7-2016

Generic anonymous identity-based broadcast encryption with chosen-ciphertext security

Kai HE
Jinan University - China

Jian WENG
Jinan University - China

Man Ho AU
Hong Kong Polytechnic University

Yijun MAO
Sun Yat-sen University

DENG, Robert H.
Singapore Management University, robertdeng@smu.edu.sg

DOI: https://doi.org/10.1007/978-3-319-40367-0_13

Published in Information Security and Privacy: 21st Australasian Conference, ACISP 2016, Melbourne, July 4-6, 2016, Proceedings
https://doi.org/10.1007/978-3-319-40367-0_13

Generic Anonymous Identity-Based Broadcast Encryption with Chosen-Ciphertext Security

Kai He[1,2], Jian Weng[1(✉)], Man Ho Au[3], Yijun Mao[4,5], and Robert H. Deng[6]

[1] Department of Computer Science, Jinan University, Guangzhou, China
hekai1214@yahoo.com, cryptjweng@gmail.com
[2] Faculty of Information Technology, Monash University, Melbourne, Australia
[3] Department of Computing, Hong Kong Polytechnic University, Hong Kong, Hong Kong
[4] School of Mathematics and Informatics, South China University of Agriculture, Guangzhou, China
[5] School of Information Science and Technology, Sun Yat-Sen University, Guangzhou, China
[6] School of Information Systems, Singapore Management University, Singapore, Singapore

Abstract. In a broadcast encryption system, a broadcaster can encrypt a message to a group of authorized receivers S and each authorized receiver can use his/her own private key to correctly decrypt the broadcast ciphertext, while the users outside S cannot. Identity-based broadcast encryption (IBBE) system is a variant of broadcast encryption system where any string representing the user's identity (e.g., email address) can be used as his/her public key. IBBE has found many applications in real life, such as pay-TV systems, distribution of copyrighted materials, satellite radio communications. When employing an IBBE system, it is very important to protect the message's confidentiality and the users' anonymity. However, existing IBBE systems cannot satisfy confidentiality and anonymity simultaneously. In this paper, using an anonymous identity-based encryption (IBE) primitive with robust property as a building block, we propose a generic IBBE construction, which can simultaneously ensure the confidentiality and anonymity under chosen-ciphertext attacks. Our generic IBBE construction has a desirable property that the public parameters size, the private key size and the decryption cost are constant and independent of the number of receivers.

Keywords: Identity-based broadcast encryption · Anonymity · Robustness · Chosen-ciphertext security · Random oracle model

1 Introduction

Broadcast encryption (BE), introduced by Fiat and Naor [16], is one kind of one-to-many encryption that allows a broadcaster to encrypt one message to a group of users who are listening to a broadcast channel, and only the authorized users can get the message. At present, BE causes a wide spread attention in theory and practice. As BE can save most computational cost and communication load relatively to repeatedly utilize point-to-point traditional encryption.

Identity-based broadcast encryption (IBBE) [12,28] is a special kind of public-key BE, in which the public key of each user can be any string just representing the user's identity (e.g., email address) and the private keys of users are generated by a private key generator (PKG) according to their identities. It is the same as in the identity-based encryption [8]. There exists a desired property is that IBBE can support exponentially many users as potential receivers.

While an encryption scheme aims to protect the message's confidentiality, another security requirement, namely, anonymity, which aims to hide the receiver's identity and it is a desirable security property in many application scenarios. Anonymity comes from the key privacy concept, which was first introduced by Bellare et al. [6]. It captures the property that an eavesdropper cannot tell which public key the ciphertext is created under. However, the receiver set S in the traditional IBBE scheme is transmitted as a part of the ciphertext. Obviously, it cannot hide the receivers' identities. Therefore, traditional IBBE schemes are unable to obtain the anonymity requirement.

1.1 Our Contributions

In this paper, we propose a generic identity-based broadcast encryption (IBBE) scheme from a generic anonymous IBE construction, which is the first IBBE scheme simultaneously provide confidentiality and anonymity against chosen-ciphertext attacks under Decisional Bilinear Diffie-Hellman (DBDH) assumption. In addition, the public parameters size, the private key size and the decryption cost are constant and independent of the number of receivers is more efficient than the existing IBBE schemes.

1.2 Related Work

Since broadcast encryption (BE) was introduced by Fiat and Naor [16], many BE schemes have been proposed, e.g., [9,12,13,17,28]. However, these schemes cannot ensure the anonymity of receivers. To address this problem, in 2006, Barth et al. [5] presented two anonymous BE constructions in the public key setting with chosen-ciphertext security. Their first construction is a generic BE construction in the standard model, where the decryption cost is linear with the number of receivers. As it need try to find an appropriate ciphertext component for decryption. Their second construction is an improved construction in which only a constant number of cryptographic operations is required for decryption, whereas the security proof relies on the random oracle model [7]. In PKC 2012, Fazio et al. [15] proposed two outsider-anonymous broadcast encryption constructions with sub-linear ciphertexts, which are adaptive CPA and CCA secure in the standard model, respectively. In the same year, Libert et al. [23] presented several anonymous broadcast encryption constructions with adaptive CCA security in the standard model and gave an united security definition for anonymous BE scheme. However, all of these constructions are in the public key setting.

In 2007, the first IBBE scheme with fix-size ciphertext and private key was proposed by Delerablee [12]. Specially, their scheme supports a flexible number of possible users. That is, the number of users are not determined in the system setup phase. Since then, lots of IBBE schemes with different properties have been proposed, e.g., [19,21,24,25,28,30,31,33,34,37,40]. When identity-based encryption is incorporated to the multi-receiver setting, many multi-receiver identity-based encryption schemes [3,4,10] have been proposed. However, among all of these IBBE and multi-receiver identity-based encryption schemes, the receivers' identities are transmitted as a part of the ciphertext. Obviously, these schemes cannot provide anonymity.

Therefore, many anonymous identity-based broadcast encryption schemes, e.g., [20,26,38] and anonymous multi-receiver identity-based encryption schemes, e.g., [11,14,22,29,35,36,39] have been successively proposed. However, none of these schemes can achieve confidentiality and anonymity simultaneously against chosen-ciphertext attacks. In this paper, we have solved this problem.

1.3 Bilinear Groups

We briefly review the concept of bilinear groups which is the underlying algebraic structure of many IBBE including ours.

We assume there is a probabilistic algorithm $\mathcal{G}$ which takes as input a security parameter λ and outputs a tuple $(p, \mathbb{G}, \mathbb{G}_T, e)$, where $\mathbb{G}$ and $\mathbb{G}_T$ are multiplicative cyclic groups of prime order p (of bit-length λ), and $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is a map, which has the following properties: **Bilinearity:** $e(u^a, v^b) = e(u, v)^{ab}$ for all $u, v \in \mathbb{G}$ and $\forall a, b \in \mathbb{Z}_p$. **Non-degeneracy:** $e(g, g) \neq 1_{\mathbb{G}}$, where g is a generator of $\mathbb{G}$. **Computability:** There exists an efficient algorithm to compute $e(u, v)$ for $\forall u, v \in \mathbb{G}$.

