Faculty of Informatics - Papers (Archive)

Faculty of Engineering and Information Sciences

1-1-2012

New constructions of OSBE schemes and their applications in oblivious 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

Recommended Citation

Han, Jinguang; Susilo, Willy; Mu, Yi; and Yan, Jun: New constructions of OSBE schemes and their applications in oblivious access control 2012, 389-401.
https://ro.uow.edu.au/infopapers/2309

New constructions of OSBE schemes and their applications in oblivious access control

Abstract

Oblivious signature-based envelope (OSBE) schemes have demonstrated their potential applications in the protection of users privacy and rights. In an OSBE protocol, an encrypted message can only be decrypted by the receiver who holds a valid signature on a public message, while the sender (encrypter) does not know whether the receiver has the signature or not. Our major contributions in this work lie in the following aspects. We improve the notion of OSBE so that a valid credential holder cannot share his/her credential with other users (i. e., all-or-nothing non-transferability). We clarify the relationship between one-round OSBE and identity-based encryption (IBE) and show that one-round OSBE and semantically secure IBE against the adaptively chosen identity attack (IND-ID-CPA) are equivalent, if the signature in the OSBE scheme is existentially unforgeable against adaptively chosen message attacks. We propose an oblivious access control scheme to protect user privacy without the aid of any zero-knowledge proof. Finally, we also highlight some other novel applications of OSBE, such as attributed-based encryption. 2012 Springer-Verlag.

Keywords

access, oblivious, applications, control, their, osbe, schemes, constructions

Disciplines

Physical Sciences and Mathematics

Publication Details

Han, J., Susilo, W., Mu, Y. & Yan, J. (2012). New constructions of OSBE schemes and their applications in oblivious access control. International Journal of Information Security, 11 (6), 389-401.

Noname manuscript No.
(will be inserted by the editor)

New Constructions of OSBE Schemes and Their Applications in Oblivious Access Control

Jinguang Han · Willy Susilo · Yi Mu · Jun Yan

Received: date / Accepted: date

Abstract Oblivious signature-based envelope (OSBE) schemes have demonstrated their potential applications in the protection of users privacy and rights. In an OSBE protocol, an encrypted message can only be decrypted by the receiver who holds a valid signature on a public message; while the sender (encrypter) does not know whether the receiver has the signature or not. Our major contributions in this work lie in the following aspects. We improve the notion of OSBE so that a valid credential holder cannot share his/her credential with other users (i.e., *all-or-nothing non-transferability*). We clarify the relationship between one-round OSBE and identity-based encryption (IBE) and show that one-round OSBE and semantically secure IBE against the adaptively chosen identity attack (IND-ID-CPA) are equivalent, if the signature in the OSBE scheme is unforgeable against adaptively chosen message attacks. We propose an oblivious access control (OAC) scheme to protect user privacy without the aid of any zero-knowledge proof. Finally, we also highlight some other novel applications of OSBE, such as attributed-based encryption (ABE).

J. Han
Centre for Computer and Information Security Research, School of Computer Science and Software Engineering, University of Wollongong, NSW 2522, Australia.
College of Science, Hohai University, Nanjing 210098, China.
E-mail: jh843@uowmail.edu.au

W. Susilo and Y. Mu
Centre for Computer and Information Security Research, School of Computer Science and Software Engineering, University of Wollongong, NSW 2522, Australia.
E-mail: wsusilo@uow.edu.au; ymu@uow.edu.au

J. Yan
School of Information Systems and Technology, University of Wollongong, NSW 2522, Australia.
E-mail: jyan@uow.edu.au

Keywords Oblivious Signature-based Envelope · Oblivious Transfer · Access Control

1 Introduction

Internet services usually require users to provide their personally identifiable information (PII) for registration. Frequent registrations using PII could make the user traceable or even impersonated. Therefore, how to protect users' PII has become increasingly important. Aiming to protect users' privacy, some elegant solutions have been proposed, for example, privacy-enhancement scheme [1,2], privacy-preserving schemes [3,4], user - centric privacy management scheme [5], identity management scheme [6], *etc.*.

Introduced by Li, Du, and Boneh [7], oblivious signature - based envelope (OSBE) is a protocol, where a sender sends an envelope, which encapsulates a secret, to a receiver, so that only the receiver who has obtained a valid signature on an agreed-upon message from the certificate authority (CA) can open the envelope, and then obtain the secret. Further, the sender does not know whether the receiver has obtained the required signature. Hence, OSBE provides oblivious property for the receiver about the signature. OSBE is especially efficient in handing the cyclic policy interdependency problem in automated trust negotiation (ATN) [8]. For example, both Alice and Bob are agents of Central Intelligence Agency (CIA). They can only communicate with other CIA agents. Consider the problem of creating a secure session between Alice and Bob. Due to their special identities, none of them wants to release their identities first. Therefore, no session can be created. OSBE can deal with this scenario efficiently. If Alice wants to initiate a session with Bob, she can send an envelope, which encapsulates her identity, such as her public key certificate, to Bob. If Bob has possessed a credential (signature on the message which can indicate the membership of CIA) from CIA, he can use it to open the envelope, and obtain Alice's identity. Otherwise, nothing about Alice's identity is released to Bob.

Li, Du, and Boneh [7] proposed three OSBE schemes based on RSA [9], BLS [10] and Rabin [11] signatures, respectively. The first one requires a two-round communication, while the rest are obtained from identity-based encryption (IBE) [12,13] and require one-round. They pointed out that OSBE can be used in some schemes, such as ATN [8], two-party secure function evaluation (SFE) and complicated policy requirements [14]. They also left an open problem that how to design an efficient and provably secure OSBE scheme from a DSA signature. They envisioned that OSBE can be used to construct oblivious access control (OAC) systems. The idea of OSBE has been also used to constructed secret handshake [15], oblivious certificates and oblivious credentials [16,17].

Nasserian and Tsudik [18] revisited OSBE and solved the problem raised in [7]. They proposed several OSBE schemes from ElGamal signature family, such as Schnorr signature, Nyberg-Ruppel signature, DSA signature, *et al.*. They also pointed out that OSBE can be used in Blogs and peer-to-peer (P2P) networks.

Proposed by Holt, Bradshaw, Seamons and Orman [19], hidden credentials are important primitives to protect services, access control policy and extremely sensitive private information. In a hidden credential scheme, a sender encrypts a secret and sends it to a receiver. The receiver must possess the required credential(s) in order to decrypt it. Hidden credentials have been used to conceal complex policies [20], and hide attributes in access control [4]. In these schemes, a receiver can access the resources if and only if his attributes satisfy the policy specified by the sender, while the sender knows nothing about the user's credentials. Moreover, he does not know whether the receiver has a credential.

Coull, Green and Hohenberger[21] proposed a protocol for anonymous access to an oblivious database using stateful anonymous credentials. Here, a stateful graph was used. With each access, the user's state was transformed from one to another. For each state, the user must possess a corresponding credential from the credential provider. If all states were used, the user could not access the database again. Camenisch, Dubovitskaya and Neven [22] proposed another protocol for anonymous access to a database, which avoided reissuing credentials, and was more efficient than that of [21]. In both schemes mentioned above, two building blocks were used, namely anonymous credential and oblivious transfer (OT). A user must obtain the required credentials from the issuer prior to access the database, and then prove them to the database server in zero knowledge. The database server and the user execute an OT protocol to deliver the services selected by the user. As a result, the following features are captured: (1) Only the authorized users can access the database; (2) The database server knows nothing about the user's attributes; and (3) The database server does not know which services the user can access.

Our Contribution

In this paper, we propose two OSBE schemes from the signatures which are existentially unforgeable in the standard model. We clarify the relationship between one-round OSBE and IBE, namely one-round OSBE and semantically secure IBE against the adaptively chosen identity attack (IND-ID-CPA) are equivalent, if the signature in the OSBE scheme is existentially unforgeable against the adaptively chosen message attacks. We improve the notion of OSBE. In our OSBE scheme, the credentials are *non-transferable.* While, in previous OSBE schemes [7,18], the credentials are transferable. Based on our second OSBE scheme and the OT protocol proposed by Chu and Tzeng [23], we propose an oblivious access control (OAC) scheme, which was initially introduced in [7]. Our OAC scheme captures the following properties: (1) The authorized user can obliviously obtain services without releasing his credentials and the content of the selected services to the service provider. Furthermore, the service provider does not know whether the user has possessed the required credentials or not. (2) Zero-knowledge proof is *not* required. So, our OAC scheme is more efficient in communication. (3) The credentials of the user are *all-or-nothing non-transferable.* Our OAC scheme can prevent illegal credentials sharing. (4) Our OAC scheme can resist the eavesdropping attacks [7], and provide forward security. Therefore, even if the credentials are compromised, nothing about the services which the user selected before can be revealed. We also point out the potential applications of OSBE in attribute-based encryption (ABE).

Paper Organization

This paper is organized as follows. In Section 2, the preliminaries required throughout this paper are introduced. We clarify the relationship between one-round OSBE and IBE, and propose an one-round OSBE scheme in Section 3. Then, a two-round OSBE scheme is proposed in Section 4. In Section 5, an OAC scheme is proposed. The applications of OSBE in ABE is described in Section 6. Section 7 concludes this paper.

2 Preliminaries

In this section, we introduce the preliminaries used throughout this paper.

In the rest of this paper, by $\alpha \overset{R}{\leftarrow} A$, we denote that α is chosen from A at random. Especially, by $\alpha \overset{R}{\leftarrow} A$, we denote that α is chosen from A identically if A is a finite set. By $\mathcal{KG}(1^\ell) \rightarrow (sk, pk)$, we denote a secret-public pair generation algorithm which takes as input a security parameter 1^ℓ, and outputs a secret-public key pair (sk, pk). By $A(x) \rightarrow y$, we denote that y is computed by running the algorithm A with input x.

