Engineering and Information Sciences

2012

Efficient oblivious transfers with access control

Jinguang Han
University of Wollongong, jh843@uowmail.edu.au

Willy Susilo
University of Wollongong, wsusilo@uow.edu.au

Yi Mu
University of Wollongong, ymu@uow.edu.au

Jun Yan
University of Wollongong, jyan@uow.edu.au

Publication Details

Han, J., Susilo, W., Mu, Y. & Yan, J. (2012). Efficient oblivious transfers with access control. Computers and Mathematics with Applications, 63 (4), 827-837.

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

Efficient oblivious transfers with access control

Abstract
Oblivious transfer (OT) is a protocol where a receiver can obtain t-out-of-n services from the sender without releasing anything about his choices. OT can be used to protect user's privacy. In principle, any user can interact with a server to request some services. This might allow some undesirable users to obtain services from the server. How to ensure that only the authorized receivers can obtain services obliviously is a daunting task. In this paper, we introduce oblivious signature based-on envelope (OSBE) to OT and propose two novel OT schemes, which only allow the legitimate receivers to obtain services obliviously. The receiver is required to authenticate himself to the issuer to possess the required credential prior to access the protected services; while no authentication from the sender needs to be done. The sender knows the number of the services selected by the receiver, but does not know anything about his choices and personally identifiable information. The feature of our scheme also lies in avoiding zero knowledge proofs and achieving all-or-nothing non-transferable credentials. Our schemes are efficient in the cost of communication and computation.

Keywords
efficient, oblivious, transfers, access, control

Disciplines
Physical Sciences and Mathematics

Publication Details
Han, J., Susilo, W., Mu, Y. & Yan, J. (2012). Efficient oblivious transfers with access control. Computers and Mathematics with Applications, 63 (4), 827-837.

This journal article is available at Research Online: http://ro.uow.edu.au/infopapers/1875

Efficient Oblivious Transfers with Access Control

Jinguang Han[a,c,*], Willy Susilo[a], Yi Mu[a], Jun Yan[b]

[a] *Centre for Computer and Information Security Research, School of Computer Science and Software Engineering, University of Wollongong, NSW2522, Australia.*
[b] *School of Information Systems and Technology, University of Wollongong, NSW2522, Australia.*
[c] *College of Science, Hohai University, Nanjing 210098, China.*

Abstract

Oblivious transfer (OT) is a protocol where a receiver can obtain t-out-of-n services from the sender without releasing anything about his choices. OT can be used to protect user's privacy. In principle, any user can interact with a server to request some services. This might allow some undesirable users to obtain services from the server. How to ensure that only the authorized receivers can obtain services obliviously is a daunting task. In this paper, we introduce oblivious signature based-on envelope (OSBE) to OT and propose two novel OT schemes, which only allow the legitimate receivers to obtain services obliviously. The receiver is required to authenticate himself to the issuer to possess the required credential prior to access the protected services; while no authentication from the sender needs to be done. The sender knows the number of the services selected by the receiver, but does not know anything about his choices and personally identifiable information. The feature of our scheme also lies in avoiding zero knowledge proofs and achieving all-or-nothing non-transferable credentials. Our schemes are efficient in the cost of communication and computation.

Keywords: Access Control, Oblivious Transfer, Oblivious Signature Based-on Envelope, Privacy.

*Corresponding author.Tel.: +61 242214824; fax: +61 242215550

Email addresses: jh843@uow.edu.au (Jinguang Han), wsusilo@uow.edu.au (Willy Susilo), ymu@uow.edu.au (Yi Mu), jyan@uow.edu.au (Jun Yan)

1. Introduction

Although the Internet has brought enormous benefits to people, security and privacy problems have been a major concern to the users. Internet users are concerned with their privacy, and require their personally identifiable information (PII) not to be collected, pilfered and illegally used. Although users believe that a small part of PII is insufficient for identifying the real identity, the malicious attackers can aggregate the collected partial PII, such as health condition, financial data and hobbies, to analyze and trace the real user. Lessons from identity theft, identity fraud, fictitious identity *etc.* suggest that PII should be released under the user's control in the critical moment.

Obviously, there is a trade-off between the accountability and privacy. How to balance them is a challenging problem. There have been some attempts toward a solution, such as identity management[1,2], user-centric system[3,4,5], privacy-preserving systems[6,7], anonymous credential[8,9,10,11,12,13,14], hidden credentials[15], k-time anonymous authentication[16,17,18,19]. These systems addressed the security of the user's PII so that the user cannot be impersonated. In practice, the adversary can trace and identify a user not only by the PII, but also by his activities, such as the websites he visited frequently, the goods he purchased online. Therefore, in order to protect users' privacy, we need a new system that captures the security of both PII and services selected by a user. The following properties should be considered:

1. Only the authorized users can access the protected services.
2. The service providers should not know anything about the user's PII.
3. The service providers should not know anything about the contents of the services the user selected.

Suppose there exists a third trusted party (TTP) called the issuer, who is trusted by all participants in the system. Prior to accessing the services, the user needs to authenticate himself to the issuer and obtain the required credentials. The user can use these credentials to access the protected services, without revealing any information about his choice and PII to the service providers. Such a system can be used in some practical scenarios. For example, in the library database system, the user registers himself to the manager and then obtains a permission to access the database system. The database will record the number of the items he accessed, without knowing anything about the contents of the selected items. The library can charge

the user according to the number recorded by the database. Both the PII and the selected services are not disseminated to the database. Therefore, this system can resist against a malicious database that analyzes the user from the partial PII and services. Other applications of this system can be found in the sensitive information system, where only the qualified people can access the protected services, such as patent search, DNA databases and multi-party computations.

Proposed by Rabin in 1981[20], and extended by Brassaard, Crépeau and Robert in 1987[21], k-out-of-n oblivious transfer (OT_k^n) is a cryptographic primitive, where the sender and the receiver have messages $M_1, M_2, \cdots, M_n$ and choices $\sigma_1, \sigma_2, \cdots, \sigma_t \in \{1, 2, \cdots, n\}$, respectively. After a transfer, the receiver obtains messages $M_{\sigma_1}, M_{\sigma_2}, \cdots, M_{\sigma_t}$, while the sender can not know anything about the receiver's choices. Adaptive k-out-of-n oblivious transfer ($\mathrm{OT}_{k\times 1}^n$), proposed by Naor and Pinkas[22,23], allows the receiver to obtain services from the sender one by one adaptively, namely the i-th choice may depend on the first $i-1$ choices. Therefore, adaptive k-out-of-n oblivious transfer can provide stronger security than k-out-of-n oblivious transfer.

A drawback of $\mathrm{OT}_{k\times 1}^n$ is that there is no limitation on the user; namely any one can interact with and receive services from the server obliviously. There exist some attempts to prevent an illegal receiver from accessing the protected services. Aiello, Ishai, and Reingold proposed a priced oblivious transfer based on homographic encryption and private information retrieval (PIR)[24], where only if the price of the selected service is less than the remaining balance, then the receiver can obtain the service from the sender obliviously. Otherwise, the selected service will be denied. Subseqently, Crescenzo, Ostrovsky and Rajagopalan[25] proposed a conditional oblivious transfer scheme where the receiver can access the protected service if and only if his secret key satisfies the public predicate. Unfortunately, the privacy of users was not considered in these schemes.

Recently, Coull, Green and Hohenberger proposed an oblivious transfer with access control using state graphs[26]. In this scheme, the receiver's state shifts from one to another after each transition. If all states are used, the receiver cannot access the protected services any longer. Camenisch, Dubovitskaya and Neven proposed another oblivious transfer with access control[27,28], which is more efficient than the former. All these schemes work as follows:

1. The receiver authenticates himself to the issuer, and obtains the required credentials from him.

2. The receiver proves that he has possessed the required credentials to the sender in zero knowledge.
3. The receiver and the sender execute an oblivious transfer[29] to obtain the intended services.

In these schemes, the user needs to authenticate himself to the issuer and obtain credentials. Then, the receiver proves that he is an authorized receiver to the sender in zero knowledge. Since the receiver needs to authenticate himself two times, the cost of computation and communication is expensive. Recently, Camenisch, Dubovitskaya, Neven and Zaverucha proposed a new oblivious transfer with access control scheme where a user can only knows whether he is granted to access the service items and dose not know anything about the access control policies[30].

Proposed by Li, Du and Boneh[31], oblivious signature-based envelope (OSBE) is a cryptographic primitive, where the receiver can obtain the secret encapsulated in the envelop by the sender if and only if he has possessed a signature from the issuer on the public message. Additionally, the receiver is not required to authenticate himself to the sender. The sender cannot distinguish the receivers who have possessed credentials from the receivers who has not possessed credentials. Therefore, the signature is a hidden credential[1][51]. OSBE has been used in automated trust negotiation (ATN)[34], secure function evaluation (SFE), secret handshakes[35]. Notably, the sender in OSBE cannot control the interaction. The reason is that the sender encrypts the secret only under the parameters obtained from the issuer, instead of using his own private key.