1.4 Decisional Bilinear Diffie-Hellman Assumption

The decisional BDH (DBDH) problem in a bilinear group $(p, \mathbb{G}, \mathbb{G}_T, e)$ is as follows: Given a tuple (g, g^a, g^b, g^c, Z) for $a, b, c \leftarrow_R \mathbb{Z}_p$ as input, output 1 if $Z = e(g, g)^{abc}$ and 0 otherwise. For a probabilistic algorithm $\mathcal{A}$, we define its advantage in solving the DBDH problem as $Adv_{\mathcal{A}}^{\text{DBDH}} = |\Pr[\mathcal{A}(g, g^a, g^b, g^c, e(g, g)^{abc}) = 1] - \Pr[\mathcal{A}(g, g^a, g^b, g^c, Z) = 1]|$, where g is a random generator in $\mathbb{G}$ and $Z \leftarrow_R \mathbb{G}_T$. We say that the DBDH assumption holds if all probabilistic polynomial-time (PPT) algorithms have a negligible advantage in solving the DBDH problem.

2 Identity-Based Broadcast Encryption

We shall review the definition and security notions for identity-based broadcast encryption [18] as follows.

An identity-based broadcast encryption scheme, associated with message space $\mathcal{M}$, consists of a tuple of four algorithms (Setup, $\mathsf{Extract}$, Enc, Dec):

Setup(1^λ)**:** On input of a security parameter λ, it outputs the public parameters $params$ and a master secret key msk.

Extract(msk, ID): On input of a master secret key msk and an identity ID, it outputs a private key sk_{ID} for the identity ID.

Enc$(params, S, M)$**:** On input of the public parameters $params$, a receiver set S and a message $M \in \mathcal{M}$, it outputs a ciphertext CT.

Dec(sk_{ID}, CT)**:** On input of a private key sk_{ID} and a ciphertext CT, it outputs either a message M or an error symbol $\perp$.

The correctness property requires that, for all $ID \in S$, if $(params,\ msk) \leftarrow$ Setup (1^λ), $sk_{ID} \leftarrow$ $\mathsf{Extract}$ $(msk,\ ID)$ and $CT \leftarrow$ Enc $(params,\ S,\ M)$, then Dec $(sk_{ID},\ CT) = M$ with overwhelming probability.

Remark. Identity-based encryption is a special case of identity-based broadcast encryption, when the size of the receiver set is only one.

Next, we shall review the security notions for an IBBE scheme. First, we review the model of indistinguishability under chosen-ciphertext attacks (IND-CCA), which means that the ciphertext does not leak any information of the message. Then, we review the model of anonymity under chosen-ciphertext attacks (ANO-CCA), which means that the ciphertext does not leak any identity in the receiver set. Last, we review the model of weakly robust against chosen-ciphertext attacks (WROB-CCA), which guarantees that the decryption attempts to fail with high probability when the "wrong" private key is used. Respectively, these security models are defined by the following games between a PPT adversary $\mathcal{A}$ and a challenger $\mathcal{C}$.

The IND-CCA Game:

Setup: Challenger $\mathcal{C}$ runs $(params,\ msk) \leftarrow \mathsf{Setup}(1^\lambda)$, and then sends the public parameters $params$ to adversary $\mathcal{A}$ and keeps the master secret key msk itself.

Phase 1: Adversary $\mathcal{A}$ adaptively issues the following queries:

- *Extraction Query:* On input of an identity ID, challenger $\mathcal{C}$ returns $sk_{ID} \leftarrow$ $\mathsf{Extract}(msk, ID)$ to adversary $\mathcal{A}$.
- *Decryption Query:* On input of an identity ID and a ciphertext CT, challenger $\mathcal{C}$ returns $m \leftarrow \mathsf{Dec}(sk_{ID}, CT)$ to adversary $\mathcal{A}$, where $sk_{ID} \leftarrow$ $\mathsf{Extract}(msk, ID)$.

Challenge: Adversary $\mathcal{A}$ submits two distinct equal-length messages M_0, M_1 $\in \mathcal{M}$ and a receiver set S^* to challenger $\mathcal{C}$. It is required that $\mathcal{A}$ has not issued *Extraction Query* on $ID \in S^*$. Then challenger $\mathcal{C}$ flips a random coin $\beta \in \{0,1\}$ and returns the challenge ciphertext $CT^* \leftarrow$ $\mathsf{Encrypt}$ $(params,\ S^*,\ M_\beta)$ to adversary $\mathcal{A}$.

Phase 2: Adversary $\mathcal{A}$ continues to adaptively issue queries as in Phase 1 subject to the following restrictions: (i) $\mathcal{A}$ cannot issue *Extraction Query* on ID, where $ID \in S^*$; (ii) $\mathcal{A}$ cannot issue *Decryption Query* on (ID, C^*), where $ID \in S^*$.

Guess: Adversary $\mathcal{A}$ outputs a guess $\beta' \in \{0, 1\}$.

Definition 1. *We define adversary $\mathcal{A}$'s advantage in the* IND-CCA Game *as* $Adv_{\mathcal{A},\mathrm{IBBE}}^{\text{IND-CCA}} = |\Pr[\beta' = \beta] - 1/2|$. *We say that an* IBBE *scheme is* IND-CCA secure*, if for any* PPT *adversary $\mathcal{A}$, the advantage $Adv_{\mathcal{A},\mathrm{IBBE}}^{\text{IND-CCA}}$ is negligible in* IND-CCA Game*.*

The ANO-CCA Game:

Setup: It is the same as in the IND-CCA Game.

Phase 1: It is the same as in the IND-CCA Game.

Challenge: Adversary $\mathcal{A}$ submits a message M^* and two distinct sets S_0, S_1 to challenger $\mathcal{C}$. It is required that $|S_0| = |S_1|$ and adversary $\mathcal{A}$ has not issued *Extraction Query* on $ID \in S_0 \triangle S_1$, where $S_0 \triangle S_1$ denotes $S_0 \cup S_1 - S_0 \cap S_1$. Then challenger $\mathcal{C}$ flips a random coin $\beta \in \{0, 1\}$ and returns the challenge ciphertext $CT^* \leftarrow \mathsf{Encrypt}(params, S_\beta, M^*)$ to $\mathcal{A}$.

Phase 2: Adversary $\mathcal{A}$ continues to adaptively issue queries as in Phase 1 with the restrictions as follows: (i) Adversary $\mathcal{A}$ cannot issue *Extraction Query* on ID, where $ID \in S_0 \triangle S_1$; (ii) Adversary $\mathcal{A}$ cannot issue *Decryption Query* on (ID, C^*), where $ID \in S_0 \triangle S_1$.

Guess: Adversary $\mathcal{A}$ outputs a guess $\beta' \in \{0, 1\}$.

Definition 2. *We define adversary $\mathcal{A}$'s advantage in the above* ANO-CCA Game *as* $Adv_{\mathcal{A},\mathrm{IBBE}}^{\text{ANO-CCA}} = |\Pr[\beta' = \beta] - 1/2|$. *We say that an* IBBE *scheme is* ANO-CCA secure*, if for any* PPT *adversary $\mathcal{A}$, the advantage $Adv_{\mathcal{A},\mathrm{IBBE}}^{\text{ANO-CCA}}$ is negligible in the above* ANO-CCA Game*.*

Remark. Note that the definition captures not only outsider attacks but also insider attacks. In other words, even when an identity $ID \in S_0 \cap S_1$ is corrupted, the anonymity of any non-corrupted $ID \in S_0 \triangle S_1$ is still preserved.