2.1 Formal Definition and Security Model of OSBE

The formal definition and security model of OSBE proposed by Li, Du and Boneh [7] are as follows.

In an OSBE scheme, there are three entities: a sender S, and two receivers R_1 and R_2. An OSBE scheme comprises three algorithms: Setup , Interaction and Open.

Setup. Taking as input a security parameter 1^ℓ, this algorithm generates the public parameters $params$, a signature algorithm (sign, verify) and a secret-public key pair $\mathcal{KG}(1^\ell) \rightarrow (sk, pk)$ for the signature algorithm. It outputs two messages M and P. It sends $(params, pk, M, P)$ to S, $(params, pk, M, \sigma)$ to R_1 and $(params, pk, M)$ to R_2, respectively, where $\sigma = \mathsf{Sign}(sk, M)$ denotes the signature on the message M.

Interaction. For $b \in \{1, 2\}$, R_b is chosen to interact with S. S encrypts the message P as $C = \mathcal{E}(params, pk, M, P)$ where partial signature parameters are used, and sends C to R_b.

Open. If $b = 1$, R_1 can use the signature σ to decrypt C, and output P. While, if $b = 2$, nothing about P can be released.

An OSBE must satisfy the following three properties: sound, oblivious and semantically secure against the receiver. The security model of OSBE are defined using the following games.

Game 1. Soundness: If a user has possessed the required signature, he can obtain the message encrypted in the ciphertext.

Setup. The challenger runs Setup algorithm to setup the system. It sends (PP, pk, M, σ) to R_1.

Interaction. The challenger and R_1 execute Interaction algorithm.

Open. R_1 outputs the message P.

Definition 1 An OSBE scheme is sound if the probability that R_1 cannot output the message P in the above game is ϵ.

Game 2. Oblivious: By an interaction, the sender cannot distinguish a receiver who has obtained a signature from the receiver who has not obtained a signature.

Setup. The challenger runs Setup algorithm to setup the system. It flips an unbiased coin with $\{1, 2\}$, and gets $b \in \{1, 2\}$.

Interaction. The challenger acts as R_b to execute Interaction with the adversary $\mathcal{A}$.

Guess. $\mathcal{A}$ outputs his guess b' on b. We say that $\mathcal{A}$ wins the game, if $b = b'$.

Definition 2 An OSBE scheme is oblivious if no probabilistic polynomial-time adversary can win the above game with the advantage $|\Pr[b' = b] - \frac{1}{2}| \geq \epsilon$.

Game 3. Semantically Secure against the Receiver: If a receiver has not obtained the required signature, he cannot gather anything about the message encrypted in the ciphertext.

Setup. The challenger runs Setup algorithm to setup the system. It sends $(params, pk, M)$ to $\mathcal{A}$, and gets back two messages P_0 and P_1 with equal length. The challenger flips an unbiased coin with $\{0, 1\}$, and obtains $b \in \{0, 1\}$.

Interaction. The challenger interacts with $\mathcal{A}$, and sends $C = \mathcal{E}(params, pk, M, P_b)$ to $\mathcal{A}$.

Guess. $\mathcal{A}$ outputs his guess b' on b. We say that $\mathcal{A}$ wins the game, if $b = b'$.

Definition 3 An OSBE scheme is semantically secure against the receiver if no probabilistic polynomial-time adversary can win the above game with the advantage $|\Pr[b' = b] - \frac{1}{2}| \geq \epsilon$.

2.2 Formal Definition and Security Model of Oblivious Access Control

An oblivious access control (OAC) scheme consists of four algorithms: Setup, Commitment, Issuing Credential and Access Service Items.

Setup. Taking as input a security parameter 1^ℓ, this algorithm outputs the public parameters $params$, and secret-public key pairs $\mathcal{KG}(1^\ell) \rightarrow (msk, mpk)$, $\mathcal{KG}(1^\ell) \rightarrow (ssk, spk)$ and $\mathcal{KG}(1^\ell) \rightarrow (rsk, rpk)$ for the credential issuer, a service provider and a receiver, respectively.

Commitment. Taking as input the security parameter 1^{ℓ}, a service item S_i and a service provider's secret key ssk, this algorithm outputs a commitment $\mathsf{Commit}(params, S_i, ssk)$ for $i = 1, 2, \cdots, n$.

Issuing Credential. Taking as input the parameters $params$, a service provider's public key spk and the receiver's public key rpk, this algorithm outputs a credential σ which can be used by the receiver to access the service items managed by the service provider with public key spk.

Access Service Items. This is an interactive algorithm executed between a receiver and a service provider. The receiver takes as input the parameters $params$, his credential σ, his secret key rsk and an identifier η_i, and outputs the service S_{η_i}. The service provider takes as input the parameters $params$ and his secret key ssk, and outputs nothing.

Correctness. We say that an oblivious access control scheme is correct if a receiver has obtained a credential on a service provider from the credential issuer, he can access the service items managed by the service provider.

Security model
We define the security of an OAC scheme by the following properties. This model is similar to that in [23].

Receiver Privacy.

1. The receiver does not reveals anything about his credential to the service provider.
2. For two choices $\mathcal{C} = \{\eta_1, \eta_2, \cdots, \eta_t\}$ and $\mathcal{C}' = \{\eta'_1, \eta'_2, \cdots, \eta'_t\}$, the transcripts received by the service provider for $\mathcal{S} = \{S_{\eta_1}, S_{\eta_2}, \cdots, S_{\eta_t}\}$ and $\mathcal{S}' = \{S_{\eta'_1}, S_{\eta'_2}, \cdots, S_{\eta'_t}\}$ are indistinguishable.

Service Provider Privacy. This property is defined by the comparison between a real world and an ideal world paradigms. In the real world, the receiver and the service provider execute the protocol. Meanwhile, in the ideal world, the functionality of the protocol is replaced by a trusted third party (TTP). The service provider sends all his messages $\{S_1, S_2, \cdots, S_n\}$ to the TTP. The receiver adaptively sends his choices $\{\eta_1, \eta_2, \cdots, \eta_t\}$ to the TTP. If $\{\eta_1, \eta_2, \cdots, \eta_t\} \subseteq \{1, 2, \cdots, n\}$, the TTP sends $\{S_{\eta_1}, S_{\eta_2}, \cdots, S_{\eta_t}\}$ to the receiver. An oblivious transfer with access control can protect the security of the service provider, if for any receiver in the real world, there exists an probabilistic polynomial-time (PPT) receiver in the ideal world such that the outputs of these two receivers are indistinguishable

We say that an OAC scheme is secure if it can satisfy the two properties mentioned above.

2.3 Complexity Assumptions

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups with prime order p. Let g_1 and g_2 be the generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. Let $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_\tau$ be a map with the following properties:

1. Bilinearity. $e(u^a, v^b) = e(u, v)^{ab}$, for all $u \in \mathbb{G}_1$, $v \in \mathbb{G}_2$ and $a, b \in \mathbb{Z}_p$.
2. Non-degeneracy. There exists $u \in \mathbb{G}_1$ and $v \in \mathbb{G}_2$ such that $e(u, v) \neq 1$, where 1 is the identity of $\mathbb{G}_\tau$.
3. Computability. There exists an efficient algorithm to compute $e(u, v)$ for all $u \in \mathbb{G}_1$ and $v \in \mathbb{G}_2$.

Definition 4 (Computational Diffie-Hellman (CDH) Assumption [24].) Given a group $\mathbb{G}$ with prime order p and a generator $g \in \mathbb{G}$, we say that the CDH assumption holds in $\mathbb{G}$ if for all probabilistic polynomial-time algorithms $\mathcal{A}$

$$Pr[\mathcal{A}(p, g, g^a, g^b) \rightarrow g^{ab}] \leq \epsilon$$

where the probability is over the random choice of $a, b \in \mathbb{Z}_p$ and the random bits consumed by $\mathcal{A}$.

Definition 5 (q-Strong Diffie-Hellman (q-SDH) Assumption [25].) Let g_1 and g_2 be the generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. Given a $(q+2)$-tuple $(g_1, g_2, g_2^x, g_2^{x^2}, \cdots, g_2^{x^q})$, we say that q-SDH assumption holds in bilinear groups $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_\tau)$ with prime order p if for all probabilistic polynomial-time algorithms $\mathcal{A}$

$$Pr[\mathcal{A}(g_1, g_2, g_2^x, g_2^{x^2}, \cdots, g_2^{x^q}) \rightarrow (c, g_1^{\frac{1}{x+c}})] \leq \epsilon$$

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

Definition 6 (Chosen-Target Computational Diffie- Hellman (CT-CDH) Assumption [26].) Given a group $\mathbb{G}$ with prime order p and a generator $g \in \mathbb{G}$, let $x \overset{R}{\leftarrow} \mathbb{Z}_p^*$, $H : \{0,1\}^* \rightarrow \mathbb{G}$ be a hash function, and $T_G(\cdot)$ and $H_G(\cdot)$ be two oracles. $T_G(\cdot)$ is a target oracle, which takes as input $i \in \mathbb{Z}_p$ and returns $w_i \in \mathbb{G}$. $H_G(\cdot)$ is a help oracle, which takes as input $w_i \in \mathbb{G}$ and returns $w_i^x \in \mathbb{G}$. Let q_T and q_H be the numbers of times which the two oracles are queried, respectively. We say that the CT-CDH assumption holds in $\mathbb{G}$ if for all probabilistic polynomial-time algorithms $\mathcal{A}$

$$Pr[\mathcal{A}^{T_G(\cdot), H_G(\cdot)}(p, g, g^x, H) \rightarrow \{(v_1, j_1), \cdots, (v_k, j_k)\}] \leq \epsilon$$

where $v_i = w_{j_i}^x$, for $i = 1, 2, \cdots, k$, $q_H < k \leq q_T$.