Our Contribution

In this paper, we propose two novel efficient oblivious transfer schemes with access control. In our schemes, only the authorized user (receiver) can obtain services from the server obliviously. The server knows how many items the authorized user can obtain but it knows nothing about the contents of the selected items. Additionally, the receiver is not required to authenticate himself to the server. Therefore, the user releases nothing about his PII to the server. Our schemes *do not* require any zero knowledge proof, and hence, our scheme is more efficient than other schemes. We propose the extended chosen-target computational Diffie-Hellman (XCT-CDH) assumption, which

[1]This notion was proposed by Holt, Bradshaw, Seamons, and Orman in 2003, and has been used to protect users' privacy[32,33]

extends the chosen-target computational Diffie-Hellman (CT-CDH) assumption, and prove that these two assumptions are equivalent.

Paper Organization
The rest of this paper is organized as follows. In Section 2, preliminaries required throughout this paper are described. In Section 3, two efficient oblivious transfer with access control schemes are proposed and proven. The complexity of the proposed schemes is analyzed. Section 4 concludes the paper.

2. Preliminaries

In this section, we review the definition and security model of oblivious transfer with access control and introduce the related assumptions. Based on the chosen-target computational Diffie-Hellman (CT-CDH) assumption, we propose the extended CT-CDH (XCT-CDH) assumption, and prove that they are equivalent.

Unless noted otherwise, in the rest of this paper, by $\omega \xleftarrow{R} \Omega$, we denote that ω is chosen at random from Ω. Especially, if Ω is a finite set, $\omega \xleftarrow{R} \Omega$ denotes that ω is chosen uniformly from Ω. By $R \xrightarrow{\Upsilon} S$ and $R \xleftarrow{\Upsilon} S$, we denote that party R sends Υ to party S, and party S sends Υ to party R, respectively. By $y \leftarrow A(x)$, we denote that y is obtained by running algorithm A on input x. We say that a function $\epsilon : \mathbb{Z} \rightarrow \mathbb{R}$ is a negligible function, if for all $c \in \mathbb{Z}$ there exists a $n \in \mathbb{Z}$ such that $|\epsilon(x)| < \frac{1}{x^c}$ for all $x > n$. By k, we denote a security parameter. We denote $\mathcal{KG}(1^k)$ as a key generator which takes as input k and outputs a secret-public key pair.

2.1. Definition and Security Model

There are three entities in an oblivious transfer with access control (OTAC) scheme: issuer I, sender S and receiver R. The issuer authenticates the receivers, and issues credentials to them. The senders send the selected services to the receivers. The receivers interact with the issuer and senders to obtain the required credentials and intended services. There are four algorithms in an oblivious transfer with access control scheme:

- Setup. Taking as input the security parameter k, this algorithm responds with the system public parameters PP. The issuer generates his secret-public key pair $(isk, ipk) \leftarrow \mathcal{KG}(1^k)$. The sender generates his secret-public key pair $(ssk, spk) \leftarrow \mathcal{KG}(1^k)$.

- Issue. Taking as input the secret key isk, the sender's identifier si and the receiver's identifier ri, it returns a credential to the receiver.

- Commit. Taking as input the secret key ssk and n messages $M_1, M_2, \cdots, M_n$, this algorithm returns n ciphertext $C_1, C_2, \cdots, C_n$.

- Transfer. Taking as input the intended indexes $\sigma_1, \sigma_2, \cdots, \sigma_t$ and the secret key ssk, respectively, the receiver and the sender interact. At the end, the receiver obtains the services $M_{\sigma_1}, M_{\sigma_2}, \cdots, M_{\sigma_t}$, while the sender knows nothing about the receiver's choice.

Correctness: An OTAC scheme is correct if the receiver can obtain his intended messages when the sender and the receiver follow the steps of the scheme.

Security Model. Since the seminal introduction of oblivious transfer, there have been many literatures that discuss its security. The security model of oblivious transfer can be classified into the following types: Honest-but curious model, half-simulation[36] and full-simulation[29,37].

Proposed by Naro and Pinkas[36] in 2005, the half-simulation is a model where the issues of protecting the receiver and the sender are separated. The security of the receiver requires that two transcripts which the receiver used to obtain services S_σ and $S_{\sigma'}$ are indistinguishable from the view of the sender. The security of the sender is defined by comparing the real world and the ideal world experiments. In the real world experiment, the receiver and the sender run the protocol. Meanwhile, in the ideal world experiment, the protocol is implemented by a trusted third party Charlie. For any malicious receiver $\mathcal{A}$ in the real world experiment, there exists a malicious receiver $\mathcal{A}'$ that plays the role of $\mathcal{A}$ in the ideal world experiment such that the outputs of $\mathcal{A}$ and $\mathcal{A}'$ are indistinguishable.

We define that an oblivious transfer with access control scheme is secure, if the following properties can be satisfied:

Privacy of the Receiver.

1. The receiver releases nothing about his PII to the sender.

2. For any two different choice sets $\mathcal{C} = \{\sigma_1, \sigma_2, \cdots, \sigma_t\}$ and $\mathcal{C}' = \{\sigma'_1, \sigma'_2, \cdots, \sigma'_t\}$, the transcripts received by the sender corresponding to $\mathcal{M} = \{M_{\sigma_1}, M_{\sigma_2}, \cdots, M_{\sigma_t}\}$ and $\mathcal{M}' = \{M_{\sigma'_1}, M_{\sigma'_2}, \cdots, M_{\sigma'_t}\}$ are indistinguishable. Especially, the choices of the receiver are unconditionally secure, if the received services $\{M_{\sigma_1}, M_{\sigma_2}, \cdots, M_{\sigma_t}\}$ and $\{M_{\sigma'_1}, M_{\sigma'_2}, \cdots, M_{\sigma'_t}\}$ are identically distributed.

Security of the Sender. Suppose that the receiver has possessed the required credentials from the issuer. To define the security of the sender, we compare the real world and the ideal world paradigms. In the real world, the receiver and the sender execute the protocol. Meanwhile, in the ideal world, the functionality is replaced by a trusted third party (TTP). The sender sends all his messages $\{M_1, M_2, \cdots, M_n\}$ to the TTP. The receiver sends his choices $\{\sigma_1, \sigma_2, \cdots, \sigma_t\}$ adaptively to the TTP. If $\{\sigma_1, \sigma_2, \cdots, \sigma_t\} \subset \{1, 2, \cdots, n\}$, the TTP sends $\{M_{\sigma_1}, M_{\sigma_2}, \cdots, M_{\sigma_t}\}$ to the receiver. An oblivious transfer with access control can protect the security of the sender, if for any receiver R in real world, there exists an probabilistic polynomial-time (PPT) receiver R' in the ideal world such that the outputs of R and R' are indistinguishable.

Semantic Security. If the receiver has not obtained the required credentials from the issuer, he can obtain nothing about the protected services.

2.2. Security Assumptions

Let $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_\tau$ be multiplicative cyclic groups with prime order p, namely $|\mathbb{G}_1| = |\mathbb{G}_2| = |\mathbb{G}_\tau| = p$. Let $g_1 \in \mathbb{G}_1$ and $g_2 \in \mathbb{G}_2$ be the generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. A bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_\tau$ satisfies the following properties:

1. Bilinearity. for all $\theta \in \mathbb{G}_1, \vartheta \in \mathbb{G}_2$ and $\alpha, \beta \in \mathbb{Z}_p$, $e(\theta^\alpha, \vartheta^\beta) = e(\theta, \vartheta)^{\alpha\beta}$.
2. No-degeneracy. $e(g_1, g_2) \neq 1$, where 1 is the identity in $\mathbb{G}_\tau$.
3. Computability. There exists an efficient algorithm to compute $e(\theta, \vartheta)$, for all $\theta \in \mathbb{G}_1, \vartheta \in \mathbb{G}_2$.