The WROB-CCA Game:

Setup: It is the same as in the IND-CCA Game.

Query Phase: It is the same as Phase 1 in the IND-CCA Game.

Output: Adversary $\mathcal{A}$ outputs a message M, a receiver set $S^* = \{ID_1, ID_2, \cdots, ID_t\}$, where $|S^*| = t$. Challenger $\mathcal{C}$ outputs the challenge ciphertext $CT^* \leftarrow \mathsf{Encrypt}\ (params,\ S^*,\ M)$.

We say that $\mathcal{A}$ wins the WROB-CCA Game if $\mathsf{Dec}(sk_{ID^*},\ CT^*) \neq \perp$, where $ID^* \notin S^*$ and $sk_{ID^*} = \mathsf{Extract}\ (msk,\ ID^*)$. It is required that $\mathcal{A}$ has not issued *Extraction Query* on ID^* in Query Phase.

We define adversary $\mathcal{A}$'s advantage as the probability of that $\mathcal{A}$ wins.

Definition 3. *We say that an* IBBE *scheme is* WROB-CCA secure*, if for all* PPT *adversaries $\mathcal{A}$, the advantage of winning the above* WROB-CCA Game *is negligible.*

Remark. The above security notions of IND-CCA, ANO-CCA and WROB-CCA can be naturally defined for an identity-based encryption (IBE) scheme by limiting the size of the receiver set to be only one.

3 Generic Anonymous IBBE from IBE

In this section, we present a generic IBBE construction which builds on a IND-CCA secure, ANO-CCA secure and WROB-CCA secure IBE primitive. The generic IBBE construction has a desirable property that the public parameters size, the private key size and the decryption cost are all constant and independent of the number of receivers, while the ciphertext size is linear with the size of the receivers.

3.1 Construction

Given an IND-CCA, ANO-CCA and WROB-CCA secure IBE scheme IBE= ($\mathsf{IBE.Setup}$, $\mathsf{IBE.Extract}$,$\mathsf{IBE.Enc}$,$\mathsf{IBE.Dec}$) and a strong one-time signature scheme $\Sigma = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$, we construct an IND-CCA and ANO-CCA secure IBBE construction $\mathsf{IBBE} = (\mathsf{IBBE.Setup}, \mathsf{IBBE.Extract}, \mathsf{IBBE.\ Enc}, \mathsf{IBBE.Dec})$.

IBBE.Setup(1^λ)**:** On input of a security parameter λ, it generates a bilinear map $(p, \mathbb{G}, \mathbb{G}_T, e)$, where $\mathbb{G}$ and $\mathbb{G}_T$ are two cyclic groups with prime order p and e is a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. Then, it chooses $g \leftarrow_R \mathbb{G}$, $\alpha \leftarrow_R \mathbb{Z}_p$ and computes $g_1 = g^\alpha$. Next, it runs $\langle \widehat{params}, \widehat{msk} \rangle \leftarrow \mathsf{IBE.Setup}(1^\lambda)$. Besides, it chooses three hash functions H_1, H_2, H_3, such that $H_1 : \{0,1\}^* \to \mathbb{G}$, $H_2 : \mathbb{G}_T \to \{0,1\}^\lambda$ and $H_3 : \{0,1\}^* \to \mathbb{Z}_p$. The public parameters are $params = (\mathbb{G}, \mathbb{G}_T, \mathbb{Z}_p, e, p, g, g_1, \widehat{params}, H_1, H_2, H_3)$ and the master secret key is $msk = (\alpha, \widehat{msk})$.

IBBE.Extract(msk, ID)**:** On input of a master secret key msk and an identity ID, it computes $sk^0_{ID} = H_1(ID)^\alpha$ and $sk^1_{ID} \leftarrow \mathsf{IBE.Extract}(\widehat{msk}, ID)$. It outputs the private key sk_{ID} =(sk^0_{ID}, sk^1_{ID}) for the identity ID.

IBBE.Enc$(params, S, M)$**:** On input of the public parameters $params$, a receiver set $S = \{ID_1, ID_2, \cdots, ID_t\}$ and a message M, it first generates a signature key pair $(svk, ssk) \leftarrow \mathsf{Gen}\ (1^\lambda)$. Then it chooses $\delta \leftarrow_R \mathbb{Z}_p$, lets $r = H_3(\delta, M)$ and computes the common part of the ciphertext $T = g^r$. Next, for each $ID \in S$, it computes $c^0_{ID} = H_2(e(g_1, H_1(ID))^r)$ and $c^1_{ID} \leftarrow \mathsf{IBE.Enc}(\widehat{params}, ID, svk \mid\mid \delta \mid\mid M)$. Let $C_1 = (c^0_{ID_1}, c^1_{ID_1}) \mid\mid \cdots \mid\mid (c^0_{ID_t}, c^1_{ID_t})$. The ciphertext is $CT = (svk, T, C_1, \sigma)$, where $\sigma = \mathsf{Sig}\ (ssk, T \mid\mid C_1)$.

IBBE.Dec(sk_{ID}, CT)**:** On input of a private key $sk_{ID} = (sk^0_{ID}, sk^1_{ID})$ and a ciphertext $CT = (svk, T, C_1, \sigma)$, where $C_1 = (\ c^0_{ID_1}, c^1_{ID_1}) \mid\mid \cdots \mid\mid (c^0_{ID_t}, c^1_{ID_t})$. It checks whether $\mathsf{Ver}(svk, T||C_1, \sigma) = 1$ holds. If not, it returns $\perp$. Otherwise, it computes $c^0_{ID} = H_2(e(T, sk^0_{ID}))$. If $c^0_{ID} \neq c^0_{ID_j}$ for all $j \in \{1, \cdots, t\}$, returns $\perp$; else considers the smallest index j such that $c^0_{ID} = c^0_{ID_j}$, then computes $L \leftarrow \mathsf{IBE.Dec}(sk^1_{ID}, c^1_{ID_j})$. If $L =\perp$, returns $\perp$; else parses L as $svk'||\delta'||M$. If $svk' \neq svk$ or $T \neq g^{H_3(\delta', M)}$, returns $\perp$; else returns M.

The correctness of IBBE construction follows directly from the correctness and weak robustness of IBE scheme.

3.2 Security Analysis

In this subsection, we analyze that the above IBBE construction is ANO-CCA secure. Regarding the IND-CCA security, we have the following Theorem 1, whose proof can be found in the full paper.

Theorem 1. *Suppose that H_3 is a random oracle, the* IBE *scheme is* IND-CCA *secure and the signature Σ scheme is a strong one-time signature, then the generic* IBBE *construction in Sect. 3 is* IND-CCA *secure.*

Next, we shall prove the following Theorem 2, which states that our IBBE construction is ANO-CCA secure.