3 One-round OSBE

In this section, we clarify the relationship between one-round OSBE and IBE, and propose an one-round OSBE scheme from BB signature [27].

3.1 One-round OSBE and IBE

By one-round OSBE, we mean that the sender can send the ciphertext directly to the recipient without having to interact with him.

Before clarifying the relationship between one-round OSBE and IBE, we review the definition of IBE. Proposed by Shamir [28], an IBE scheme is a public encryption scheme where the public key can be arbitrary string. The first satisfying scheme of IBE was proposed by Boneh and Franklin [29]. An IBE scheme consists of the following four algorithms:

Setup. Taking as input a security parameter 1^{ℓ}, this algorithm returns the system parameters *pramas* and a master secret key *msk*.

KeyGen. Taking as input the public parameters *params*, an identity ID and the master key *msk*, this algorithm generates a secret key K_{ID} for ID.

Enc. Taking as input the system parameters *params*, an identity ID and a message m, this algorithm returns a ciphertext $CT = \mathsf{Enc}(params, ID, m)$.

Dec. Taking as input the system parameters *params*, the corresponding secret key K_{ID} and the ciphertext CT, this algorithm returns the message $m = \mathsf{Dec}(mpk, K_{ID}, C)$.

IBE has been researched extensively. Schemes satisfying different security requirements have been proposed [30,31,32,33,34]. In [30], Chow classified IBE schemes into six types, namely reduction improvement, multi-recipient and hierarchical IBE (HIBE), exponent-inversion IBE, standard model (commutative-blinding), standard model (with user anonymity) and generations of IBE. Due to the fact that an OSBE is a semantically secure public key encryption, we only concentrate on the IBE schemes which are also semantically secure. There are two kinds of attacks on semantically secure IBE schemes. The first one is restricted chosen (selective) identity attacks [31]. The second one is adaptively chosen (full) identity attacks [32,33,34]. In the latter attack, an adversary can query the KeyGen oracle with adaptively selected identities, whilst this is not permitted in the former. We use the following game between a challenger and an adversary $\mathcal{A}$ to define the semantic security of IBE against the adaptively chosen identity attacks (IND-ID-CPA).

Setup. The challenger runs Setup algorithm to setup the system. It sends *params* to $\mathcal{A}$, and keeps *msk* secrete.

Query phase 1. $\mathcal{A}$ can adaptively query secrete keys for identity $ID_1, ID_2, \cdots, ID_j$. The challenger responds with $K_{ID_1}, K_{ID_2}, \cdots, K_{ID_j}$ by running KeyGen algorithm.

Challenge. $\mathcal{A}$ sends an identity ID^* and two messages m_0 and m_1 to the challenger, where the only constraint is that $\mathcal{A}$ has not queried a secret key for ID^*. The challenger flips an unbiased coin with $\{0,1\}$, and gets $b \in \{0,1\}$. The challenger computes the challenged ciphertext as $CT^* = \mathsf{Enc}(mpk, ID^*, m_b)$ and sends CT^* to $\mathcal{A}$.

Query phase 2. $\mathcal{A}$ can adaptively query secret keys for identities $ID_{j+1}, ID_{j+2}, \cdots, ID_{q_{ID}}$, where the only restriction is that $\mathcal{A}$ can not query a secret key for ID^*. The challenger returns as in Query phase 1.

Guess. $\mathcal{A}$ outputs his guess b' on b. We say that $\mathcal{A}$ wins the game, if $b = b'$.

Definition 7 An IBE scheme is (t, q_{ID}, ϵ) semantically secure under adaptively chosen identity attack (IND-ID-CPA), if no probabilistic polynomial-time adversary $\mathcal{A}$ who adaptively makes at most q_{ID} secret key queries can win the above game with the advantage $|\Pr[b' = b] - \frac{1}{2}| \geq \epsilon$.

We use the following three theorems to clarify the relationship between one-round OSBE and IBE.

Theorem 1 *A one-round OSBE implies a (t, q_{ID}, ϵ) IND-ID-CPA secure IBE if the signature in the one-round OSBE scheme is (t, q_{ID}, ϵ) existentially unforgeable against adaptively chosen message attacks.*

Proof As mentioned in the beginning of this section, one-round OSBE is a semantically secure IBE scheme, where the master key is the signing key. The secret key for ID is the signature on m, where $m = ID$. The public key is the message and public parameters. If there exists an adversary $\mathcal{A}$ can break the IND-ID-CPA secure IBE from the one-round OSBE with advantage at least ϵ, we will show that there exists an algorithm $\mathcal{B}$ who can use $\mathcal{A}$ to forge a signature. Due to the encryption in OSBE is semantically secure, what we need to prove is that if the adversary $\mathcal{A}$ can compute a secret key for an unqueried identity, he can forge a signature for a message.

Setup. The challenger runs Setup algorithm in the OSBE scheme to setup the system. It sends $(params, pk)$ to $\mathcal{A}$.

Query phase 1. $\mathcal{A}$ can adaptively query secret keys for identities $ID_1, ID_2, \cdots, ID_j$. The challenger responds with $K_{ID_1}, K_{ID_2}, \cdots, K_{ID_j}$, where $K_{ID_i} = \mathsf{Sign}(sk, ID_i)$, for $i = 1, 2, \cdots, j$.

Challenge. $\mathcal{A}$ submits an identity ID^* and two messages m_0 and m_1 with equal length to the challenger. The challenger sends $C^* = \mathsf{Enc}(params, ID^*, m_b)$ to $\mathcal{A}$, where $b \in \{0,1\}$.

Query phase 2. $\mathcal{A}$ can adaptively query secret keys for identities $ID_{j+1}, ID_{j+2}, \cdots, ID_{q_{ID}}$. The challenger responds as in Query phase 1.

Guess. $\mathcal{A}$ output his guess b' on b.

We only consider the semantic security, namely the security of the secret key. Therefore, if $|\Pr[b' = b] - \frac{1}{2}| \geq \epsilon$, $\mathcal{A}$ can compute a secret key for ID^* with the same advantage ϵ. So, $\mathcal{B}$ aborts. $\mathcal{B}$ can use $\mathcal{A}$ to forge a signature on a message m with the advantage at least ϵ, where $m = ID^*$. □

Theorem 2 *An (t, q_{ID}, ϵ) IND-ID-CPA secure IBE implies an one-round OSBE, where the signature in the one-round OSBE scheme is (t, q_{ID}, ϵ) existentially unforgeable against adaptively chosen message attacks.*

Proof Naor (see Section 5 in [29]) pointed out that any IBE scheme can be converted to a signature scheme, where the signing key is the master key in the IBE scheme. The public key is the public parameters and identities in the IBE scheme. The signature on a message m is the secret key for ID, where $m = ID$. To verify the signature on m, we can choose m', encrypt it using the patrial signature on m, and try to decrypt the ciphertext using the signature. The difference between this signature and the traditional one is that the verification algorithm in the former is random, instead of a deterministic algorithm. So, IBE is a one-round OSBE. Since the IBE scheme is semantically secure, we will only consider the security of the secret key. If there exists an adversary $\mathcal{A}$ who can forge a signature for a unqueried message (identity), we will show that there exists an algorithm $\mathcal{B}$ that can use $\mathcal{A}$ to break the security of the IND-ID-CPA IBE. The proof can be deduced very similarly to the above theorem. Therefore, we omit it. □

Based on the above two theorems, we can conclude the following theorem.

Theorem 3 *One-round OSBE and (t, q_{ID}, ϵ) IND-ID-CPA secure IBE are equivalent, if the signature in the OSBE scheme is (t, q_{ID}, ϵ) existentially unforgeable against the adaptively chosen message attack.*

Boneh and Franklin [29] claimed that a secure IBE scheme requires both a public-key encryption scheme and a digital signature scheme.

3.2 BB Signature Scheme

BB signature scheme was proposed by Boneh and Boyen [27]. This scheme is described as follows:

Setup. Taking as input a security parameter 1^ℓ, this algorithm returns bilinear groups $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_\tau)$ with prime order p. Let g and h be the generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively.

KeyGen. Taking as input $x \overset{R}{\leftarrow} \mathbb{Z}_p^*$, this algorithm returns $y = h^x \in \mathbb{G}_2$. The secret ky is x and the public key is (g, h, y).

Sign. Taking as input a message $m \in \mathbb{Z}_p$ and the secret key x, this algorithm returns a signature $\sigma = g^{\frac{1}{x+m}}$.

Verify. Taking as inputs the message-signature pair (m, σ), this algorithm returns True if and only if $e(\sigma, yh^m) = e(g, h)$. Otherwise, it returns Reject.

Theorem 4 *The* BB *signature Scheme is (t, q_S, ϵ) existentially unforgeable against the weakly chosen message attacks under the q-SDH assumption [27]*[1].

3.3 BB-OSBE

Based on the BB signature scheme, we propose an OSBE scheme as follows.