Let $\mathcal{GG}(1^k)$ be a bilinear group generator that takes as input k and output the description of groups $(\mathbb{G}_1,\ \mathbb{G}_2,\ \mathbb{G}_\tau)$ with prim order p and a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_\tau$. Let $\mathcal{G}(1^k)$ be a group generator which takes as input k and output the description of group $\mathbb{G}$ with prime order p

Definition 1. ℓ-Strong Diffie-Hellman (ℓ-SDH) Assumption[38]. *Let* $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_\tau) \leftarrow \mathcal{GG}(1^k)$ *be a bilinear group. Let* g_1 *and* g_2 *be the generators of* $\mathbb{G}_1$ *and* $\mathbb{G}_2$*, respectively. We say that* ℓ*-SDH assumption holds in* $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_\tau)$*, given* $\ell + 2$*-tuple* $(g_1, g_2, g_2^x, g_2^{x^2}, \cdots, g_2^{x^\ell})$*, if for all probabilistic polynomial-time adversary* $\mathcal{A}$

$$Adv_{\mathcal{A}}^{\ell-SDH}(k) = Pr[(\gamma, g_1^{\frac{1}{x+\gamma}} \leftarrow \mathcal{A}(g_1, g_2, g_2^x, g_2^{x^2}, \cdots, g_2^{x^\ell}))] \leq \epsilon(k)$$

where the probability is over the random choice of $x \in \mathbb{Z}_p^*$ *and the random bits consumed by* $\mathcal{A}$*.*

Definition 2. Chosen-target Computational Diffie-Hellman (CT-CDH) Assumption[39]. *Let* g *be a generator of group* $\mathbb{G} \leftarrow \mathcal{G}(1^k)$ *with prime order* p *and* $x \overset{R}{\leftarrow} \mathbb{Z}_p$*. Let* $\mathcal{H} : \{0,1\}^* \rightarrow \mathbb{G}$ *be a cryptographic hash function. There are two oracles* $T_G(\cdot)$ *and* $H_G(\cdot)$*.* $T_G(\cdot)$ *is called the target oracle, which takes as input* $j \in \mathbb{Z}_p$*, and responds with* $g_j \in \mathbb{G}$*.* $H_G(\cdot)$ *is called the help oracle, which takes as input* $g_j \in \mathbb{G}$*, and returns* $g_j^x \in \mathbb{G}$*. Let* Q_T *and* Q_H *denote the numbers that the two oracles are queried, respectively. CT-CDH assumption holds in* $\mathbb{G}$*, if for all probabilistic polynomial-time adversary* $\mathcal{A}$

$$Adv_{\mathcal{A}}^{CT-CDH}(1^k) \;=\; \Pr\left[\begin{array}{l} ((\psi_1, i_1), \cdots, (\psi_{\pi+1}, i_{\pi+1})) \leftarrow \\ \mathcal{A}^{T_G(\cdot), H_G(\cdot)}(g, g^x, \mathcal{H}, p) \end{array}\right] \leq \epsilon(k)$$

where $\psi_l = g_{i_l}^x$*, for* $l = 1, 2, \cdots, \pi + 1$*, and* $Q_H < \pi + 1 \leq Q_T$*.*

Intuitively, CT-CDH assumption demonstrates that the adversary can query the help oracle on at most π elements in $\mathbb{G}$, and get back with these elements to the power x. If the orders of these π elements on the generator of $\mathbb{G}$ are unknown, the adversary can not compute a new element in $\mathbb{G}$ to the power of x, which orders on the generator and the π queried elements are unknown. Based on CT-CDH assumption, we propose the extended CT-CDH (XCT-CDH) assumption. We replace the target oracle in CT-CDH assumption with $\pi + 1$ random elements of $\mathbb{G}$. We will proof that the XCT-CD assumption and the CT-CDH assumption are equivalent.

Definition 3. E$\mathbb{X}$tended Chosen-target Computational Diffie-Hellman (XCT-CDH) Assumption. *Let* g *be a generator of the group* $\mathbb{G} \leftarrow \mathcal{G}(1^k)$ *with prime order* p*, and* $x \overset{R}{\leftarrow} \mathbb{Z}_p$*. There is a help oracle* $H_G(\cdot)$*, which takes as input* $g_j \in \mathbb{G}$*, returns* $g_j^x \in \mathbb{G}$*. Given* $(\pi + 1)$*-tuple* $\{g^{a_1}, g^{a_2}, \cdots, g^{a_{\pi+1}}\}$*, where*

$a_l \xleftarrow{R} \mathbb{Z}_p^*$ for $l = 1, 2, \cdots, \pi + 1$, XCT-CDH assumption holds in $\mathbb{G}$, if for all probabilistic polynomial-time adversary $\mathcal{A}$

$$Adv_{\mathcal{A}}^{XCT-CDH}(K) = Pr[g^{xa_{i_{\pi+1}}} \leftarrow \mathcal{A}^{H_G(\cdot)}(p, g, g^x, g^{a_{i_1}}, g^{a_{i_2}}, \cdots, g^{a_{i_\pi}})] \leq \epsilon(k)$$

where $a_{i_l} \in \{a_1, a_2, \cdots, a_{\pi+1}\}$, for $l = 1, 2, \cdots, \pi + 1$.

Theorem 1. *Chosen-target computational Diffie-Hellman (CT-CDH) assumption and extended chosen-target computational Diffie-Hellman (XCT-CDH) assumption are equivalent.*

Proof. Given $\{g^{a_1}, g^{a_2}, \cdots, g^{a_{\pi+1}}\}$, we define $\mathcal{H} : l \rightarrow g^{a_{i_l}} \in \mathbb{G}$, where $a_{i_l} \in \{a_1, a_2, \cdots, a_{\pi+1}\}$, for $l \in \{1, 2, \cdots, \pi + 1\}$; otherwise $\mathcal{H} : l \rightarrow g^{b_l}$, where $b_l \xleftarrow{R} \mathbb{Z}_p$. So, $\mathcal{H}(\cdot)$ is a cryptographic hash function.

On the one hand, if the adversary $\mathcal{A}$ can break the CT-CDH assumption, we will show that there exists an algorithm $\mathcal{B}$, who can uses $\mathcal{A}$ to break the XCT-CDH assumption. Given $\{g^{a_1}, g^{a_2}, \cdots, g^{a_{\pi+1}}\}$, for Q_T ($Q_T \leq \pi+1$) target oracle queries, the challenger returns $g^{a_{i_1}}, g^{a_{i_2}}, \cdots, g^{a_{i_{Q_T}}}$, where $a_{i_j} \in \{a_1, a_2, \cdots, a_{\pi+1}\}$, for $j = 1, 2, \cdots, Q_T$. For Q_H ($Q_H \leq \pi$) help oracle queries, the challenger queries the help oracle $H_G(\cdot)$ in the XCT-CDH assumption, and returns $g^{xa_{i_1}}, g^{xa_{i_2}}, \cdots, g^{xa_{i_{Q_H}}}$, where $a_{i_t} \in \{a_1, a_2, \cdots, a_{\pi+1}\}$, for $t = 1, 2, \cdots, Q_H$. If $\mathcal{A}$ can compute $\psi_{\pi+1} = g_{i_{\pi+1}}^x$, $\mathcal{B}$ can compute $g^{xa_{i_{\pi+1}}} = g_{i_{\pi+1}}^x$, where $\mathcal{H}(\pi + 1) = g_{i_{\pi+1}} = g^{a_{i_{\pi+1}}}$. So, $\mathcal{B}$ can break XCT-CDH assumption.

On the other hand, if $\mathcal{A}$ can break the XCT-CDH assumption, we will show that there exists an algorithm $\mathcal{B}$, who can use $\mathcal{A}$ to break the CT-CDH assumption. When $\mathcal{A}$ queries help oracle on $\{g^{a_{i_1}}, g^{a_{i_2}}, \cdots, g^{a_{i_\pi}}\}$, the challenger queries the help oracle $H_G(\cdot)$ in CT-CDH assumption, and gets back with $\{g^{xa_{i_1}}, g^{xa_{i_2}}, \cdots, g^{xa_{i_\pi}}\}$, where $\pi = Q_H$. If $\mathcal{A}$ can outputs $g^{xa_{i_{\pi+1}}}$, $\mathcal{B}$ can compute $\psi_{\pi+1} = g_{i_{\pi+1}}^x$, where $\mathcal{H}(\pi + 1) = g_{i_{\pi+1}} = g^{a_{i_{\pi+1}}}$ and $\pi + 1 = Q_H + 1 > Q_H$. So, $\mathcal{B}$ can break the CT-CDH assumption.

Therefore, the chosen-target computational Diffie-Hellman (CT-CDH) assumption and the extended chosen-target computational Diffie-Hellman (XCT-CDH) assumption are equivalent.

Note that the extended chosen-target computational Diffie-Hellman (XCT-CDH) assumption is computational Diffie-Hellman (CDH) assumption, if the help oracle $H_G(\cdot)$ in XCT-CDH assumption is canceled.

Indistinguishability. We define that two distribution families $\Omega_1(k)$ and $\Omega_2(k)$ are (statistically) indistinguishable, if

$$\sum_y |Pr_{x\in\Omega_1(k)}[x=y] - Pr_{x\in\Omega_2(k)}[x=y]| \leq \epsilon(k)$$

3. Oblivious Transfer with Access Control

In this section, two efficient oblivious transfer with access control schemes are proposed. The first one is very simple, while the credentials of the receiver are transferable. Comparatively, the second one sacrifices a little efficiency, while the credentials of the receiver are all-or-nothing nontransferable, which means that all credentials are shared, if the receiver share one with others[8].

Overview. Our idea is as follows: at first, the receiver interacts with the issuer to obtain a credential, which is a signature on a public message, for example the identifier of the sender in the trusted circle [2]. Then, the sender commits his services using OSBE under the public message and *his private key.* Finally, the receiver interacts with the sender, decrypts the ciphertexts using the possessed credential, and obtains the intended services. In our schemes, only the qualified receivers can obtain services from the sender obliviously, while are not required to authenticate (proof) himself to the sender in zero knowledge. Additionally, nothing about the protected services can be released to the illegal receiver, who has not obtained the required credentials from the issuer.