Theorem 2. *Suppose that H_1, H_2, H_3 are random oracles, the* IBE *scheme are* WROB-CCA *and* ANO-CCA secure, *the signature Σ scheme is a strong one-time signature scheme and the* DBDH *assumption holds, then the above* IBBE *construction is* ANO-CCA *secure.*

Proof. We proceed by a sequence of hybrid games starting with $Game_0$ where adversary $\mathcal{A}$ is given an encryption of M^* on S_0. At the last game, adversary $\mathcal{A}$ is given an encryption of M^* on S_1. Without loss of generality, we suppose S_0 and S_1 are different by only one receiver and $|S_0| = |S_1| = t$. (The general case can be proved through a hybrid argument, which is the adversary $\mathcal{A}$ selects the receiver sets differing by only one receiver each time.) Let ID_v be the unique element of $S_0 \backslash S_1$, ID_w be the unique element of $S_1 \backslash S_0$. (Note that $S_i \backslash S_j = \{ID | ID \in S_i \cap ID \notin S_j\}$)

Game$_0$: The challenge ciphertext CT^* is a correctly encrypted M^* on receiver set S_0, where $CT^* = (svk^*, T^*, C^*_1, \sigma^*)$ and $C^*_1 = (c^{0*}_{ID_1},\ c^{1*}_{ID_1})\ ||\cdots||\ (c^{0*}_{ID_t},\ c^{1*}_{ID_t})$. Let $c = (c^{0*}_{ID_v},\ c^{1*}_{ID_v}) = (H_2(e(g_1,\ H_1(ID_v))^r),\ \mathsf{IBE.Enc}(\widehat{params},\ ID_v,\ svk^*\ ||\delta^*||\ M^*))$ be the challenge ciphertext component which is related to the identity ID_v.

Game$_1$: It is the same as $Game_0$, but the challenger rejects all post challenge *Decryption Query* $\langle ID, CT\rangle$, where CT contains the same verification key svk^*.

Game$_2$: c is replaced with $(R,\ \mathsf{IBE.Enc}(\widehat{params},\ ID_v,\ svk^*\ ||\delta^*||\ M^*))$, where $R \leftarrow_R \{0,1\}^\lambda$.

Game$_3$: c is replaced with $(R,\ \mathsf{IBE.Enc}(\widehat{params},\ ID_w,\ svk^*\ ||\delta^*||\ M^*))$.

Game$_4$: c is replaced with $(H_2(\ e(g_1,\ H_1(ID_w))^r),\ \mathsf{IBE.Enc}(\widehat{params},\ ID_w,\ svk^*\ ||\delta^*||\ M^*))$. Notice that the component is now encrypted on ID_w instead of ID_v.

Game$_5$: It is the same as $Game_4$, but the challenger does not reject all post challenge *Decryption Query* $\langle ID, CT\rangle$, where CT contains the same verification key svk^*. Notice that the challenge ciphertext CT^* is correctly encrypted M^* under the receiver set S_1 now.

The above games differ slightly from each other. In the following lemmas, we shall show that every two adjacent games are computationally indistinguishable. Transitivity shows that $Game_0$ and $Game_5$ are computationally indistinguishable. The challenge ciphertext CT^* in $Game_0$ is encrypted M^* on receiver set S_0 and the challenge ciphertext CT^* in $Game_5$ is encrypted M^* on receiver set S_1. According to the ANO-CCA Game, we can achieve that the above IBBE construction is ANO-CCA secure.

Lemma 1. *Suppose that the signature scheme Σ is a strong one-time signature scheme, then $Game_0$ and $Game_1$ are computationally indistinguishable.*

Proof. We define event F that adversary $\mathcal{A}$ makes a legal *Decryption Query* on $(ID, CT = (svk, T, C_1, \sigma))$, where $\mathsf{Ver}(svk, T||C_1, \sigma) = 1$ and $svk = svk^*$ and $\langle(T||C_1), \sigma\rangle \neq \langle(T^*||C_1^*), \sigma^*\rangle$. Suppose event F happens, then it is easy to construct a PPT algorithm $\mathcal{C}$, which makes use of adversary $\mathcal{A}$ to break the underlying one-time signature scheme Σ.

Setup: $\mathcal{C}$ is given a verification key svk^*. Then $\mathcal{C}$ runs $(params,\ msk) \leftarrow \mathsf{IBBE.Setup}(1^\lambda)$. Next, it returns $params$ to $\mathcal{A}$ and keeps msk itself.

Phase 1: $\mathcal{A}$ can adaptively issue *Extraction Query* and *Decryption Query*. $\mathcal{C}$ can answer any *Extraction Query* and *Decryption Query* since it has the master secret key msk.

Challenge: $\mathcal{A}$ submits a message M^* and two distinct sets S_0, S_1 to $\mathcal{C}$. It is required that $\mathcal{A}$ has not issued *Extraction Query* on ID in Phase 1, where $ID \in \{ID_v, ID_w\}$. $\mathcal{C}$ first runs $\mathsf{IBBE.Enc}(params,\ S_0,\ M^*)$ to obtain a part of ciphertext $\langle T^*, C_1^*\rangle$, and then obtains (from its signing oracle) a signature σ^* on the "message"$\langle T^*||C_1^*\rangle$. Finally, $\mathcal{C}$ sends challenge ciphertext $CT^* = (svk^*, T^*, C_1^*, \sigma^*)$ to $\mathcal{A}$.

Phase 2: $\mathcal{A}$ continues to adaptively issue queries as follows:

- *Extraction Query:* $\mathcal{A}$ issues *Extraction Query* on ID, such that $ID \notin \{ID_v,\ ID_w\}$, $\mathcal{C}$ handles them as in Phase 1.
- *Decryption Query:* $\mathcal{A}$ issues *Decryption Query* on $\langle ID, CT\rangle$, $\mathcal{C}$ parses CT as $(svk,\ \sigma,\ T,\ C_1)$, if $\mathsf{Ver}\ (svk,\ T\ ||C_1,\ \sigma) = 1$, $svk = svk^*$ and $\langle(T||C_1), \sigma\rangle \neq \langle(T^*||C_1^*), \sigma^*\rangle$, then $\mathcal{C}$ presents $\langle(T||C_1), \sigma\rangle$ as a forgery and aborts. Otherwise, $\mathcal{C}$ answers these queries with the master secret key msk as in Phase 1.

Guess: $\mathcal{A}$ outputs a bit $b' \in \{0, 1\}$.

Observe that $Game_0$ and $Game_1$ are identical as long as event F does not happen. If event F happens with a non-negligible probability, then $\mathcal{C}$ can forge a valid signature with a non-negligible advantage. However, since the signature scheme Σ is a strong one-time signature scheme, then event F happens with negligible probability.

Hence, $Game_0$ and $Game_1$ are computationally indistinguishable.

Lemma 2. *Suppose that* DBDH *assumption holds, then* $Game_1$ *and* $Game_2$ *are computationally indistinguishable.*

Proof. Suppose there exists an adversary $\mathcal{A}$ who can distinguish $Game_1$ from $Game_2$. It is easy to construct a PPT algorithm $\mathcal{C}$ that makes use of $\mathcal{A}$ to solve the DBDH problem. Suppose $\mathcal{C}$ is given a DBDH challenge (g, g^a, g^b, g^c, Z) with unknown $a, b, c \in \mathbb{Z}_p$, $\mathcal{C}$'s goal is to output 1 if $Z = e(g, g)^{abc}$ and 0 otherwise. $\mathcal{C}$ acts as a challenger with adversary $\mathcal{A}$ as follows.