Setup. Taking as input a security parameter 1^ℓ, this algorithm returns the public parameters $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_\tau, g, h)$ and a secret-public key pair $\mathcal{KG}(1^\ell) \to (x, y)$ for the BB signature scheme, where g is a generator of $\mathbb{G}_1$, h is a generator of $\mathbb{G}_2$ and $y = h^x$. Additionally, it generates a hash function $H(\cdot)$ which extracts a key for the semantically secure symmetric encryption algorithm $\mathcal{E}(\cdot)$. It chooses two messages $m \in \mathbb{Z}_p$ and $P \in \{0,1\}^\ell$, and computes a signature $\sigma = g^{\frac{1}{x+m}}$. It sends (m, P, g, h, y) to S, (m, σ, g, h, y) to R_1 and (m, g, h, y) to R_2, respectively.

[1] By weakly chosen message attack, the authors mean that the adversary must submit all his queries before obtaining the public key.

Interaction. S chooses $t \overset{R}{\leftarrow} \mathbb{Z}_p \backslash \{0,1\}$, and computes $T_1 = (yh^m)^t$, $T_2 = e(g,h)^t$ and $C = \mathcal{E}_{H(T_2)}(P)$. S sends the cipthertext (T_1, C) to R_1 and R_2.

Open. Receiving (T_1, C) from S, R_1 computes $T_2 = e(\sigma, T_1)$ and $H(T_2)$, decrypts C, and obtains P.

Theorem 5 BB-OSBE *is sound.*

Proof

$$\begin{aligned} e(\sigma, T_1) &= e(g^{\frac{1}{x+m}}, (yh^m)^t) \\ &= e(g^{\frac{1}{x+m}}, h^{x+m})^t \\ &= e(g,h)^t = T_2 \end{aligned}$$

□

Theorem 6 BB-OSBE *is oblivious.*

Proof In our BB-OSBE scheme, S receives nothing from R_1 and R_2, so he cannot distinguish R_1 from R_2. Therefore, BB-OSBE is oblivious. □

Theorem 7 BB-OSBE *is semantically secure against the receiver, if no probabilistic polynomial-time adversary can forge a* BB *signature .*

Proof BB-OSBE uses a semantically secure symmetric encryption algorithm $\mathcal{E}(\cdot)$, where $H(\cdot)$ is modeled as a random oracle. BB-OSBE is semantically secure against the receiver if there exists no probabilistic polynomial-time adversary $\mathcal{A}$ who can compute the secret key which the sender uses to extract the encryption key with non-negligible probability. Namely, BB-OSBE is semantically secure against the receiver if no probabilistic polynomial -time adversary $\mathcal{A}$ can win the following game against the challenger $\mathcal{X}$ with non-negligible probability:

1. $\mathcal{A} \xleftarrow{m,g,h,y} \mathcal{X}$. $\mathcal{X}$ sends the public parameters (m,g,h,y) to $\mathcal{A}$.
2. $\mathcal{A} \xrightarrow{P_0,P_1} \mathcal{X}$. $\mathcal{A}$ sends two messages P_0 and P_1 with equal length to $\mathcal{X}$.
3. $\mathcal{A} \xleftarrow{T_1,C} \mathcal{X}$. $\mathcal{X}$ flips an unbiased coin with $\{0,1\}$ and obtains $b \in \{0,1\}$. $\mathcal{X}$ chooses $t \overset{R}{\leftarrow} \mathbb{Z}_p \backslash \{0,1\}$, and computes $T_1 = (yh^m)^t$, $T_2 = e(g,h)^t$ and $C = \mathcal{E}_{H_2(T_2)}(P_b)$. It sends T_1 and C to $\mathcal{A}$.
4. $\mathcal{A} \xrightarrow{b'} \mathcal{X}$. $\mathcal{A}$ outputs his guess b' on b. $\mathcal{A}$ wins the game, if $b' = b$.

If there exists an adversary $\mathcal{A}$ who can break the semantic security of BB-OSBE against the receiver with advantage at least ϵ, we will show that there exists an algorithm $\mathcal{B}$ who can use $\mathcal{A}$ to forge a BB signature with the same advantage.

Given (m,g,h,y), the aim of $\mathcal{B}$ is to compute a signature σ^* such that $e(\sigma^*, yh^m) = e(g,h)$.

1. $\mathcal{B}$ sends (m,g,h,y) to $\mathcal{A}$.
2. $\mathcal{A}$ submits two messages P_0 and P_1 with the equal length.
3. $\mathcal{B}$ flips an unbiased coin with $\{0,1\}$ and obtains $b \in \{0,1\}$. $\mathcal{B}$ chooses $t \overset{R}{\leftarrow} \mathbb{Z}_p \backslash \{0,1\}$, and computes $T_1 = (yh^m)^t$, $T_2 = e(g,h)^t$ and $C = \mathcal{E}_{H_2(T_2)}(P_b)$. It sends T_1 and C to $\mathcal{A}$.
4. If $\mathcal{A}$ can output his guess with the advantage $|\Pr[b' = b] - \frac{1}{2}| \geq \epsilon$, he can computes a σ^* such that $e(\sigma^*, T_1) = e(g,h)^t$ with the same advantage.
5. $\mathcal{B}$ abort. $\mathcal{B}$ can uses $\mathcal{A}$ to forge a BB message-signature pair (m, σ^*) with the advantage at least ϵ, where $e(\sigma^*, yh^m) = e(g^{\frac{1}{x+m}}, h^{x+m}) = e(g,h)$.

□

4 Modified BBS (MBBS)-OSBE

Modified BBS (MBBS) signature scheme was proposed by Boneh, Boyen and Shacham [35], and was modified and proven by Au, Susilo and Mu [36]. In this section, we review the MBBS signature scheme, and propose an OSBE scheme from it. In our MBBS-OSBE scheme, a user's credentials are *all-or-nothing non-transferable.* By all-or-nothing non-transferability, we mean that all credentials of the user are shared, once he shares one of them with others [37].

4.1 Modified BBS (MBBS) Signature

The MBBS signature is described as follows.

Setup. Taking as input a security parameter 1^ℓ, this algorithm returns bilinear groups $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_\tau)$ with prime order p. Let $g_0, g_1, g_2, \cdots, g_{l+1}$ be the generators of $\mathbb{G}_1$, and h be the generator of $\mathbb{G}_2$.

KeyGen. Taking as input $x \overset{R}{\leftarrow} \mathbb{Z}_p^*$, this algorithm returns $y = h^x \in \mathbb{G}_2$. The secret ky is x and the public key is $(g_0, g_1, g_2, \cdots, g_{l+1}, h, y)$.

Sign. Taking as input messages $(m_1, m_2, \cdots, m_l) \in \mathbb{Z}_p^l$, $r \overset{R}{\leftarrow} \mathbb{Z}_p (r \neq -x \bmod p)$ and $s \overset{R}{\leftarrow} \mathbb{Z}_p^*$, this algorithm returns a signature (σ, r, s) on $(m_1, m_2, \cdots, m_l)$, where $\sigma = (g_0 g_1^s g_2^{m_1} g_3^{m_2} \cdots g_{l+1}^{m_l})^{\frac{1}{x+r}}$.

Verify. Taking as input (σ, r, s) and $(m_1, m_2, \cdots, m_l)$, this algorithm returns True if and only if $e(\sigma, yh^r) = e(g_0 g_1^s g_2^{m_1} g_3^{m_2} \cdots g_{l+1}^{m_l}, h)$. Otherwise, it returns Reject.

Theorem 8 *The* MBBS *signature Scheme is* (t, q_S, ϵ) *existentially unforgeable against the adaptively chosen message attacks under the q-SDH assumption [36].*

4.2 MBBS-OSBE

Based on the MBBS signature scheme, we propose an OSBE scheme as follows.

Setup. Taking as input a security parameter 1^ℓ, this algorithm returns the public parameters $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_\tau, g, g_0, g_1, g_2, \cdots, g_l, h)$ and a secret-public key pair $\mathcal{KG}(1^\ell) \rightarrow (x, y)$ for the MBBS signature scheme, where $g, g_0, g_1, \cdots, g_l$ are the generators of $\mathbb{G}_1$, h is the generator of $\mathbb{G}_2$ and $y = h^x$. Additionally, it generates a hash function $H(\cdot)$ which extracts a key for a semantically secure symmetric encryption algorithm $\mathcal{E}(\cdot)$, and two security parameters ℓ_1 and ℓ_2 which are linear in ℓ.

The receiver generates his secret-public key pair $\mathcal{KG}(1^\ell) \rightarrow (x_u,\, y_u)$, where $x_u \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and $y_u = g^{x_u}$.

This algorithm chooses messages $m_1, m_2, \cdots, m_{l-1}, r, s \overset{R}{\leftarrow} \mathbb{Z}_p^{l+1}$ and $P \in \{0,1\}^\ell$, and computes the signature $\sigma = (g_0 g_1^s g_2^{m_1} g_3^{m_2} \cdots g_l^{m_{l-1}} y_u)^{\frac{1}{x+r}}$. It sends $(m_1, m_2, \cdots, m_{l-1}, P, g, g_0, g_1, g_2, \cdots, g_l, h, y)$ to S, $(m_1, m_2, \cdots, m_{l-1}, g, g_0, g_1, g_2, \cdots, g_l, h, y, \sigma, r, s)$ to R_1, and $(m_1, m_2, \cdots, m_{l-1}, g, g_0, g_1, g_2, \cdots, g_l, h, y)$ to R_2, respectively.

Interaction.