3.1. Oblivious Transfer with Access Control-I

Based on the short signature[38] and the oblivious transfer[40], we proposed an oblivious transfer with access control scheme AC-OT$^n_{k\times 1}$-I, where only the receiver who has possessed the required credential can get services from the sender adaptively, without releasing anything about his PII and the contents of the selected service to the sender. The sender knows how many services the receiver can obtain if he has possessed a credential, but knows nothing about the credential of the receiver. AC-OT$^n_{k\times 1}$-I is described in Fig. 1.

Theorem 2. *AC-OT$^n_{k\times 1}$-I is correct.*

[2]Trusted circle is a domain where all participants trust the issuer.

Setup. Taking as input a security parameter λ, this algorithm outputs a bilinear group $(e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_\tau) \leftarrow \mathcal{GG}(1^\lambda)$ with prime order q, where $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_\tau$. Let g and h be the generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. The issuer I generates his private-public key pair $(x, y) \leftarrow \mathcal{KG}(1^\lambda)$, where $x \xleftarrow{R} \mathbb{Z}_q^*$ and $y = h^x$. The sender S generates his private-public key pair $(z, Z) \leftarrow \mathcal{KG}(1^\lambda)$, where $z \xleftarrow{R} \mathbb{Z}_q^*$ and $Z = e(g, h)^z$. The issuer selects $r \xleftarrow{R} \mathbb{Z}_q^*$, and sends r to the sender [a], where $z \not\equiv x + r \pmod q$ and $r + x \not\equiv 0, 1 \pmod{\text{q}}$.

Issue. The issuer computes $\sigma = g^{\frac{1}{x+r}}$, and sends (σ, r) to the the receiver R. R checks $e(\sigma, yh^r) \stackrel{?}{=} e(g, h)$.

Suppose that S has messages $M_1, M_2, \cdots, M_n \in \mathbb{G}_\tau$.

Commitment Phase. S chooses $t_1, t_2, \cdots, t_n \xleftarrow{R} \mathbb{Z}_q^*$, and computes $T = yh^r$ and $C_i = (C_{i,1}, C_{i,2})$, where $C_{i,1} = T^{t_i}$ and $C_{i,2} = e(g, h)^{zt_i} \cdot M_i$, for $i = 1, 2, \cdots, n$. S sends $\{(C_1, C_2, \cdots, C_n)\}_{i=1}^n$ to R.

Transfer Phase.

1. R chooses $s_j \xleftarrow{R} \mathbb{Z}_q^*$, and computes

$$A_{i_j} = e(\sigma, C_{i_j,1}) = e(g, h)^{t_{i_j}}, \quad B_{i_j} = A_{i_j}^{s_j}$$

   where $i_j \in \{1, 2, \cdots, n\}$ and $j \in \{1, 2, \cdots, k\}$.
2. $R \xrightarrow{B_{i_j}} S$.
3. $R \xleftarrow{D_{i_j}} S$. S computes $D_{i_j} = (B_{i_j})^z$, and sends D_{i_j} to R.
4. R computes $E_{i_j} = D_{i_j}^{s_j^{-1}}$ and $M_{i_j} = \frac{C_{i_j,2}}{E_{i_j}}$.

[a] r is the identifier of the sender in the trusted circle.

Figure 1: Oblivious Transfer with Access Control-I (AC-OT$_{k\times 1}^n$-I)

Proof. If the receiver R holds a credential (σ, r), he can compute

$$\begin{aligned} A_{i_j} &= e(\sigma, C_{i_j,1}) \\ &= e(g^{\frac{1}{x+r}}, (yh^r)^{t_{i_j}}) \\ &= e(g^{\frac{1}{x+r}}, h^{x+r})^{t_{i_j}} \\ &= e(g, h)^{t_{i_j}}, \end{aligned}$$

and

$$\begin{aligned}
\frac{C_{i_j,2}}{E_{i_j}} &= \frac{e(g,h)^{zt_{i_j}} \cdot M_{i_j}}{D_{i_j}^{s_j^{-1}}} \\
&= \frac{e(g,h)^{zt_{i_j}} \cdot M_{i_j}}{B_{i_j}^{zs_j^{-1}}} \\
&= \frac{e(g,h)^{zt_{i_j}} \cdot M_{i_j}}{A_{i_j}^{z}} \\
&= \frac{e(g,h)^{zt_{i_j}} \cdot M_{i_j}}{e(g,h)^{zt_{i_j}}} \\
&= M_{i_j}.
\end{aligned}$$

Theorem 3. *AC-$OT^n_{k\times 1}$-I is unconditionally receiver-secure.*

Proof. For any B_{i_j} received by the sender from the receiver, there exists an $s_w \in \mathbb{Z}_q (w \neq j)$ such that $B_{i_j} = A_{i_j}^{s_j} = e(g,h)^{s_j t_{i_j}} = e(g,h)^{s_w t_{i_w}} = A_{i_w}^{s_w} = B_{i_w}$, namely $s_w = \frac{s_j t_{i_j}}{t_{i_w}} \bmod q$.

So, from the view of the sender, B_{i_j} is computed from $C_{i_j,1}$ or $C_{i_w,1}$ is identically distributed. AC-$\mathrm{OT}^n_{k\times 1}$-I is unconditionally receiver-secure.

Theorem 4. *AC-$OT^n_{k\times 1}$-I is sender-secure, if the the XCT-CDH assumption holds in $\mathbb{G}_\tau$.*

Proof. For any probabilistic polynomial-time malicious receiver $\hat{R}$ in the real model, we can construct an probabilistic polynomial-time malicious receiver $\hat{R}^*$ in the ideal model such that the outputs of $\hat{R}$ and $\hat{R}^*$ are indistinguishable.

1. S sends $M_1, M_2, \cdots, M_n$ to the trusted third party Charlie.
2. $\hat{R}^*$ sends $C_1^*, C_2^*, \cdots, C_n^*$ to Charlie, where $C_i^* = (C_{i_1}^*, C_{i_2}^*) \xleftarrow{R} \mathbb{G}_\tau^2$, for $i = 1, 2, \cdots, n$.
3. $\hat{R}^*$ monitors the outputs of $\hat{R}$. If $\hat{R}$ can compute $A_{i_1}, A_{i_2}, \cdots, A_{i_k}$ and $B_{i_1}, B_{i_2}, \cdots, B_{i_k}$, $\hat{R}^*$ chooses $A_{i_1}^*, A_{i_2}^*, \cdots, A_{i_k}^*$ and $B_{i_1}^*, B_{i_2}^*, \cdots, B_{i_k}^*$, where $A_{i_v}^*, B_{i_v}^* \xleftarrow{R} \mathbb{G}_\tau$, for $v = 1, 2, \cdots, k$.

4. When $\hat{R}$ takes as input $B_{i_1}, B_{i_2}, \cdots, B_{i_k}$ to obtain $D_{i_1}, D_{i_2}, \cdots, D_{i_k}$, $\hat{R}^*$ queries the help oracle $H_{\mathbb{G}_\tau}(\cdot)$ on $B^*_{i_1}, B^*_{i_2}, \cdots, B^*_{i_k}$, and gets back with $D^*_{i_1}, D^*_{i_2}, \cdots, D^*_{i_k}$, where $D^*_{i_w} = B^{z^*}_{i_j}$, for $w = 1, 2, \cdots, k$.

5. If $\hat{R}$ can compute $E_{i_j} = e(g,h)^{zt_{i_j}}$, $\hat{R}^*$ sends i_j to Charlie. Charlie returns $\frac{C^*_{i_j,2}}{M_{i_j}}$.

6. $\hat{R}^*$ outputs $(A^*_{i_1}, A^*_{i_2}, \cdots, A^*_{i_k}, B^*_{i_1}, B^*_{i_2}, \cdots, B^*_{i_k},\ D^*_{i_1}, D^*_{i_2}, \cdots, D^*_{i_k}, C^*_1, C^*_2, \cdots, C^*_n)$.

If $\hat{R}$ obtains $k+1$ messages, $\hat{R}^*$ does not know which k indices are really selected by $\hat{R}$. The simulation fails. Otherwise, we will show that $\hat{R}$ can get at most k messages under the XCT-CDH assumption. If $\hat{R}$ can get $k+1$ messages, he can compute E_{i_j}, for $j = 1, 2, \cdots, k+1$. Namely, after receiving $(e(g,h)^{t_{i_1}})^z, (e(g,h)^{t_{i_2}})^z, \cdots, (e(g,h)^{t_{i_k}})^z$, $\hat{R}$ can compute $(e(g,h)^{t_{i_{k+1}}})^z$. This contradicts to the XCT-CDH assumption. So, $\hat{R}$ can obtain at most k messages from the sender.