Setup: $\mathcal{C}$ runs $(\widehat{params}, \widehat{msk}) \leftarrow \mathsf{IBE.Setup}(1^\lambda)$, sets $g_1 = g^a$, and chooses H_1, H_2, H_3 as random oracles. $\mathcal{C}$ gives the public parameters $params = (\widehat{params}$, g, g_1, H_1, H_2, $H_3)$ to $\mathcal{A}$ and keeps $\widehat{msk}$ itself.

Phase 1: $\mathcal{A}$ adaptively issues queries as follows:

$Hash_1$ Query: On input of an identity ID, $\mathcal{C}$ does as follows: if there exists a record $\langle ID, Q, q, \varpi \rangle$ in the H_1-list, which the list is initially empty, returns Q; else chooses $\varpi \leftarrow_R \{0, 1\}$ and $q \leftarrow_R \mathbb{Z}_p$. If $\varpi = 0$, computes $Q = g^q$; else computes $Q = g^{bq}$ and adds $\langle ID, Q, q, \varpi \rangle$ into the H_1-list. $\mathcal{C}$ returns Q to $\mathcal{A}$.

$Hash_2$ Query: On input of X, $\mathcal{C}$ does the following: if there exists a record $\langle X, v \rangle$ in the H_2-list, which the list is initially empty, returns v; else selects $v \leftarrow_R \mathbb{Z}_p$, and adds $\langle X, v \rangle$ into the H_2-list. $\mathcal{C}$ returns v to $\mathcal{A}$.

$Hash_3$ Query: On input of (δ, M), $\mathcal{C}$ does the following: if there exists a record $\langle \delta, M, r, g^r \rangle$ in the H_3-list, which the list is initially empty, returns r; else selects $r \leftarrow_R \mathbb{Z}_p$, adds $\langle \delta, M, r, g^r \rangle$ into the H_3-list. Returns r to adversary $\mathcal{A}$.

Extraction Query: On input of an identity ID, $\mathcal{C}$ first issues $Hash_1$ *Query* on the identity ID and gets the tuple $\langle ID, Q, q, \varpi \rangle$. If $\varpi = 1$, $\mathcal{C}$ outputs $\perp$ and aborts; else $\mathcal{C}$ computes $sk_{ID}^0 = g_1^q$. Then runs $\mathsf{IBE.Extract}(\widehat{msk}, ID)$ to obtain sk_{ID}^1. $\mathcal{C}$ returns $sk_{ID} = (sk_{ID}^0, sk_{ID}^1)$ to adversary $\mathcal{A}$.

Decryption Query: On input of $\langle ID, CT \rangle, \mathcal{C}$ parses CT as (svk, σ, T, C_1), where $C_1 = (c_{ID_1}^0, c_{ID_1}^1)||\cdots||(c_{ID_t}^0, c_{ID_t}^1)$. If $\mathsf{Ver}(svk, T||C_1, \sigma) = 0$, $\mathcal{C}$ outputs $\perp$; else $\mathcal{C}$ issues $Hash_1$ Query on ID to obtain the tuple $\langle ID, Q, q, \varpi \rangle$. When $\varpi = 0$, $\mathcal{C}$ computes $sk_{ID}^0 = g_1^q$, and then uses sk_{ID}^0 and the master secret key $\widehat{msk}$ to respond this *Decryption Query*. When $\varpi = 1$, $\mathcal{C}$ computes $sk_{ID}^1 \leftarrow \mathsf{IBE.Extract}(\widehat{msk}, ID)$, computes $L = \mathsf{IBE.Dec}(sk_{ID}^1, c_{ID_j}^1)$ in turn for $j \in \{1, 2, \cdots, t\}$. If L is $\perp$, continues to the next j until L as $svk'||\delta'||M'$. Then checks if $svk = svk'$, if not, output $\perp$; else queries $Hash_3$ *Query* on (δ', M') to gets $(\delta', M', r', g^{r'})$, and then checks if $T = g^{r'}$, if not, outputs $\perp$; else returns M'.

Challenge: Adversary $\mathcal{A}$ submits a message M^* and two distinct sets S_0, S_1 to $\mathcal{C}$. It is required that $\mathcal{A}$ has not issued *Extraction Query* on ID in Phase 1, where $ID \in \{ID_v, ID_w\}$. $\mathcal{C}$ first runs $(svk^*, ssk^*) \leftarrow \mathsf{Gen}(1^\lambda)$ and sets $T^* = g^c$. Then, $\mathcal{C}$ issues $Hash_1$ Query on ID_v to obtain the tuple $\langle ID_v, Q_v, q_v, \varpi_v \rangle$. If $\varpi_v = 0$, $\mathcal{C}$ outputs $\perp$ and aborts; else $\mathcal{C}$ computes $X_v^* = Z^{q_v}$. $\mathcal{C}$ issues $Hash_1$ Query on all ID_j, where $ID_j \in S_0/ID_v$, to obtain the corresponding tuple $\langle ID_j, Q_j, q_j, \varpi_j \rangle$. If there exists some $\varpi_j = 1$, outputs $\perp$ and aborts; else computes $X_j^* = e(g^a, g^c)^{q_j}$. Meanwhile, for all $ID_j \in S_0$, $\mathcal{C}$ queries $Hash_2$ *Query* on X_j^* to obtain $c_{ID_j}^{0*}$, where $c_{ID_j}^{0*} = H_2(X_j^*)$. Next, $\mathcal{C}$ chooses a random δ^* and runs $c_{ID_j}^{1*} \leftarrow \mathsf{IBE.Enc}(\widehat{params}, ID_j, svk^* || \delta^* || M^*)$ for $ID_j \in S_0$. Let $C_1^* = (c_{ID_1}^{0*}, c_{ID_1}^{1*}) || \cdots || (c_{ID_t}^{0*}, c_{ID_t}^{1*})$. Last, $\mathcal{C}$ runs $\sigma^* \leftarrow \mathsf{Sig}(ssk^*, T^* || C_1^*)$ and returns $CT^* = (svk^*, T^*, C_1^*, \sigma^*)$ to adversary $\mathcal{A}$.

Phase 2: $\mathcal{A}$ continues to adaptively issue queries as follows:

Extraction Query: Adversary $\mathcal{A}$ issues *Extraction Query* on ID, where $ID \notin \{ID_v, ID_w\}$, $\mathcal{C}$ handles them as in Phase 1.