1. (a) $R_1 \xrightarrow{(r,s)}$ S.
   (b) $R_2 \xrightarrow{(r',s')}$ S. Where $r', s' \overset{R}{\leftarrow} \mathbb{Z}_p$.
2. S chooses $t \overset{R}{\leftarrow} \mathbb{Z}_p$, and computes

$$T_0 = e(g,h)^t,\ T_1 = (yh^r)^t,\ T_1' = (yh^{r'})^t,$$

$$T_2 = e(g_0 g^s g_2^{m_1} \cdots g_l^{m_{l-1}}, h)^t,$$

$$T_2' = e(g_0 g^{s'} g_2^{m} \cdots g_l^{m_{l-1}}, h)^t$$

$$C = \mathcal{E}_{H(T_2)}(P),$$

and

$$C' = \mathcal{E}_{H(T_2')}(P).$$

   (a) $R_1 \xleftarrow{(T_0, T_1, C)}$ S.
   (b) $R_2 \xleftarrow{(T_0, T_1', C')}$ S.

Open. Receiving (T_0, T_1, C) from S, R_1 computes $T_2 = \frac{e(\sigma, T_1)}{T_0^{x_u}}$ and $H(T_2)$, decrypts C, and obtains P.

Theorem 9 MBBS-OSBE *is sound.*

Proof

$$\begin{aligned}\frac{e(\sigma, T_1)}{T_0^{x_u}} &= \frac{e((g_0 g_1^s g_2^{m_1} \cdots g_l^{m_{l-1}} y_u)^{\frac{1}{x+r}}, (yh^r)^t)}{e(g,h)^{t x_u}} \\ &= \frac{e(g_0 g_1^s g_2^{m_1} \cdots g_l^{m_{l-1}} y_u, h)^t}{e(y_u, h)^t} \\ &= \frac{e(g_0 g_1^s g_2^{m_1} \cdots g_l^{m_{l-1}}, h)^t e(y_u, h)^t}{e(y_u, h)^t} \\ &= e(g_0 g_1^s g_2^{m_1} \cdots g_l^{m_{l-1}}, h)^t \\ &= T_2\end{aligned}$$

□

Before proving that MBBS- OSBE is oblivious, we introduce the definition of statistic indistinguishability proposed in [7]. Two distribution families $\mathcal{D}^1(\ell)$ and $\mathcal{D}^2(\ell)$ are statistically indistinguishable, if

$$\sum_y |Pr_{x \in \mathcal{D}^1(\ell)}[x = y] - Pr_{x \in \mathcal{D}^2(\ell)}[x = y]|$$

is negligible in ℓ.

Theorem 10 MBBS-OSBE *is oblivious.*

Proof Suppose that two distribution families are $\mathcal{D}^1(\ell_1) = \{(r \bmod p,\ \ s \bmod p) | (r, s) \in \{1..2^{\ell_1} p\} \times \{1..2^{\ell_1} p\}\}$ and $\mathcal{D}^2(\ell_1) = \{(r' \bmod p,\ s' \bmod p)\ |(r',\, s') \in \{1, \cdots, 2^{\ell_1} p\} \times \{1, \cdots, 2^{\ell_1} p\}\}$. Each distribution has p^2 points. The difference of the probability on any points is at most $\frac{1}{2^{2\ell_1} p^2}$. So, the total difference between the two distribution families is at most $\frac{p^2}{2^{2\ell_1} p^2} = \frac{1}{2^{2\ell_1}}$, which is negligible in ℓ_1. Due to ℓ_1 is linear in ℓ, the total probability difference between the two distribution is negligible in ℓ.

Therefore, $(\hat{r}, \hat{s})$ sent by the two receivers R_1 and R_2 is indistinguishable from the view of sender S, where $(\hat{r}, \hat{s}) = (r, s)$ or (r', s'). S cannot distinguish R_1 from R_2. MBBS-OSBE is oblivious. □

Theorem 11 MBBS-OSBE *is semantically secure against the receiver if no probabilistic polynomial-time adversary can forge a* MBBS *signature.*

Proof MBBS-OSBE uses a semantically secure symmetric encryption algorithm $\mathcal{E}(\cdot)$, where $H(\cdot)$ is modeled as a random oracle. MBBS-OSBE is semantically secure against the receiver if there is no probabilistic polynomial-time adversary $\mathcal{A}$ who can compute the secret key which the sender uses to extract the encryption key with non-negligible probability. Namely, MBBS

- OSBE is semantically secure against the receiver if no probabilistic polynomial-time adversary $\mathcal{A}$ can win the following game against the challenger $\mathcal{X}$ with non -negligible probability:

1. $\mathcal{A} \xleftarrow{(m_1,m_2,\cdots,m_{l-1},g,g_0,g_1,g_2,\cdots,g_l,h,y)} \mathcal{X}$. $\mathcal{X}$ sends the public parameters $(m_1, m_2, \cdots, m_{l-1},\ g,\ g_0,\ g_1, g_2, \cdots, g_l, h, y)$ to $\mathcal{A}$.
2. $\mathcal{A} \xrightarrow{r',s',P_0,P_1} \mathcal{X}$. $\mathcal{A}$ sends partial signature (r', s') and two messages P_0 and P_1 with the same length to $\mathcal{X}$.
3. $\mathcal{A} \xleftarrow{T_0,\ T_1,\ C} \mathcal{X}$. $\mathcal{X}$ flips an unbiased coin with $\{0,1\}$ and obtains $b \in \{0,1\}$. $\mathcal{X}$ chooses $t \overset{R}{\leftarrow} \mathbb{Z}_p \backslash \{0,1\}$, and computes $T_0 = e(g,h)^t$, $T_1 = (yh^{r'})^t$, $T_2 = e(g_0 g^s g_2^{m_1} \cdots g_l^{m_{l-1}}, h)^t$ and $C = \mathcal{E}_{H_2}(T_2)(P_b)$. It sends T_0, T_1 and C to $\mathcal{A}$.
4. $\mathcal{A} \xrightarrow{b'} \mathcal{X}$. $\mathcal{A}$ outputs his guess b' on b. $\mathcal{A}$ wins the game, if $b' = b$.

If there exists an adversary $\mathcal{A}$ who can break the semantic security of MBBS-OSBE against the receiver with advantage at least ϵ, we will show that there exists an algorithm $\mathcal{B}$ who can use $\mathcal{A}$ to forge a MBBS signature with the same advantage.

1. Given $(m_1, m_2, \cdots, m_{l-1}, g, g_0, g_1, \cdots, g_l, h, y)$, the aim of $\mathcal{B}$ is to compute a signature (σ^*, r', s') such that $e(\sigma^*, yh^{r'}) = e(g_0 g_1^{s'} g_2^{m_1} \cdots\ g_l^{m_{l-1}}, h)$. $\mathcal{B}$ sends $(m_1, m_2, \cdots, m_{l-1}, g, g_0, g_1, g_2, \cdots, g_l, h, y)$ to $\mathcal{A}$.
2. $\mathcal{A}$ sends (r', s') and two messages P_0 and P_1 with equal length to $\mathcal{B}$.
3. $\mathcal{B}$ flips an unbiased coin with $\{0,1\}$, and obtains $b \in \{0,1\}$. $\mathcal{B}$ chooses $t \overset{R}{\leftarrow} \mathbb{Z}_p \backslash \{0,1\}$, and computes $T_0 = e(g,h)^t$, $T_1 = (yh^{r'})^t$, $T_2 = e(g_0 g^s g_2^{m_1} \cdots g_l^{m_{l-1}},\ h)^t$ and $C = \mathcal{E}_{H_2}(T_2)(P_b)$. It sends T_0, T_1 and C to $\mathcal{A}$.
4. If $\mathcal{A}$ can outputs his guess with the advantage $|\Pr[b' = b] - \frac{1}{2}| \geq \epsilon$, he can compute a σ^* with the same advantage such that
$$e(\sigma^*, T_1) = e(g_0 g_1^{s'} g_2^{m_1} \cdots g_l^{m_{l-1}}, h)^t,$$
namely
$$\sigma^* = (g_0 g_1^{s'} g_2^{m_1} \cdots g_l^{m_{l-1}})^{\frac{1}{x+r'}}.$$
5. $\mathcal{B}$ aborts. $\mathcal{B}$ can use $\mathcal{A}$ to forge a MBBS message-signature pair $(m_1, m_2, \cdots, m_{l-1}, \sigma^*, r', s')$ with advantage at least ϵ, where
$$\begin{aligned} e(\sigma^*, yh^{r'}) &= e((g_0 g_1^{s'} g_2^{m_1} \cdots g_l^{m_{l-1}})^{\frac{1}{x+r'}}, h^{x+r'}) \\ &= e(g_0 g_1^{s'} g_2^{m_1} \cdots g_l^{m_{l-1}}, h). \end{aligned}$$

□

Theorem 12 *The credential in our MBBS-OSBE is all-or-nothing non-transferable under the computational Diffie-Hellman assumption.*

Proof Given a credential (σ, s, r), if an adversary $\mathcal{A}$ can compute T_2, there will exist an algorithm $\mathcal{B}$ who can use $\mathcal{A}$ to break the CDH assumption as follows.