$\{A_{i_1}, A_{i_2}, \cdots, A_{i_k}\}$ and $\{B_{i_1}, B_{i_2}, \cdots, B_{i_k}\}$ are random elements in $\mathbb{G}_\tau$. $C_1, C_2, \cdots, C_n$ are random elements in $\mathbb{G}_2 \times \mathbb{G}_\tau$. $\{D_{i_1}, D_{i_2}, \cdots, D_{i_k}\}$ and $\{D^*_{i_1}, D^*_{i_2}, \cdots, D^*_{i_k}\}$ are identically distributed. Therefore, the outputs of $\hat{R}$ and $\hat{R}^*$ are indistinguishable.

Theorem 5. *AC-$OT^n_{k\times 1}$-I is semantically secure under the ℓ-SDH assumption and XCT-CDH assumption.*

Proof. There are two types adversaries:

Type-I: The adversary can compute $A_i = e(g,h)^{t_i}$, then he can act as the authorized receiver to interact with the sender.

Type-II: The adversary can compute the decryption key $e(g,h)^{zt_i}$ from C_i.

We will show that Type-I adversary can be used to break the ℓ-SDH assumption or XCT-CDH assumption and Type-II adversary can be used to break the XCT-CDH assumption.

Type-I: Suppose that $\mathcal{A}$ is Type-I adversary.

1. If $\mathcal{A}$ can compute the signature (σ, r), then compute A_i, B_i, and E_i, there exists an algorithm $\mathcal{B}$ can use $\mathcal{A}$ to break the ℓ-SDH assumption [3].

2. If $\mathcal{A}$ can not compute σ, he can compute A_i from $C_{i,1} = (yh^r)^{t_i}$. If it is, there exists an algorithm $\mathcal{B}$ who can use $\mathcal{A}$ to break the XCT-CDH assumption as follows: Given $e(g, C_{i,1}) = (e(g,h)^{x+r})^{t_i}$ and $e(g,h)$, the aim of $\mathcal{B}$ is to compute $e(g,h)^{t_i}$. $\mathcal{B}$ sends $C_{i,1}$ to $\mathcal{A}$, if $\mathcal{A}$ can compute $e(g,h)^{t_i}$, $\mathcal{B}$ aborts. $\mathcal{B}$ can use $\mathcal{A}$ to break the XCT-CDH assumption.

Type-II: Suppose that $\mathcal{A}$ is Type-II adversary. If $\mathcal{A}$ can compute $e(g,h)^{zt_i}$ from $C_{i,1}$, there exists an algorithm $\mathcal{B}$ can uses $\mathcal{A}$ to break the XCT-CDH assumption as follows: Given $(e(g,h)^{x+r})^{t_i}$, and $e(g,h)^z$, the aim of $\mathcal{B}$ is to compute $(e(g,h)^z)^{t_i}$. $\mathcal{B}$ sends $C_i = (C_{i,1}, C_{i,2})$ to $\mathcal{A}$. If $\mathcal{A}$ can compute M_i, $\mathcal{B}$ aborts. $\mathcal{B}$ can compute $e(g,h)^{zt_i} = \frac{C_{i,2}}{M_i}$. So $\mathcal{B}$ can use $\mathcal{A}$ to break the XCT-CDH assumption.

Therefore, AC-OT$^n_{k\times 1}$-I is semantically secure.

Complexity. Suppose that $e(g,h)$ can be pre-computed. In the setup stage, the issuer needs to compute one exponentiation, and send one element in $\mathbb{Z}_q$ to the sender. The sender needs to compute one exponentiation. In the issue phase, the issuer needs to compute one exponentiation, and send one element in $\mathbb{G}_1$ and one element in $\mathbb{Z}_p$ to the receiver. The receiver needs to compute one exponentiation and one pairing. In the commitment phase, the sender needs to compute $2n+1$ exponentiations, and send n elements in $\mathbb{G}_2$ and n elements in $\mathbb{G}_\tau$ to the receiver. In the transfer phase, The receiver needs to computes k pairings and $2k$ exponentiations, and send k elements in $\mathbb{G}_\tau$ to the sender. The sender needs to compute k exponentiations, and sends k elements in $\mathbb{G}_\tau$ to the receiver. The costs of computation and communication in our AC-OT$^n_{k\times 1}$-I are listed in TABLE 1 and TABLE 2, respectively. By e and p, we denote one exponentiation and one paring computing, respectively. By E_1, E_τ and E_q, we denote one element in $\mathbb{G}_1$, $\mathbb{G}_\tau$ and $\mathbb{G}_q$, respectively.

[3] The short signature is existentially unforgeable against the weakly chosen message attack under the ℓ-SDH assumption[38].

3.2. Oblivious Transfer with Access Control-II

Based on the signature[17] [4], and the oblivious transfer[40], we propose an oblivious transfer with access control AC-OT$^n_{k\times 1}$-II, where only the authorized receivers can obtain services from the sender adaptively. The sender knows the number of the services the receiver can obtain if he has been authorized, but knows nothing about the contents of the selected services. Additionally, the credential of the receiver is all-or-nothing non-transferable. Namely, our scheme captures the following properties:

1. Zero knowledge proof is not required.
2. The receiver is not required to authenticate himself to the sender.
3. The sender knows the number of the services that can be obtained by the authorized receiver, and nothing about the contents of the selected services.
4. The receiver can not share his credentials with others.

AC-OT$^n_{k\times 1}$-II is described in Fig 2.

Theorem 6. *AC-OT$^n_{k\times 1}$-II is correct.*

Proof. If the receiver R has obtained a credential (σ, s, r), he can compute

$$\begin{aligned} A_{i_j} &= e(\sigma, C_{i_j,1}) \\ &= e((g_0 g_1^s g_2^{x_u})^{\frac{1}{x+r}}, (yh^r)^{t_{i_j}}) \\ &= e((g_0 g_1^s g_2^{x_u})^{\frac{1}{x+r}}, h^{x+r})^{t_{i_j}} \\ &= e(g_0 g_1^s g_2^{x_u}, h)^{t_{i_j}} \\ &= e(g_0, h)^{t_{i_j}} e(g_1, h)^{st_{i_j}} e(g_2, h)^{x_u t_{i_j}}, \end{aligned}$$

$$\begin{aligned} B_{i_j} &= (\frac{A_{i_j}}{C_{i_j,2}^s C_{i_j,3}^{x_u}})^{s_j} \\ &= (\frac{e(g_0, h)^{t_{i_j}} e(g_1, h)^{st_{i_j}} e(g_2, h)^{x_u t_{i_j}}}{e(g_1, h)^{st_{i_j}} e(g_2, h)^{x_u t_{i_j}}})^{s_j} \\ &= e(g_0, h)^{s_j t_{i_j}}, \end{aligned}$$

[4] This signature scheme was proposed by Boneh, Boyen and Shacham[41], and modified and proven secure by Au, Susilo, and Mu[17].

Setup. Taking as input a security parameter λ, this algorithm outputs a bilinear group $(e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_\tau) \leftarrow \mathcal{GG}(1^\lambda)$ with prime order q, where $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_\tau$. Let g_0, g_1, g_2, g_3 be the generators of $\mathbb{G}_1$, and h be the generator of $\mathbb{G}_2$, respectively. The issuer I generates his private-public key pair $(x, y) \leftarrow \mathcal{KG}(1^\lambda)$, where $x \xleftarrow{R} \mathbb{Z}_q^*$ and $y = h^x$. The receiver R generates his private-public key pair $(x_u, y_u) \leftarrow \mathcal{KG}(1^\lambda)$, where $x_u \xleftarrow{R} \mathbb{Z}_q^*$ and $y_u = g_2^{x_u}$. The sender S generates his private-public key pair $(z, Z) \leftarrow \mathcal{KG}(1^\lambda)$, where $z \xleftarrow{R} \mathbb{Z}_q^*$ and $Z = e(g_0, h)^z$. The issuer selects $r \xleftarrow{R} \mathbb{Z}_q^*$, and sends r to the sender [a], where $z \not\equiv x+r \pmod q$ and $x + r \not\equiv 0, 1 \pmod q$.

Issue. The issuer chooses $s \xleftarrow{R} \mathbb{Z}_q^*$, computes $\sigma = (g_0 g_1^s g_2^{x_u})^{\frac{1}{x+r}}$, and sends (σ, r, s) to the receiver R. R checks $e(\sigma, yh^r) \stackrel{?}{=} e(g_0 g_1^s g_2^{x_u}, h)$.

Commitment Phase. Suppose that S has messages $M_1, M_2, \cdots, M_n \in \mathbb{G}_\tau$. S chooses $t_1, t_2, \cdots, t_n \xleftarrow{R} \mathbb{Z}_q^*$, and computes $T = yh^r$ and $(C_{i,1}, C_{i,2}, C_{i,3}, C_{i,4})$, where $C_{i,1} = T^{t_i}$, $C_{i,2} = e(g_1, h)^{t_i}$, $C_{i,3} = e(g_2, h)^{t_i}$, $C_{i,4} = e(g_0, h)^{zt_i} \cdot M_i$, for $i = 1, 2, \cdots, n$. S sends $\{(C_{i,1}, C_{i,2}, C_{i,3}, C_{i,4})\}_{i=1}^n$ to R.