Decryption Query: Adversary $\mathcal{A}$ issues *Decryption Query* on $\langle ID, CT \rangle$. $\mathcal{C}$ parses $CT = (svk, T, C_1, \sigma)$, where $C_1 = (c_{ID_1}^0, c_{ID_1}^1) || \cdots || (c_{ID_t}^0, c_{ID_t}^1)$. If $svk = svk^*$ or $\mathrm{Ver}(svk, T || C_1, \sigma) = 0$, $\mathcal{C}$ outputs $\perp$. Otherwise, $\mathcal{C}$ does as follows:

- When $CT = CT^*$ and $ID \in \{ID_v, ID_w\}$, $\mathcal{C}$ outputs $\perp$;
- When $CT = CT^*$ and $ID \in S_0 \cap S_1$, $\mathcal{C}$ outputs M^*;
- When $(CT = CT^*$ and $ID \notin S_0 \cup S_1)$ or $(CT \neq CT^*$ and $ID \notin \{ID_v, ID_w\})$, $\mathcal{C}$ answers as in Phase 1;
- When $CT \neq CT^*$ and $ID \in \{ID_v, ID_w\}$, $\mathcal{C}$ computes $sk_{ID}^1 \leftarrow \mathsf{IBE.Extract}$ $(\widehat{msk}, ID)$. If there does not exist $j \in \{1, 2, \cdots, t\}$, such that $c_{ID_j}^1 = c_{ID_v}^{1*}$, $\mathcal{C}$ answers as in Phase 1; Otherwise, if there exists some $j \in \{1, 2, \cdots, t\}$, such that $c_{ID_j}^1 = c_{ID_v}^{1*}$, where $c_{ID_v}^{1*} \leftarrow \mathsf{IBE.Enc}(\widehat{params}, ID_v, svk^* || \delta^* || M^*)$. When $ID = ID_v$, $\mathcal{C}$ outputs $\perp$, as the corresponding message is $svk^* || \delta^* || M^*$, as $svk = svk^*$ has been rejected. When $ID = ID_w$, $\mathcal{C}$ answers as in Phase 1.

Guess: $\mathcal{A}$ outputs a bit $b' \in \{0, 1\}$.

It is easy to observe that, if $Z = e(g, g)^{abc}$, then $\mathcal{C}$ has properly simulated $Game_1$. If Z is uniform and independent in G_T then $\mathcal{C}$ has properly simulated $Game_2$. Therefore, if $\mathcal{A}$ can distinguish $Game_1$ and $Game_2$ with a non-negligible advantage, then $\mathcal{C}$ also has a non-negligible advantage to resolve the DBDH problem. However, the DBDH assumption is hard to resolve. Hence, $Game_1$ and $Game_2$ are computationally indistinguishable.

Lemma 3. *Suppose that the* IBE *scheme are* ANO-CCA *secure and WROB-CCA secure, then $Game_2$ and $Game_3$ are computationally indistinguishable.*

Proof. Suppose there exists an adversary $\mathcal{A}$ who can distinguish $Game_2$ from $Game_3$, it is easy to construct a PPT algorithm $\mathcal{C}$ who makes use of $\mathcal{A}$ to break the IBE scheme's ANO-CCA security or the IBE scheme's WROB-CCA security. $\mathcal{C}$ acts as a challenger and plays with adversary $\mathcal{A}$ as follows.

Setup: $\mathcal{C}$ first receives the master public key $\widehat{params}$ from the IBE challenger. Then $\mathcal{C}$ picks generator $g \in_R \mathbb{G}$, $\alpha \in_R \mathbb{Z}_p$, computes $g_1 = g^\alpha$ and chooses hash functions H_1, H_2, H_3. Next, $\mathcal{C}$ gives public parameters $params = (\widehat{params}, g, g_1, H_1, H_2, H_3)$ to $\mathcal{A}$ and keeps α itself.

Phase 1: $\mathcal{A}$ adaptively issues queries as follows:

- *Extraction Query:* On input of an identity ID, $\mathcal{C}$ first issues *Extraction Query* on ID to the IBE challenger to obtain sk^1_{ID}, and then $\mathcal{C}$ computes $sk^0_{ID} = H_1(ID)^\alpha$. Finally, $\mathcal{C}$ returns $sk_{ID} = (\ sk^0_{ID}, sk^1_{ID})$ to adversary $\mathcal{A}$.
- *Decryption Query:* On input of $\langle ID, CT\rangle$, $\mathcal{C}$ first parses CT as (svk, σ, T, C_1), where $C_1 = (c^0_{ID_1}, c^1_{ID_1})\ ||\cdots||(\ c^0_{ID_t}, c^1_{ID_t})$. If $\mathsf{Ver}(svk, T||C_1, \sigma) = 0$, $\mathcal{C}$ outputs $\perp$; else $\mathcal{C}$ computes $sk^0_{ID} = H_1(ID)^\alpha$ and $c^0_{ID} = H_2(\ e(T, sk^0_{ID}))$. If there is no $c^0_{ID_j} = c^0_{ID}$ for $j \in \{1, \cdots, t\}$, $\mathcal{C}$ returns $\perp$; else $\mathcal{C}$ considers the smallest index j such that $c^0_{ID_j} = c^0_{ID}$, and then $\mathcal{C}$ issues *Decryption Query* on (ID, c^1_{ID}) to the IBE challenger and obtains a result L. If $L = \perp$, $\mathcal{C}$ outputs $\perp$; else parses L as $svk'||\delta'||M'$, checks if $svk = svk'$, if not, outputs $\perp$; else issues $Hash_3$ *Query* on (δ', M') and obtains $(\delta', M', r', g^{r'})$, checks whether $T = g^{r'}$ holds, if not, outputs $\perp$; else returns M'.

Challenge: $\mathcal{A}$ submits a message M^* and two distinct sets S_0, S_1 to $\mathcal{C}$. It is required that $\mathcal{A}$ has not issued *Extraction Query* on $ID \in \{ID_v, ID_w\}$ in $\mathsf{Phase\ 1}$. First, $\mathcal{C}$ picks $\delta^* \leftarrow_R \mathbb{Z}_p$, computes $r = H_3(\delta^*, M^*)$ and sets $T^* = g^r$. Second, $\mathcal{C}$ runs $(svk^*, ssk^*) \leftarrow \mathsf{Gen}(1^\lambda)$, sets $m^* = svk^*||\delta^*||M^*$ and sends m^* and (ID_v, ID_w) to the IBE challenger and receives a ciphertext $c^{1*}_{ID_\beta} \leftarrow \mathsf{IBE.Enc}$ $(\widehat{params}, ID_\beta, m^*)$ from IBE challenger. Third, $\mathcal{C}$ chooses a random $R \in \{0,1\}^\lambda$ and sets $c^{0*}_{ID_\beta} = R$. For $ID_j \in S_0 \cap S_1$, $\mathcal{C}$ computes $c^0_{ID_j} = H_2(e(g_1, H_1(ID_j))^r)$ and $c^1_{ID_j} \leftarrow \mathsf{IBE.Enc}(\widehat{params}, ID_j, svk^*||\delta^*||M^*)$. Let C^*_1 be the concatenation of $(c^0_{ID_j}, c^1_{ID_j})$ for all $ID_j \in S_\beta$. Fianlly, $\mathcal{C}$ runs $\sigma^* \leftarrow \mathsf{Sig}(ssk^*, T^*||C^*_1)$ and returns the challenge ciphertext $CT^* = (svk^*, T^*, C^*_1, \sigma^*)$ to adversary $\mathcal{A}$.