$\mathcal{A}$ can get the ciphertext (T_0, T_1, C), and compute

$$\begin{aligned} e(\sigma, T_1) &= e((g_0 g_1^c g_2^{m_1} \cdots g_l^{m_{l-1}} y_u)^{\frac{1}{x+r}}, h^{x+r})^t \\ &= e(g_0 g_1^s g_2^{m_1} \cdots g_l^{m_{l-1}}, h)^t e(y_u, h)^t \\ &= e(g_0 g_1^s g_2^{m_1} \cdots g_l^{m_{l-1}}, h)^t e(g, h)^{tx_u} \end{aligned}$$

and

$$T_0 = e(g,h)^t$$

If $\mathcal{A}$ can compute $T_2 = e(g_0 g_1^s g_2^{m_1} \cdots g_l^{m_{l-1}}, h)^t$, he can computes $e(g,h)^{tx_u} = \frac{e(\sigma, T_1)}{T_2}$. Namely, given $e(g,h)^t$ and $e(g,h)^{x_u}$, $\mathcal{B}$ can use $\mathcal{A}$ to compute $e(g,h)^{tx_u}$. So, $\mathcal{B}$ can use $\mathcal{A}$ to break the CDH assumption. □

5 Oblivious Access Control

In this section, we propose an oblivious access control (OAC) scheme based on our MBBS-OSBE scheme and the oblivious transfer (OT) scheme [23]. Actually, our OAC scheme can be implemented by introducing an OSBE scheme to an OT scheme. In our scheme, a user needs to possess a credential from the issuer (manager) prior to access the protected services. Then, he can use his credential to obtain services from the service providers obliviously without releasing his credential and the selected services to them. The service providers only know the number of the services selected by the user if he has possessed the required credential from the issuer. Furthermore, the service providers do not know whether the user has obtained a credential from the issuer or not. Notably, zero-knowledge proof is *not required* in our OAC scheme. Additionally, the credentials of users in our scheme are all-or-nothing non-transferable. Our OAC scheme can resist the eavesdropping attack, and also provide forward security.

5.1 CT-Adaptive t-out-of-n Oblivious Transfer

Chu and Tzeng [23] proposed an efficient t-out-of-n adaptive oblivious transfer (CT-$OT^n_{k\times 1}$) scheme based on chosen target computational Diffie-Hellman assumption. The CT-$OT^n_{k\times 1}$ is as follows:

Setup. Taking as input a security parameter 1^ℓ, this algorithm returns a group $\mathbb{G}$ with prime order p and two hash function H_1 and H_2, where $H_1 : \{0,1\}^* \rightarrow$

$\mathbb{G}$, and $H_2 : \mathbb{G} \rightarrow \{0,1\}^\ell$. Let g be a generator of $\mathbb{G}$. The sender generates his secret-public key pair $\mathcal{KG}(1^\ell) \rightarrow (x, y)$, where $x \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and $y = g^x$. Suppose that the sender has n messages $m_1, m_2, \cdots, m_n \in \{0,1\}^\ell$.

Commitment Phase.

1. The sender computes $\sigma_i = H_1(i)$ and $E_i = m_i \oplus H_2(\sigma_i^x)$, for $i = 1, 2, \cdots, n$.
2. The sender sends $E_1, E_2, \cdots, E_n$ to the receiver.

Transfer Phase.

1. The receiver selects $\gamma_l \in \{1, 2, \cdots, n\}$ and $\beta_l \in \mathbb{Z}_p^*$, and computes $\sigma_{\gamma_l} = H_1(\gamma_l)$ and $Z_l = \sigma_{\gamma_l} g^{\beta_l}$, where $l = 1, 2, \cdots, k$.
2. The receiver sends $Z_1, Z_2, \cdots, Z_k$ to the sender.
3. The sender responds with $C_l = Z_l^x$, for $l = 1, 2, \cdots, k$.
4. The receiver computes $D_l = \frac{C_l}{y^{\beta_l}}$ and obtains $m_{\gamma_l} = E_{\gamma_l} \oplus H_2(D_l)$.

Theorem 13 *$CT\text{-}OT^n_{k\times 1}$ scheme is unconditionally receiver -secure [23].*

Theorem 14 *$CT\text{-}OT^n_{k\times 1}$ scheme is sender-secure under the CT-CDH assumption [23].*

5.2 Oblivious Access Control Scheme

Our OAC scheme consists of the following four algorithms:

Setup. Taking as input a security parameter 1^ℓ, this algorithm returns bilinear groups $(e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_\tau)$ with prime order p, where $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_\tau$. It also generates three hash functions H_1, H_2 and H_3, where $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$, $H_2 : \mathbb{G}_1 \rightarrow \{0,1\}^\ell$, $H_3 : \mathbb{G}_\tau \rightarrow \{0,1\}^\ell$ which is used to extract a key for the semantically secure symmetric encryption $\mathcal{E}(\cdot)$. Let g_0, g_1, g_2, g_3, g_4 be the generators of $\mathbb{G}_1$, and h be the generator of $\mathbb{G}_2$. The issuer generates his secret-public key pair $\mathcal{KG}(1^\ell) \rightarrow (x, y)$, where $x \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and $y = h^x$. Suppose that there are n service providers $SP_1, SP_2, \cdots, SP_n$ in the system. SP_i generates his secret-public key pair $\mathcal{KG}(1^\ell) \rightarrow (x_i, y_i)$, where $x_i \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and $y_i = g_4^{x_i}$ for $i = 1, 2, \cdots, n$. The user generates his secret-public key pair $\mathcal{KG}(1^\ell) \rightarrow (z_u, y_u)$, where $z_u \overset{R}{\leftarrow} \mathbb{Z}_p^*$ and $y_u = g_2^{z_u}$.

Commitment. Suppose that SP_i has k_i service items $S_{i_1}, S_{i_2}, \cdots, S_{i_{k_i}}$, where $S_{i_j} \in \{0,1\}^\ell$ for $j = 1, 2, \cdots, k_i$ and $i = 1, 2, \cdots, n$. SP_i computes $\omega_{i_j} = H_1(i_j)$ and $E_{i_j} = S_{i_j} \oplus H_2(\omega_{i_j}^{x_i})$, and publishes E_{i_j}, for $j = 1, 2, \cdots, k_i$.

Issuing Credentials.

1. The user chooses a service provider SP_i, and sends it to the issuer.
2. The issuer chooses $c, r \overset{R}{\leftarrow} \mathbb{Z}_p$ $(r \neq -x)$, and computes $\sigma_{u_i} = (g_0 g_1^c y_u g_3^{s_i})^{\frac{1}{x+r}}$, where $s_i \in \mathbb{Z}_p^*$ is the identifier of SP_i in the system.

The credential for the user is $(\sigma_{u_i}, c,\ r, s_i)$, which can be used to access the services managed by SP_i.

Access service items.

1. The user chooses $\gamma_l \in \{1, 2, \cdots, k_i\}$, $\beta_l \overset{R}{\leftarrow} \mathbb{Z}_p$, and computes $\omega_{\gamma l} = H_1(\gamma_l)$ and $Z_l = \omega_{\gamma l} g_4^{\beta l}$, for $l = 1, 2, \cdots, \pi_i$, where π_i is determined by SP_i and $\pi_i \leq k_i$. The user sends (r, c, Z_l) to SP_i.
2. SP_i chooses $t \overset{R}{\leftarrow} \mathbb{Z}_p$, and computes $K_l = Z_l^{x_i}$, $T_1 = (yh^r)^t$, $T_2 = e(g_2, h)^t$, $T_3 = e(g_0 g_1^c g_3^{s_i}, h)^t$, $C_l = \mathcal{E}_{H_3(T_3)}(K_l)$, for $l = 1, 2, \cdots, \pi_i$. SP_i sends $D = (T_1, T_2, C_l)$ to the user.
3. The user compute $T_3 = \frac{e(\sigma_{u_i}, T_1)}{T_2^{z_u}}$ and $H_3(T_3)$, decrypts C_l, and gets K_l, for $l = 1, 2, \cdots, \pi_i$. Then, the user computes $A_l = \frac{K_l}{y_i^{\beta_l}}$ and $S_{i_{\gamma_l}} = E_{i_{\gamma_l}} \oplus H_2(A_l)$, for $l = 1, 2, \cdots, \pi_i$.

Theorem 15 *Our oblivious access control system is sound.*

Proof

$$\begin{aligned}
\frac{e(\sigma_{u_i}, T_1)}{T_2^{z_u}} &= \frac{e((g_0 g_1^c g_2^{z_u} g_3^{s_i})^{\frac{1}{x+r}}, yh^r)^t}{e(g_2, h)^{tz_u}} \\
&= \frac{e((g_0 g_1^c g_2^{z_u} g_3^{s_i})^{\frac{1}{x+r}}, h^{x+r})^t}{e(g_2, h)^{tz_u}} \\
&= \frac{e(g_0 g_1^c g_3^{s_i}, h)^t \cdot e(g_2, h)^{tz_u}}{e(g_2, h)^{tz_u}} \\
&= e(g_0 g_1^c g_3^{s_i}, h)^t \\
&= T_3,
\end{aligned}$$

$$A_l = \frac{K_l}{y_i^{\beta_l}} = \frac{Z_l^{x_i}}{y_i^{\beta_l}} = \frac{\omega_{\gamma_l}^{x_i} g_4^{x_i \beta_l}}{y_i^{\beta_l}} = \frac{\omega_{\gamma_l}^{x_i} y_i^{\beta_l}}{y_i^{\beta_l}} = \omega_{\gamma_l}^{x_i},$$

and

$$E_{i_{\gamma_l}} \oplus H_2(A_l) = S_{i_{\gamma_l}} \oplus H_2(\omega_{\gamma_l}^{x_i}) \oplus H_2(\omega_{\gamma_l}^{x_i}) = S_{i_{\gamma_l}}.$$

□

Theorem 16 *Our oblivious access control system is receiver secure.*

Proof 1. In our OAC scheme, the service provider SP_i cannot detect whether the user has a credential or not; otherwise, there will exist an algorithm $\mathcal{B}$, which can use SP_i to break the oblivion property of $\mathsf{MBBS\text{-}OSBE}$.

2. In our OAC scheme, SP_i knows nothing about the content of the service items selected by the user; otherwise, there will exists an algorithm $\mathcal{B}$, which can use SP_i to break the unconditional receiver-security of CT-$OT^n_{k\times 1}$. This proof is the same as that in [23].