Transfer Phase.

1. R chooses $s_j \xleftarrow{R} \mathbb{Z}_q^*$, and computes

$$A_{i_j} = e(\sigma, C_{i_j,1}) = e(g_0, h)^{t_{i_j}} e(g_1, h)^{st_{i_j}} e(g_2, h)^{x_u t_{i_j}}$$

$$B_{i_j} = (\frac{A_{i_j}}{C_{i_j,2}^s C_{i_j,3}^{x_u}})^{s_j} = e(g_0, h)^{s_j t_{i_j}}$$

   where $i_j \in \{1, 2, \cdots, n\}$ and $j \in \{1, 2, \cdots, k\}$.
2. $R \xrightarrow{B_{i_j}} S$.
3. $R \xleftarrow{D_{i_j}} S$. S computes $D_{i_j} = (B_{i_j})^z$, and sends D_{i_j} to R.
4. R computes $E_{i_j} = D_{i_j}^{s_j^{-1}}$ and $M_{i_j} = \frac{C_{i,4}}{E_{i_j}}$.

[a] r is the identifier of the sender in the trusted circle.

Figure 2: Oblivious Transfer with Access Control-II (AC-OT$^n_{k\times 1}$-II)

$$E_{i_j} = D_{i_j}^{s_j^{-1}} = B_{i_j}^{zs_j^{-1}} = e(g_0, h)^{zt_{i_j}},$$

and

$$\begin{aligned} \frac{C_{i_j,4}}{E_{i_j}} &= \frac{e(g_0, h)^{zt_{i_j}} \cdot M_{i_j}}{e(g_0, h)^{zt_{i_j}}} \\ &= M_{i_j}. \end{aligned}$$

Theorem 7. *AC-OT$^n_{k\times 1}$-II is unconditionally receiver-secure.*

Proof. For any B_{i_j} received by the sender from the receiver, there exists an $s_u \in \mathbb{Z}_q (u \neq j)$ such that $B_{i_j} = A_{i_j}^{s_j} = e(g, h)^{s_j t_{i_j}} = e(g, h)^{s_u t_{i_u}} = A_{i_u}^{s_u} = B_{i_u}$, namely $s_u = \frac{s_j t_{i_j}}{t_{i_u}} \bmod q$.

Hence, from the view of the sender, B_{i_j} is computed from $C_{i_j,1}$ or $C_{i_u,1}$ is identically distributed. AC-OT$^n_{k\times 1}$-II is unconditionally receiver-secure.

Theorem 8. *AC-OT$^n_{k\times 1}$-II is sender-secure, if the XCT-CDH assumption holds in $\mathbb{G}_\tau$.*

Proof. For any probabilistic polynomial-time malicious $\hat{R}$ in the real model, we can construct an probabilistic polynomial-time malicious $\hat{R}^*$ in the ideal model such that the outputs of $\hat{R}$ and $\hat{R}^*$ are indistinguishable.

1. S sends $M_1, M_2, \cdots, M_n$ to the trusted third party Charlie.
2. $\hat{R}^*$ sends $C_1^*, C_2^*, \cdots, C_n^*$ to Charlie, where $C_i^* = (C_{i_1}^*, C_{i_2}^*, C_{i_3}^*, C_{i_4}^*) \xleftarrow{R} \mathbb{G}_2 \times \mathbb{G}_\tau^3$, for $i = 1, 2, \cdots, n$.
3. $\hat{R}^*$ monitors the outputs of $\hat{R}$. If $\hat{R}$ can compute $A_{i_1}, A_{i_2}, \cdots, A_{i_k}$ and $B_{i_1}, B_{i_2}, \cdots, B_{i_k}$, $\hat{R}^*$ chooses $A_{i_1}^*, A_{i_2}^*, \cdots, A_{i_k}^*$ and $B_{i_1}^*, B_{i_2}^*, \cdots, B_{i_k}^*$, where $A_{i_w}^*, B_{i_w}^* \xleftarrow{R} \mathbb{G}_\tau$, for $w = 1, 2, \cdots, k$.
4. When $\hat{R}$ takes as input $B_{i_1}, B_{i_2}, \cdots, B_{i_k}$ to obtain $D_{i_1}, D_{i_2}, \cdots, D_{i_k}$, $\hat{R}^*$ queries the help oracle $H_{\mathbb{G}_\tau}(\cdot)$ on $B_{i_1}^*, B_{i_2}^*, \cdots, B_{i_k}^*$, and gets back with $D_{i_1}^*, D_{i_2}^*, \cdots, D_{i_k}^*$, where $D_{i_w}^* = B_{i_w}^{z^*}$, for $w = 1, 2, \cdots, k$.
5. If $\hat{R}$ can compute $E_{i_j} = e(g_0, h)^{zt_{i_j}}$, $\hat{R}^*$ sends i_j to Charlie. Charlie returns $\frac{C_{i_j,4}^*}{M_{i_j}}$.

6. $\hat{R}^*$ outputs $(A^*_{i_1}, A^*_{i_2}, \cdots, A^*_{i_k}, B^*_{i_1}, B^*_{i_2}, \cdots, B^*_{i_k},\ D^*_{i_1}, D^*_{i_2}, \cdots, D^*_{i_k}, C^*_1, C^*_2, \cdots, C^*_n)$.

If $\hat{R}$ obtains $k+1$ messages, $\hat{R}^*$ does not know which k indices are really selected by $\hat{R}$. The simulation fails. Otherwise, we will show that $\hat{R}$ can get at most k messages under the XCT-CDH assumption. If $\hat{R}$ can get $k+1$ messages, he can compute E_{i_j}, for $j = 1, 2, \cdots, k+1$. Namely, after receiving $(e(g_0, h)^{t_{i_1}})^z, (e(g_0, h)^{t_{i_2}})^z, \cdots, (e(g_0, h)^{t_{i_k}})^z$, $\hat{R}$ can compute $(e(g_0, h)^{t_{i_{k+1}}})^z$. This contradicts to the XCT-CDH assumption. Hence, $\hat{R}$ can obtain at most k messages.

$\{A_{i_1}, A_{i_2}, \cdots, A_{i_k}\}$ and $\{B_{i_1}, B_{i_2}, \cdots, B_{i_k}\}$ are random elements in $\mathbb{G}_\tau$. $\{C_1, C_2, \cdots, C_n\}$ are random elements in $\mathbb{G}_2 \times \mathbb{G}^3$. $\{D_{i_1}, D_{i_2}, \cdots, D_{i_k}\}$ and $\{D^*_{i_1}, D^*_{i_2}, \cdots, D^*_{i_k}\}$ are identically distributed.

Therefore, the outputs of $\hat{R}$ and $\hat{R}^*$ are indistinguishable.

Theorem 9. *AC-OT$^n_{k\times 1}$-II is semantically secure under the ℓ-SDH assumption and XCT-CDH assumption.*

Proof. There are two types adversaries:

Type-I: The adversary can compute $\hat{A}_i = e(g, h)^{t_i}$, then he can act as the authorized receiver to interact with the sender.

Type-II: The adversary can compute the decryption key $e(g, h)^{zt_i}$ from C_i.

We will show that Type-I adversary can be used to break the ℓ-SDH assumption or XCT-CDH assumption and Type-II adversary can be used to break the XCT-CDH assumption.

Type-I: Suppose that $\mathcal{A}$ is Type-I adversary.

1. If $\mathcal{A}$ can forge a signature (σ^*, r, s^*) on x^*_u, then compute $A_i, B_i,$ and E_i, there exists an algorithm $\mathcal{B}$ who can use $\mathcal{A}$ to break the ℓ-SDH assumption [5].

[5]The signature is existentially unforgeable against the adaptively chosen messages attack under ℓ-SDH assumption[17].

2. If $\mathcal{A}$ can not compute (σ^*, r, s^*), he can compute $\hat{A}_i$ from $C_{i,1}, C_{i,2}$, $C_{i,3}$. If it is, there exists an algorithm $\mathcal{B}$ can use $\mathcal{A}$ to break the XCT-CDH assumption as follows: Given $e(g, C_{i,1}) = (e(g,h)^{x+r})^{t_i}$, $e(g_1,h)^{t_i}$, $e(g_2,h)^{t_i}$ and $e(g_0,h)$, the aim of $\mathcal{B}$ is to compute $e(g_0,h)^{t_i}$. $\mathcal{B}$ sends $C_{i,1}, C_{i,2}$, $C_{i,3}$ to $\mathcal{A}$, if $\mathcal{A}$ can compute $e(g_0,h)^{t_i}$, $\mathcal{B}$ aborts. $\mathcal{B}$ can use $\mathcal{A}$ to break the XCT-CDH assumption.