Phase 2: $\mathcal{A}$ continues to adaptively issue queries as follows:

Extraction Query: $\mathcal{A}$ issues *Extraction Query* on ID, where $ID \notin \{ID_v, ID_w\}$, $\mathcal{C}$ handles them as in $\mathsf{Phase\ 1}$.
Decryption Query: $\mathcal{A}$ issues *Decryption Query* on $\langle ID, CT\rangle$, $\mathcal{C}$ parses CT as (svk, σ, T, C_1), where $C_1 = (c^0_{ID_1}, c^1_{ID_1})||\cdots||(\ c^0_{ID_t}, c^1_{ID_t})$. If $svk = svk^*$ or $\mathsf{Ver}(svk, T||C_1, \sigma) = 0$, then $\mathcal{C}$ outputs $\perp$. Otherwise, $\mathcal{C}$ does as follows:

- When $CT = CT^*$ and $ID \in \{ID_v, ID_w\}$, $\mathcal{C}$ outputs $\perp$;
- When $CT = CT^*$ and $ID \in S_0 \cap S_1$, $\mathcal{C}$ outputs M^*;
- When $(CT = CT^*$ and $ID \notin S_0 \cup S_1)$ or $(CT \neq CT^*$ and $ID \notin \{ID_v, ID_w\})$, $\mathcal{C}$ answers as in $\mathsf{Phase\ 1}$;
- When $CT \neq CT^*$ and $ID \in \{ID_v, ID_w\}$, $\mathcal{C}$ first computes $sk^0_{ID} = H_1(ID)^\alpha$ and $c^0_{ID} = H_2(e(T, sk^0_{ID}))$. For each $j \in \{1, \cdots, t\}$, if $c^0_{ID_j} \neq c^0_{ID}$, $\mathcal{C}$ returns $\perp$; else $\mathcal{C}$ considers the smallest index j such that $c^0_{ID_j} = c^0_{ID}$. If $c^1_{ID} = c^{1*}_{ID_\beta}$, $\mathcal{C}$ outputs $\perp$. Since $c^{1*}_{ID_\beta} \leftarrow \mathsf{IBE.Enc}(ID_\beta, svk^*||\delta^*||M^*)$, when $ID = ID_\beta$,

$\mathsf{IBE.Dec}(sk_{ID_\beta}, c^{1*}_{ID_\beta})$ and the corresponding message is $svk^*||\delta^*||M^*$, as $svk = svk^*$ has been rejected; When $ID \in \{ID_v, ID_w\}/\{ID_\beta\}$. As the IBE scheme is WROB-CCA secure, then $\mathsf{IBE.Dec}(sk_{ID}, c^{1*}_{ID_\beta}) \neq \perp$ with negligible probability. Otherwise, $\mathcal{C}$ issues *Decryption Query* on (ID, c^1_{ID}) to IBE challenger as in Phase 1.

Guess: $\mathcal{A}$ outputs a bit $b' \in \{0,1\}$.

If the IBE challenger encrypts $svk^*||\delta^*||M^*$ under ID_v, then $\mathcal{C}$ is simulating $Game_2$; else the IBE challenger encrypts $svk^*||\delta^*||M^*$ under ID_w, that is $\mathcal{C}$ is simulating $Game_3$. Therefore, if adversary $\mathcal{A}$ can distinguish $Game_2$ from $Game_3$ with a non-negligible advantage, then $\mathcal{C}$ also have a non-negligible advantage to break the ANO-CCA security or WROB-CCA security of the IBE scheme. However, the IBE scheme is ANO-CCA secure and WROB-CCA secure. Hence, $Game_2$ and $Game_3$ are computationally indistinguishable.

Lemma 4. *Suppose that* DBDH *assumption holds, then* $Game_3$ *and* $Game_4$ *are computationally indistinguishable.*

Proof. The case for distinguishing $Game_3$ from $Game_4$ is symmetric with the case for distinguishing $Game_1$ from $Game_2$.

Lemma 5. *Suppose that the signature scheme* Σ *is a strong one-time signature scheme, then* $Game_4$ *and* $Game_5$ *are computationally indistinguishable.*

Proof. The case for distinguishing $Game_4$ from $Game_5$ is symmetric with the case for distinguishing $Game_0$ from $Game_1$.

4 Comparisons

In this section, we compare the security and performance among the existing anonymous IBBE schemes and our concrete instantiation from our generic IBBE construction which is presented in Appendix A. The results of comparisons are presented in Table 1.

In Table 1, it shows that the constructions [14,29] and the first construction [39] have some security flaws in their security proofs. As constructions [11,29] both pointed out construction [14] does not achieve anonymity. Constructions [22,35] both pointed out construction [29] does not achieve anonymity. Construction [36] gave an insider attack about anonymity for the first scheme of [39]. Construction [11] and the second construction [39] do not have security proofs. Construction [32] is only an outsider-anonymous IBBE with adaptive CPA security in standard model. Constructions [20,26,38] are all CPA, while our construction can simultaneously ensure the confidentiality and anonymity under chosen-ciphertext attacks. In particular, our scheme is not less efficient than these existing IBBE schemes, although all of them cannot obtain the same security as ours. Thus, the comparison results indicate that our concrete IBBE scheme has a better overall security and performance. The symbol "×" means there exists some security flaws or problems in their security proofs and "–" means there is no security proof in the scheme.

Table 1. Security and Performance Comparisons

	[14]	[11]	[29]	[39]-1	[39]-2	[20]	[26]	[38]	[32]	Ours
Confidentiality	CCA	-	CCA	CCA	-	CPA	CPA	CPA	CPA	CCA
Outsider Anonymity	$\times$	-	CCA	CCA	-	CPA	CPA	CPA	CPA	CCA
Insider Anonymity	$\times$	-	$\times$	$\times$	-	CPA	CPA	CPA	–	CCA
Security Model	ROM	-	ROM	ROM	-	ROM	STD	STD	STD	ROM
Pk Size	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(n)$	$\mathcal{O}(\ell)$	$\mathcal{O}(\ell)$	$\mathcal{O}(1)$
Sk Size	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(k)$	$\mathcal{O}(k)$	$\mathcal{O}(1)$
CT Size	$\mathcal{O}(k)$	$\mathcal{O}(k)$	$\mathcal{O}(k)$	$\mathcal{O}(k)$	$\mathcal{O}(k)$	$\mathcal{O}(k)$	$\mathcal{O}(k)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(k)$
Decryption time	$\mathcal{O}(1)$	$\mathcal{O}(k)$	$\mathcal{O}(1)$	$\mathcal{O}(k)$	$\mathcal{O}(k)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$

5 Conclusion

In this paper, we propose a generic IBBE scheme from a generic anonymous IBE construction. The generic IBBE scheme obtains the confidentiality and anonymity against chosen-ciphertext attacks simultaneously. In addition, the scheme has a desirable property, that is the public parameters size, the private key size and the decryption cost are constant and independent of the number of receivers. However, our construction is proved in the random oracle model. So our future work is to construct a generic anonymous IBBE construction with chosen-ciphertext security in the standard model.

Acknowledgments. This work was supported by National Science Foundation of China (Grant Nos. 61272413, 61133014, 61272415 and 61472165), Program for New Century Excellent Talents in University (Grant No. NCET-12-0680), Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20134401110011), Foundation for Distinguished Young Talents in Higher Education of Guangdong (Grant No. 2012LYM 0027), the Fundamental Research Funds for the Central Universities (Grant No. 11613106), and this work is also supported by China Scholarship Council.