So, our oblivious access control system is receiver-secure. □

Theorem 17 *Our oblivious access control system is sender-secure under the q-SDH assumption and $\mathsf{CT\text{-}CDH}$ assumption.*

Proof If there exist an adversary $\mathcal{A}$, who has not possessed a credential, can get π_i services from SP_i, there exist an algorithm $\mathcal{B}$ who can use $\mathcal{A}$ to forge a BBS signature and break the sender-security of CT-$OT^n_{k\times 1}$ as follows:

Given $(g_0, g_1, g_2, g_3, g_4, s_i, y, y_i)$, $\mathcal{A}$ sends (r', c') to SP_i. SP_i picks $t \overset{R}{\leftarrow} \mathbb{Z}_p\backslash\{0,1\}$, computes $T_1 = (yh^{r'})^t$, $T_2 = e(g_2, h)^t, T_3 = e(g_0 g_1^{c'} g_3^{s_i}, h)^t$, and $C_l = \mathcal{E}_{H_3(T_3)}(K_l)$, for $l = 1, 2, \cdots, \pi_i$. SP_i sends (T_1, T_2, C_l) to $\mathcal{A}$. If $\mathcal{A}$ can decrypt C_l, he can compute a σ^*, such that $e(\sigma^*, T_1) = e(\sigma^*, h^{x+r'})^t = e(g_0 g_1^{c'} g_3^{s_i}, h)^t = T_3$, namely $\sigma^* = (g_0 g_1^{c'} g_3^{s_i})^{\frac{1}{x+r'}}$, $\mathcal{B}$ aborts. $\mathcal{B}$ can use $\mathcal{A}$ to forge an MBBS signature (σ^*, r', c') on message s_i, where $e(\sigma^*, yh^{r'}) = e((g_0 g_1^{c'} g_3^{s_i})^{\frac{1}{x+r'}}, h^{x+r'}) = e(g_0 g_1^{c'} g_3^{s_i}, h)$.

If $\mathcal{B}$ dose not abort, he can obtain m_{γ_l} from $\mathcal{A}$, for $l = 1, 2, \cdots, \pi_i$. So $\mathcal{B}$ can use $\mathcal{A}$ to break the sender-security of CT-$OT^n_{k\times 1}$. This proof is the same as that in [23].

So, our oblivious access control system is sender-secure. □

Theorem 18 *Our oblivious access control system is secure against the eavesdropping attack under the q-strong Diffie-Hellman assumption.*

Proof Suppose that an adversary $\mathcal{A}$ has possessed a credential $(\sigma^*, r^*, c^*,\ s_i)$, where $\sigma^* = (g_0 g_1^c g_2^{z^*} g_3^{s_i})^{\frac{1}{x+r^*}}$. If $\mathcal{A}$ can get services $s_{i_{\gamma_1}}, s_{i_{\gamma_2}}, \cdots, s_{i_{\gamma_k}}$, which the legal user selected, we will show that there exists an algorithm $\mathcal{B}$ who can use $\mathcal{A}$ to break the q-SDH assumption and the unconditional receiver-security of CT-$OT^n_{k\times 1}$ as follows:

$\mathcal{A}$ can get the ciphertext $D = (T_1, T_2, C_l)$, where $T_1 = (yh^r)^t$, $T_2 = e(g_2, h)^t$, $T_3 = e(g_0 g_1^c g_3^{s_i}, h)^t$ and $C_l = \mathcal{E}_{H(T_3)}(K_l)$. If $\mathcal{A}$ can decrypt C_l, he can compute a σ such that $e(\sigma, T_1) = e(\sigma, h^{x+r})^t = e(g_0 g_1^c g_3^{s_i}, h)^t = T_3$. $\mathcal{B}$ aborts. $\mathcal{B}$ can use $\mathcal{A}$ to forge a signature (σ, c, r) on s_i, where $e(\sigma, yh^r) = e(g_0 g_1^c g_3^{s_i}, h)$. This will contradict MBBS signature scheme is existentially unforgeable against the adaptively chosen message attacks under the q-strong Diffie-Hellman assumption.

If $\mathcal{B}$ dose not abort, he can get $s_{i_{\gamma_1}}, s_{i_{\gamma_2}}, \cdots, s_{i_{\gamma_{\pi_i}}}$ from $\mathcal{A}$. So $\mathcal{B}$ can use $\mathcal{A}$ to break the the unconditional receiver-security of CT-$OT^n_{k\times 1}$. □

Theorem 19 *Our oblivious access control system is forward secure under computational Diffie-Hellman assumption.*

Proof If the adversary $\mathcal{A}$ who gets the user's credential $(\sigma_{u_i}, c, r, s_i)$ can obtain the services $s_{i_{\gamma_1}}, s_{i_{\gamma_2}}, \cdots, s_{i_{\gamma_{\pi_i}}}$ which the user selected before, we will show that there exists an algorithm $\mathcal{B}$ who can use $\mathcal{A}$ to break the CDH assumption as follows.

From $\mathsf{Theorem}$ 12, if $\mathcal{A}$ can decrypt C_l, he can break the CDH assumption. $\mathcal{B}$ aborts.

If $\mathcal{B}$ dose not abort, he can get the services $s_{i_{\gamma_1}}, s_{i_{\gamma_2}}, \cdots, s_{i_{\gamma_{\pi_i}}}$ from $\mathcal{A}$. $\mathcal{B}$ can use $\mathcal{A}$ to break the unconditional receiver-security of CT-$OT^n_{k\times 1}$. □

6 Other Application

6.1 Attribute-Based Encryption

Proposed by Sahai and Waters [39], attribute-based encryption (ABE) is a public encryption scheme, where both the secret key and the ciphertext are labeled with sets of descriptive attributes. A secret key can decrypt the ciphertext if and only if there is a match between the secret key and the attributes listed in the ciphertext. In an access control system, a user needs to possess a credential (signature) for each attribute of him from the manager (issuer). These credentials are called attribute certificate. So, we can use our OSBE scheme to construct an ABE scheme as follows.

Let $\mathcal{E}_{sign(sk,m)}(P)$ denote the ciphertext of P, which can be decrypted if and only if the user has obtained a signature on m. Suppose that $A_{k_1}, A_{k_2}, \cdots, A_{k_{l_k}}$ are different attributes, where $k = 1, 2, \cdots, n$. If the manager wants to encrypts a message which can be decrypted if and only if the attributes of the user satisfy the following conjunctive normal form

$$(A_{1_1} \vee A_{1_2} \vee \cdots \vee A_{1_{l_1}}) \wedge \cdots \wedge (A_{n_1} \vee A_{n_2} \vee \cdots \vee A_{n_{l_n}})$$

The manager works as follows:

1. Generate his secret-public key pair $\mathcal{KG}(1^\ell) \rightarrow (sk, pk)$, where 1^ℓ is a security parameter.

2. Choose $K_1, K_2, \cdots, K_n$, and computes $K = K_1 \oplus K_2 \oplus \cdots \oplus K_n$.

3. Compute and broadcast

$$\mathcal{E}_{sign(sk,A_{1_1})}(K_1),\ \mathcal{E}_{sign(sk,A_{1_2})}(K_1),\ \cdots,$$

$$\mathcal{E}_{sign(sk,A_{1_{l_1}})}(K_1),\ \cdots,\ \mathcal{E}_{sign(sk,A_{n_1})}(K_n),$$

$$\cdots, \mathcal{E}_{sign(sk,A_{n_{l_n}})}(K_n).$$

4. Compute and broadcast $C = \mathcal{E}_{H(K)}(P)$, where $H(\cdot)$ is a hash function which is used to extract a encryption key for semantically secure encryption $\mathcal{E}(\cdot)$.

If a user has attributes $A_{1_{i_1}}, A_{2_{i_2}}, \cdots, A_{n_{i_n}}$, and has obtained attribute certificates $sign(sk, A_{1_{i_1}})$, $sign(sk, A_{2_{i_2}})$, $\cdots$, $sign(sk, A_{n_{i_n}})$, where $i_j \in \{1, 2, \cdots, l_i\}$. He can use his attribute certificates to decrypt the ciphertext as follows:

1. Decrypts $\mathcal{E}_{sign(sk,A_{1_{i_1}})}(K_1)$, $\mathcal{E}_{sign(sk,A_{2_{i_2}})}(K_2)$, $\cdots$, $\mathcal{E}_{sign(sk,A_{n_{i_n}})}(K_n)$ and obtains K_1, K_2 ,$\cdots$, K_n.

2. Computes $K = K_1 \oplus K_2 \oplus \cdots \oplus K_n$.

3. Decrypts $C = \mathcal{E}_{H(K)}(P)$ and obtains P.

7 Conclusion

In this paper, we clarified the relationship between the one-round OSBE and IBE. We proposed two novel OSBE schemes based on BB signature and MBBS signature. The credentials in our MBBS-OSBE scheme are all-or-nothing non-transferable. Based on our MBBS-OSBE scheme and an oblivious transfer scheme, we proposed a new access control scheme called oblivious access control (OAC). In our OAC scheme, legal users can obliviously obtain services from the service providers. As a result, the user does not release anything about his credential and the selected services to the service providers; while there are no aid of zero knowledge proof. We also pointed out the potential applications of OSBE in ABE.

Acknowledgment

The first author was supported by PhD scholarships of Smart Services Cooperative Research Centre (CRC) and University of Wollongong. The second author was supported by the ARC Future Fellowship FT0991397.