Type-II: Suppose that $\mathcal{A}$ is Type-II adversary. If $\mathcal{A}$ can compute $e(g_0,h)^{zt_i}$ from $C_{i,1}, C_{i,2}, C_{i,3}$, there exists an algorithm $\mathcal{B}$ can uses $\mathcal{A}$ to break the XCT-CDH assumption as follows: Given $e(g, C_{i,1}) = (e(g,h)^{x+r})^{t_i}$, $e(g_1,h)^{t_i}$, $e(g_2,h)^{t_i}$ and $Z = e(g_0,h)^z$, the aim of $\mathcal{B}$ is to compute $(e(g_0,h)^z)^{t_i}$. $\mathcal{B}$ sends $C_i = (C_{i,1}, C_{i,2}, C_{i,3}, C_{i,4})$ to $\mathcal{A}$, if $\mathcal{A}$ can compute M_i, $\mathcal{B}$ aborts. $\mathcal{B}$ can compute $e(g_0,h)^{zt_i} = \frac{C_{i,4}}{M_i}$. So, $\mathcal{B}$ can use $\mathcal{A}$ to break the XCT-CDH assumption.

Therefore, AC-OT$^n_{k\times 1}$-II is semantically secure.

Complexity. Suppose that $e(g_0,h)$, $e(g_1,h)$ and $e(g_2,h)$ can be pre-computed. In the setup stage, the issuer needs to compute one exponentiation, and send one element in $\mathbb{Z}_q$ to the sender. The receiver needs to compute one exponentiation. The sender needs to compute one exponentiation. In the issue phase, the issuer needs to compute two exponentiations and send one element in $\mathbb{G}_1$ and two elements in $\mathbb{Z}_q$ to the receiver. The receiver needs to compute two exponentiations and two parings. In the commitment phase, the sender needs to compute $4n+1$ exponentiations, and send n elements in $\mathbb{G}_2$ and $3n$ elements in $\mathbb{G}_\tau$ to the receiver. In the transfer phase, The receiver needs to computes k pairings and $4k$ exponentiations, and send k elements in $\mathbb{G}_\tau$ to the sender. The sender needs to compute k exponentiations, and sends k elements in $\mathbb{G}_\tau$ to the receiver. The costs of computation and communication in our AC-OT$^n_{k\times 1}$-II are listed in TABLE 3 and TABLE 4, respectively.

4. Conclusion

One of the fundamental challenges in open communication channel is to protect user's privacy, including both PII and the selected services. In this paper, we proposed two efficient oblivious transfer with access control schemes. In our schemes, the receiver can obtain services from the sender

adaptively if he has been authorized by the issuer. The sender knows the number of the selected items, but nothing about the receiver's choices and his PII. The receiver is required to authenticate himself to the issuer to obtain a credential, and is not required to prove that he is an authorized receiver to the sender. Notably, there is no need of zero knowledge proof. The credentials in the first scheme are transferable, and all-or-nothing non-transferable in the second one.

Acknowledgment

The first author was supported by PhD scholarships of Smart Services Cooperative Research Centre (CRC) and University of Wollongong.

References

[1] J. Camenisch and B. Pfitzmann. Federated identity managemen. In Proceedings: Security, Privacy, and Trust in Modern Data Management (M. Petkovic and W. Jonker, eds.), vol. 2851 of Data-Centric Systems and Applications, (Secaucus, NJ, USA), pp. 213-238, Springer-Verlag, July 2007.

[2] J. Han, Y. Mu, W. Susilo, and J. Yan. A generic construction of dynamic single sign-on with strong security. In Proceedings: International ICST Conference on Security and Privacy in Communication Networks-SecureComm 2010 (S. Jajodia and J. Zhou, eds.), vol. 50 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, (Singapore), pp. 181-198, Springer-Verlag, September 7-9, 2010.

[3] A. B. Spantzely, J. Camenisch, T. Gross, and D. Sommer. User centricity: A taxonomy and open issues. In Proceeding: ACM Workshop on Digital Identity Managemen- DIM 2006 (A. Juels, M. Winslett, and A. Goto, eds.), (Alexandria, Virginia, USA), pp. 1-10, ACM, November 3, 2006.

[4] S. Suriadi, E. Foo, and A. Jsang. A user-centric federated single sign-on system. Journal of Network and Computer Applications, vol. 32, pp. 388-401, March 2009.

[5] V. Poursalidis and C. Nikolaou. A new user-centric identity management infrastructure for federated systems. In Proceedings: 3rd International Conference on Trust, Privacy and Security in Digital Business-TrustBus 2006 (S. F. Hbner, S. Furnell, and C. Lambrinoudakis, eds.), vol. 4083 of Lecture Notes in Computer Science, (Krakow, Poland), pp. 11-20, Springer-Verlag, September 4-8, 2006.

[6] J. Argyrakis, S. Gritzalis, and C. Kioulafas. Privacy enhancing technologies: A review. In Proceedings: Electronic Government- EGOV 2003 (R. Traunmller, ed.), vol. 2739 of Lecture Notes in Computer Science, (Prague, Czech Republi), pp. 282-287, Springer-Verlagn, September 1-5, 2003.

[7] Y.-C. Chang and M. Mitzenmacher. Privacy preserving keyword searches on remote encrypted data. In Proceedings: Applied Cryptography and Network Security-ACNS 2005 (J. Ioannidis, A. D. Keromytis, and M. Yung, eds.), vol. 3531 of Lecture Notes in Computer Science, (New York, USA), pp. 442-455, Springer-Verlag, June 7-10, 2005.

[8] J. Camenisch and A. Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In Proceedings: Advances in Cryptology- Eurocrypt 2001 (B. Pfitzmann, ed.), vol. 2045 of Lecture Notes in Compture Science, pp. 93-118, Springer-Verlag, May 6-10, 2001.

[9] J. Camenisch and E. V. Herreweghen. Design and implementation of the idemix anonymous credential system. In Proceedings: ACM Conference on Computer and Communications Security-CCS 2002 (V. Atluri, ed.), (Washingtion, DC, USA), pp. 21-30, ACM, November 18-22, 2002.

[10] J. Camenisch and T. Groβ. Efficient attributes for anonymous credentials. In Proceedings: the 15th ACM conference on Computer and communications security-CCS 2008 (P. Ning, P. F. Syverson, and S. Jha, eds.), (Alexandria, Virginia, USA), pp. 345-356, ACM, October 27-31, 2008.

[11] J. Camenisch and A. Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials. In Proceedings: Advances in Cryptology-CRYPTO 2002 (M. Yung, ed.), vol. 2442 of

Lecture Notes in Compture Science, (Santa Barbara, California, USA), pp. 61-76, Springer-Verlag, August 18-22, 2002.

[12] J. Camenisch and A. Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In Proceedings: Advances in Cryptology-CRYPTO 2004 (M. Franklin, ed.), vol. 3152 of Lecture Notes in Computer Science, (Santa Barbara, California, USA), pp. 56-72, Springer-Verlag, August 15-19, 2004.

[13] J. Camenisch and A. Lysyanskaya. A signature scheme with efficient protocols. In Proceedings: Security in Communication Networks-SCN 2002 (S. Cimato, C. Galdi, and G. Persiano, eds.), vol. 2576 of Lecture Notes in Computer Science, (Amalfi, Italy), pp. 268-289, Springer-Verlag, September 11-13, 2003.

[14] A. Lysyanskaya, R. L. Rivest, A. Sahai, and S. Wolf, Pseudonym systems. In Proceedings: Selected Areas in Cryptography-SAC 1999 (H. Heys and C. Adams, eds.), vol. 1758 of Lecture Notes in Computer Science, (Kingston,Ontario, Canada), pp. 184-199, Springer-Verlag, August 9-10, 1999.

[15] J. E. Holt, R. W. Bradshaw, K. E. Seamons, and H. Orman. Hidden credentials. In Proceedings: ACM Workshop on Privacy in the electronic society-WPES 2003 (S. Jajodia, P. Samarati, and P. F. Syverson, eds.), (Washington, DC, USA), pp. 1-8, ACM, October 30, 2003.

[16] I. Teranishi, J. Furukawa, and K. Sako. K-times anonymous authentication. In Proceedings: Advances in Cryptology- ASIACRYPT 2004 (P. J. Lee, ed.), vol. 3329 of Lecture Notes in Computer Science, (Jeju Island, Korea), pp. 308-322, Springer- Verlag, December 5-9, 2004.

[17] M. H. Au, W. Susilo, and Y. Mu. Constant-size dynamic k-TAA. In Proceedings: Security and Cryptography for Networks- SCN 2006 (R. D. Prisco and M. Yung, eds.), vol. 4116 of Lecture Notes in Computer Science, (Maiori, Italy), pp. 111-125, Springer-Verlag, September 6-8, 2006.

[18] I. Teranishi and K. Sako. K-times anonymous authentication with a constant proving cost. In Proceedings: Public Key Cryptography-PKC 2006 (M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, eds.), vol. 3958

of Lecture Notes in Computer Science, (New York, USA), pp. 525-542, Springer-Verlag, 24-26, April 2006.

[19] L. Nguyen. Efficient dynamic K-times anonymous authentication. In Proceedings: Progressin Cryptology-VIETCRYPT 2006 (P. Q. Nguyen, ed.), vol. 4341 of Lecture Notes in Computer Scienc, (Vietnam, Hanoi, Vietnam), pp. 81-98, Springer-Verlag, September 25-28, 2006.

[20] M. O. Rabin. How to exchange secrets by oblivious transfer. technical report tr-81, Aiken Computation Laboratory, Harvard University, 1981.

[21] G. Brassard, C. Créepeau, and J.-M. Robert. Information theoretic reductions among disclosure problems. In Proceedings: 28th Annual Symposium on Foundations of Computer Science- FOCS 1987, (Los Angeles, California), pp. 427-437, IEEE, October 12-14,1987.

[22] M. Naor and B. Pinkas. Oblivious transfer and polynomial evaluation. In Proceedings: 31th Annual ACM Symposium on the Theory of Computing-STOC 1999, (Atlanta, Georgia, USA), pp. 245-254, ACM, May 1-4, 1999.

[23] M. Naor and B. Pinkas. Oblivious transfer with adaptive queries. In Proceedings: Advances in Cryptology-CRYPTO 1999 (M. iener, ed.), vol. 1666 of Lecture Notes in Computer Science, (Santa Barbara, California), pp. 573-590, Springer-Verlag, August 15- 19, 1999.

[24] B. Aiello, Y. Ishai, and O. Reingold. Priced oblivious transfer: How to sell digital goods. In Proceedings: Advances in Cryptology-EUROCRYPT 2001 (B. Pfitzmann, ed.), vol. 2045 of Lecture Notes in Computer Scienc, (Innsbruck, Austria), pp. 119-135, Springer-Verlag, May 6-10, 2001.

[25] G. D. Crescenzo, R. Ostrovsky, and S. Rajagopalan. Conditional oblivious transfer and timed-release encryption. In Proceedings: Advances in Cryptology-EUROCRYPT 1999 (J. Stern, ed.), vol. 1592 of Lecture Notes in Computer Scienc, (Prague, Czech Republic,), pp. 74-89, Springer-Verlag, May 2-6, 1999.

[26] S. Coull, M. Green, and S. Hohenberger. Controlling access to an oblivious database using stateful anonymous credentials. In Proceedings: Public Key Cryptography-PKC 2009 (S. Jarecki and G. Tsudik, eds.), vol.

5443 of Lecture Notes in Computer Science, (Irvine, CA, USA), pp. 502-520, Springer-Verlag, March 18-20, 2009.

[27] J. Camenisch, M. Dubovitskaya, and G. Neven. Oblivious transfer with access control. In Proceedings: the 16th ACM conference on Computer and communications security-CCS 2009 (E. Al-Shaer, S. Jha, and A. D. Keromytis, eds.), (Chicago, Illinois, USA), pp. 131-140, ACM, November 9-13, 2009.

[28] J. Camenisch, M. Dubovitskaya, and G. Neven. Unlinkable priced oblivious transfer with rechargeable wallets. In Proceedings: Financial Cryptography and Data Security-FC 2010 (R. Sion, ed.), vol. 6052 of Lecture Notes in Computer Science, (Tenerife, Canary Islands), pp. 66-81, Springer-Verlag, January 25-28, 2010.

[29] J. Camenisch, G. Neven, and A. Shelat. Simulatable adaptive oblivious transfer. In Proceedings: Advances in Cryptology-EUROCRYPT 2007 (M. Naor, ed.), vol. 4515 of Lecture Notes in Computer Science, (Barcelona, Spain), pp. 573-590, Springer-Verlag, May 20-24, 2007.

[30] J. Camenisch, M. Dubovitskaya, G. Neven, and G. M. Zaveruch. Oblivious transfer with hidden access control policies. In Proceedings: Public Key Cryptography-PKC 2011 (D. Catalano et al. eds.), vol. 6571 of Lecture Notes in Computer Science, (Taormina, Italy), pp. 192-209, Springere-Verlag, March 6-9, 2011.

[31] N. Li, W. Du, and D. Boneh. Oblivious signature-based envelope. In Proceedings: 22th Annual Symposium on Principles of distributed computing-PODC 2003, (Boston, Massachusetts, USA), pp. 182-189, ACM, July 13-16, 2003.

[32] R. W. Bradshaw and J. E. H. K. E. Seamons. Concealing complex policies with hidden credentials. In Proceedings: ACM Conference on Computer and Communications Security-CCS 2004 (V. Atluri, B. Pfitzmann, and P. D. McDaniel, eds.), (Washingtion, DC, USA), pp. 146-157, ACM, October 25-29, 2004

[33] K. Frikken, M. Atallah, and J. Li. Attribute-based access control with hidden policies and hidden credentials. IEEE Transaction on Computers, vol. 55, pp. 1259-1270, October 2006.

[34] W. H. Winsborough, K. E. Seamons, and V. E. Jones. Automated trust negotiation. In Proceedings: DARPA Information Survivability Conference and Exposition-DISCEX 2000, (Hilton Head, South Carolina, USA), pp. 88-102, IEEE, Janunary 25-27, 2000.

[35] L. Zhou, W. Susilo, and Y. Mu. Three-round secret handshakes based on EIg gamal and DSA. In Proceedings: Information Security Practice and Experience-ISPEC 2006 (K. Chen, R. H. Deng, X. Lai, and J. Zhou, eds.), vol. 3903 of Lecture Notes in Computer Scienc, (Hangzhou, China), pp. 332-342, Springer-Verlag, April 11-14, 2006.

[36] M. Naor and B. Pinkas. Computationally secure oblivious transfer. Journal of Cryptology, vol. 18, no. 1, pp. 1-35, 2005.

[37] K. Kurosawa and R. Nojima. Simple adaptive oblivious transfer without random oracle. In Proceedings: Advances in Cryptology-ASIACRYPT 2009 (M. Matsui, ed.), vol. 5912 of Lecture Notes in Computer Scienc, (Tokyo, Japan), p. 334-346, Springer-Verlag, December 6-10, 2009.

[38] D. Boneh and X. Boyen. Short signatures without random oracles. In Proceedings: Advances in Cryptology-EUROCRYPT 2004 (C. Cachin and J. Camenisch, eds.), vol. 3027 of Lecture Notes in Computer Science, (Interlaken, Switzerland), pp. 56-73, Springer-Verlag, May 2-6, 2004.

[39] A. Boldyreva. Threshold signatures, multisignatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme. In Proceedings: Public Key Cryptography-PKC 2003 (Y. Desmedt, ed.), vol. 2567 of Lecture Notes in Computer Scienc, (Miami, FL, USA), pp. 31-46, Springer-Verlag, January 6-8, 2003.

[40] C.-K. Chu and W.-G. Tzeng. Efficient k-out-of-n oblivious transfer schemes with adaptive and non-adaptive queries. In Proceedings: Public Key Cryptography-PKC 2005 (S. Vaudenay, ed.), vol. 3386 of Lecture Notes in Computer Science, (Les Diablerets, Switzerland), pp. 172-183, Springer-Verlag, January 23-26, 2005.

[41] D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In Proceedings: Advances in Cryptology-CRYPTO 2004 (M. Franklin, ed.), vol. 3152 of Lecture Notes in Computer Science, (Santa Barbara, California, USA), pp. 41-55, Springer-Verlag, August 15-19, 2004.

Table 1: The computation cost in AC-OT$^n_{k\times 1}$-I scheme

Schem	Computation Cost								
	Setup			Issue		Commitment Phase		Transfer Phase	
	I	R	S	I	R	S	R	S	R
AC-OT$^n_{k\times 1}$-I	e	0	e	e	$e+2p$	$(2n+1)e$	0	ke	$2ke+kp$

Table 2: The communication cost in AC-OT$^n_{k\times 1}$-I scheme

Scheme	Communication Cost						
	Setup	Issue		Commitment Phase		Transfer Phase	
	I→S	I→R	I→S	S→R	R→S	S→R	R→S
AC-OT$^n_{k\times 1}$-I	E_q	E_1+E_q	0	nE_2+nE_τ	0	kE_τ	kE_τ

Table 3: The computation cost in our AC-OT$^n_{k\times 1}$-II scheme

Scheme	Computation Cost								
	Setup			Issue		Commitment Phase		Transfer Phase	
	I	R	S	I	R	S	R	S	R
AC-OT$^n_{k\times 1}$-II	e	e	e	$2e$	$2e+2p$	$(4n+1)e$	0	ke	$4ke+kp$

Table 4: The communication cost in our AC-OT$^n_{k\times 1}$-II scheme

Scheme	Communication Cost						
	Setup	Issue		Commitment Phase		Transfer Phase	
	I→S	I→R	I→S	S→R	R→S	S→R	R→S
AC-OT$^n_{k\times 1}$-I	E_q	E_1+2E_q	0	nE_2+3nE_τ	0	kE_τ	kE_τ