References

1. Argyrakis, J., Gritzalis, S., Kioulafas, C: Privacy enhancing technologies: A review. In: Traunmller R. (ed) Electronic Government (EGOV 2003), vol. 2739 of Lecture Notes in Compture Science, pp. 282-287. Springer, Berlin (2003)
2. Camenisch, J.: Privacy-enhancing cryptography: From theory into prac tice. In: Micciancio, D. (ed) 7th Theory of Cryptography Conference (TCC 2010), vol. 5978 of Lecture Notes in Compture Science, pp. 498-498. Springer, Berlin (2010)
3. Chang, Y.C., Mitzenmacher, M: Privacy preserving keyword searches on remote encrypted data. In: Ioannidis, J., Keromytis A.D., Yung M. (eds) Applied Cryptography and Network Security (ACNS 2005), vol. 3531 of Lecture Notes in Compture Science, pp. 442-455. Springer, Berlin (2005)
4. Frikken, K., Atallah, M., Li, J.: Attribute-based access control with hidden policies and hidden credentials. IEEE Transaction on Computers 55(10): 1259-1270 (2006)
5. Bhargav-Spantzel, A., Camenisch, J., Gross, T., Sommer, D: User centricity: a taxonomy and open issues. In: 2nd ACM workshop on Digital identity management (DIM 2006), pp.2006: 1-10. ACM (2006)
6. Camenisch, J., Pfitzmann, B.: Federated identity management. In: Milan, P., Willem, J. (eds), Security, Privacy, and Trust in Modern Data Man agement, Data-Centric Systems and Applications, pp. 218-238. Springer, Berlin (2007)
7. Li, N., Du, W., Boneh, D.: Oblivious signature-based envelope. In: 22nd Annual Symposium on Principles of Distributed Computing (PODC 2003), pp. 182-189. ACM (2003)
8. Winsborough, W.H., Seamons, K.E., Jones, V.E.: Automated trust negotiation. In: DARPA Information Survivability Conference and Exposition (DISCEX 2000), pp. 88-102. IEEE (2000)
9. Rivest, R.L., Shamir, A., Adleman, L.M.: A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 21(2): 120-126 (1978)
10. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the weil pairing. In: Boyd, C. (ed) Advances in Cryptology (ASIACRYPT 2001), vol. 2248 of Lecture Notes in Compture Science, pp. 514-532. Springer, Berlin (2001)
11. Rabin, M.: Digitalized signatures and public-key functions as in tractable as factorization. Tech. Rep. MIT/LCS/TR-212; MIT Laboratory for Computer Science (1979)
12. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed) Advances in Cryptology (CRYPTO 2001), vol. 2139 of Lecture Notes in Compture Science, pp. 213-229. Springer, Berlin (2001)
13. Cocks, C.: An identity based encryption scheme based on quadratic residues. In: Honary, B. (ed) Cryptography and Coding, vol. 2260 of Lecture Notes in Compture Science, pp. 360-363. Springer, Berlin (2001)
14. Li, N., Du, W., Boneh, D.: Oblivious signature-based envelope. Distributed Computing. 17(4): 293-302 (2005)
15. Zhou, L., Susilo, W., Mu, Y.: Three-round secret handshakes based on ELGamal and DSA. In: Chen, K., Deng, R.H., Lai, X., Zhou, J. (eds) Information Security Practice and Experience (ISPEC 2006), vol. 3903 of Lecture Notes in Compture Science, pp. 332-342. Springer, Berlin (2006)
16. Li, J., Li, N.: A construction for general and efficient oblivious commitment based envelope protocols.

In: Ning, P., Qing, S., Li, N. (eds) 8th International Conference on Information and Communications Security (ICICS 2006), vol. 4307 of Lecture Notes in Compture Science, pp. 122-138. Springer, Berlin (2006)

17. Li, J., Li, N.: Oacerts: Oblivious attribute certificates. In: Ioannidis, J., Keromytis, A.D., Yung, M. (eds) Applied Cryptography and Network Security (ACNS 2005), vol. 3531 of Lecture Notes in Compture Science, pp. 301-317. Springer, Berlin (2005)
18. Nasserian, S., Tsudik, G.: Revisiting oblivious signature-based envelopes. In: Crescenzo, G.D. (ed). Financial Cryptography and Data Security (FC 2006), vol. 4107 of Lecture Notes in Compture Science, pp. 221-235. Springer, Berlin (2006)
19. Holt, J.E., Bradshaw, R.W., Seamons, K.E., Orman, H.: Hidden credentials. In: Jajodia, S., Samarati, P., Syverson, P.F. (eds) Workshop on Privacy in the electronic society (WPES 2003), pp. 2003:1-8. ACM (2003)
20. Bradshaw, R.W., Holt, J.E., Seamons, K.E.: Concealing complex policies with hidden credentials. In: Atluri, V., Pfitzmann, B., McDaniel, P.D. (eds) 11th ACM conference on Computer and communications security (CCS 2004), pp. 146-157. ACM (2004)
21. Coull, S., Green, M., Hohenberger, S.: Controlling access to an oblivious database using stateful anonymous credentials. In: JareckiJ, S., Tsudik, G. (eds) Public Key Cryptography (PKC 2009), vol. 5443 of Lecture Notes in Compture Science, pp. 501-520. Springer, Berlin (2009)
22. Camenisch, J., Dubovitskaya, M., Neven, G.: Oblivious transfer with access control. In: Al-Shaer, E., Jha, S., Keromytis, A.D. (eds) 16th ACM conference on Computer and communications security (CCS 2009), pp. 131-140. ACM (2009)
23. Chu, C.K., Tzeng, W.G.: Efficient k-out-of-n oblivious transfer schemes with adaptive and non-adaptive queries. In: Vaudenay, S. (ed) Public Key Cryptography (PKC 2005), vol. 3386 of Lecture Notes in Compture Science, pp. 172-183. Springer, Berlin (2005)
24. Diffie, W., and Hellman, M. E.: New directions in cryptography. IEEE Transactions on Information Theory. IT-22(6):644654 (1976)
25. Boneh, D. and Boyen, X.: Short signatures without random oracles. In Cachin, C. and Camenisch, J. (eds) Advances in Cryptology (EUROCRYPT 2004), vol. 3027 of Lecture Notes in Computer Science, pp. 5673. Springer, Berlin (2004)
26. Boldyreva, A.: Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme. In Desmedt, Y. (ed) Public Key Cryptography (PKC 2003), vol. 2567 of Lecture Notes in Computer Science, pp. 3146. Springer, Berlin (2003)
27. Boneh, D., Boyen, X.: Short signatures without random oracles. In: Cachin, C., Camenisch, J. (eds) Advances in Cryptology (EUROCRYPT 2004), vol. 3027 of Lecture Notes in Compture Science, pp. 56-73. Springer, Berlin (2004)
28. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakley, G.R., Chaum, D. (eds) Advances in Cryptology (CRYPTO 1984), vol. 196 of Lecture Notes in Compture Science, pp. 47-53. Springer, Berlin (1985)
29. Boneh D and Franklin M. Identity-based encryption from the weil pairing. In: Kilian J, ed. Advances in Cryptology (CRYPTO 2001); vol. 2139 of Lecture Notes in Compture Science. Santa Barbara, California, USA: Springer-Verlag, pp. 213-229. Springer, Berlin (2001)
30. Chow, S.S:. Removing escrow from identity-based encryption new security notions and key management techniqu. In: Jarecki, S., Tsudik, G. (eds) Public Key Cryptography (PKC 2009), vol. 5443 of Lecture Notes in Compture Science, pp. 256-276. Springer, Berlin (2009)
31. Boneh, D., Boyen, X.: Efficient selective-Id secure identity-based encryption without random oracles. In: Cachin, C., Camenisch, J. (eds) Advances in Cryptology (EUROCRYPT 2004), vol. 3027 of Lecture Notes in Compture Science, pp. 223-238. Springer, Berlin (2004)
32. Gentry, C.: Practical identity-based encryption without random oracles. In: Vaudenay, S. (ed) Advances in Cryptology (EUROCRYPT 2006), vol. 4004 of Lecture Notes in Compture Science, pp. 445-464. Springer, Berlin (2006)
33. Kiltz, E.: From selective-ID to full security: The case of the inversion- based boneh-boyen IBE scheme. Cryptology ePrint Archive 2007/033 (2007)
34. Waters, B.: Efficient identity-based encryption without random oracles. In: Cramer, R. (ed) Advances in Cryptology (EUROCRYPT 2005), vol. 3494 of Lecture Notes in Compture Science, pp. 114-127. Springer, Berlin (2005)
35. Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Franklin, M.K. (ed) Advances in Cryptology (CRYPTO 2004), vol. 3152 of Lecture Notes in Compture Science, pp. 41-55. Springer, Berlin (2004)
36. Au, M.H., SusiloJ, W., Mu, Y.: Constant-size dynamic k-TAA. In: Prisco, R.D., Yung, M. (eds) Security and Cryptography for Networks (SCN 2006), vol. 4116 of Lecture Notes in Compture Science, pp. 111-125. Springer, Berlin (2006)
37. Camenisch, J., Lysyanskaya, A.: An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: Pfitzmann, B. (ed) Advances in Cryptology (EUROCRYPT 2001), vol. 2045 of Lecture Notes in Compture Science, pp. 93-118. Springer, Berlin (2001)
38. Camenisch, J., Neven, G., Shelat, A.: Simulatable adaptive oblivious trans- fer. In: Naor, M. (ed) Advances in Cryptology (EUROCRYPT 2007), vol. 4515 of Lecture Notes in Compture Science, pp. 573-590. Springer, Berlin (2007)
39. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed) Advances in Cryptology (EUROCRYPT 2005), vol. 3494 of Lecture Notes in Compture Science, pp. 457-473. Springer, Berlin (2005)