A A Concrete Instantiation

We shall present a concrete instantiation based on the generic IBBE construction, employing Boneh-Franklin IBE scheme [8], which is IND-CCA secure and ANO-CCA secure as noticed in [1] and WROB-CCA secure as noticed in [2] and a concrete signature scheme, e.g. [27] which is a strong one-time signature scheme $\Sigma = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$.

Setup(1^λ)**:** On input of a security parameter λ, it first chooses a bilinear group $\mathbb{G}, \mathbb{G}_T$ of prime order p with bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ and a generator $g \leftarrow_R \mathbb{G}$, and then picks $\alpha, \beta \leftarrow_R \mathbb{Z}_p$, computes $g_1 = g^\alpha$ and $g_2 = g^\beta$, chooses hash functions $H_1 : \{0,1\}^* \to \mathbb{G}$, $H_2 : \{0,1\}^\ell \times \{0,1\}^n \to \mathbb{Z}_p$, $H_3 : \mathbb{G}_T \to \{0,1\}^\ell$, $H_4 : \{0,1\}^\ell \to \{0,1\}^{(\lambda+\ell+n)}$, $H_5 : \{0,1\}^\ell \times \{0,1\}^{\lambda+\ell+n} \to \mathbb{Z}_p$ which are modeled as random oracles. The public parameters are $params = (\mathbb{G}, \mathbb{G}_T, \mathbb{Z}_p, p, e, g, g_1, g_2, H_1, H_2, H_3, H_4, H_5)$ and the master secret key is $msk = (\alpha, \beta)$.

Extract(msk, ID)**:** On input of the master secret key msk and an identity ID, it computes $sk^0_{ID} = H_1(ID)^\alpha$ and $sk^1_{ID} = H_1(ID)^\beta$. The private key is $sk_{ID} = (sk^0_{ID}, sk^1_{ID})$.

Enc$(params, S, M)$**:** On input of the public parameters $params$, a receiver set $S = \{ID_1, ID_2, \cdots, ID_t\}$ and a message $M \in \{0,1\}^n$, it first runs $(svk, ssk) \leftarrow \mathsf{Gen}(1^\lambda)$, chooses $\delta_1, \delta_2 \leftarrow_R \{0,1\}^\ell$, lets $r_1 = H_2(\delta_1||M)$ and $r_2 = H_5(\delta_2||svk||\delta_1 \, ||M)$, and then computes $T_1 = g^{r_1}$ and $T_2 = g^{r_2}$. For each $ID \in S$, it computes $c^0_{ID} = H_3(e(g_1, H_1(ID))^{r_1})$ and $c^1_{ID} = (c^{10}_{ID}, c^{11}_{ID}) = (H_3(e(g_2, H_1(ID))^r) \oplus \delta_2, H_4(\delta_2) \oplus (svk||\delta_1 \, ||M))$. Let $C_1 = (c^0_{ID_1}, c^1_{ID_1})|| \cdots ||(c^0_{ID_t}, c^1_{ID_t})$. The ciphertext is $CT = (svk, T_1, T_2, C_1, \sigma)$, where $\sigma = \mathsf{Sig}(ssk, T_1||T_2||C_1)$.

Dec(sk_{ID}, CT)**:** On input of a private key sk_{ID} and a ciphertext CT, it parses CT as (svk, σ, T, C_1), where $C_1 = (c^0_{ID_1}, c^1_{ID_1})|| \cdots ||(c^0_{ID_t}, c^1_{ID_t})$. If $\mathsf{Ver}(svk, T_1||T_2||C_1, \sigma)$=0, returns $\perp$; else computes $c^0_{ID} = H_3\ (e(T_1, sk^0_{ID}))$ and determines which ciphertext should be decrypted among $(c^0_{ID_1}, c^1_{ID_1})|| \cdots ||(c^0_{ID_t}, c^1_{ID_t})$. For each $ID_j \in S$, if $c^0_{ID} \neq c^0_{ID_j}$, returns $\perp$; else chooses the smallest index j such that $c^0_{ID} = c^0_{ID_j}$ and $c^1_{ID} = c^1_{ID_j}$. It computes $\delta'_2 = H_3(e(T_2, sk^1_{ID})) \oplus c^{10}_{ID}$, $svk||\delta_1||M = H_4(\delta'_2) \oplus c^{11}_{ID}$. If $T_1 \neq g^{H_2(\delta_1||M)}$ or $T_2 \neq g^{H_5(\delta_2||svk||\delta_1||M)}$, returns $\perp$; else returns M.

References

1. Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T., Malone-Lee, J., Neven, G., Paillier, P., Shi, H.: Searchable encryption revisited: consistency properties, relation to anonymous IBE, and extensions. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 205–222. Springer, Heidelberg (2005)
2. Abdalla, M., Bellare, M., Neven, G.: Robust encryption. In: IACR Cryptology ePrint Archive, 2008/440 (2008)
3. Baek, J., Safavi-Naini, R., Susilo, W.: Efficient multi-receiver identity-based encryption and its application to broadcast encryption. In: Vaudenay, S. (ed.) PKC 2005. LNCS, vol. 3386, pp. 380–397. Springer, Heidelberg (2005)
4. Barbosa, M., Farshim, P.: Efficient identity-based key encapsulation to multiple parties. In: IACR Cryptology ePrint Archive, 2005/217 (2005)
5. Barth, A., Boneh, D., Waters, B.: Privacy in encrypted content distribution using private broadcast encryption. In: Di Crescenzo, G., Rubin, A. (eds.) FC 2006. LNCS, vol. 4107, pp. 52–64. Springer, Heidelberg (2006)
6. Bellare, M., Boldyreva, A., Desai, A., Pointcheval, D.: Key-privacy in public-key encryption. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 566–582. Springer, Heidelberg (2001)
7. Bellare, M., Rogaway, P.: Random oracles are practical: A paradigm for designing efficient protocols (1995)

8. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
9. Boneh, D., Gentry, C., Waters, B.: Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 258–275. Springer, Heidelberg (2005)
10. Chatterjee, S., Sarkar, P.: Multi-receiver identity-based key encapsulation with shortened ciphertext. In: Barua, R., Lange, T. (eds.) INDOCRYPT 2006. LNCS, vol. 4329, pp. 394–408. Springer, Heidelberg (2006)
11. Chien, H.-Y.: Improved anonymous multi-receiver identity-based encryption. Comput. J. **55**(4), 439–446 (2012)
12. Delerablée, C.: Identity-based broadcast encryption with constant size ciphertexts and private keys. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 200–215. Springer, Heidelberg (2007)
13. Dodis, Y., Fazio, N.: Public key broadcast encryption for stateless receivers. In: Security and Privacy in Digital Rights Management, ACM CCS-9 Workshop, DRM 2002, Washington, DC, USA, November 18, 2002, pp. 61–80 (2002)
14. Fan, C.-I., Huang, L.-Y., Ho, P.-H.: Anonymous multireceiver identity-based encryption. IEEE Trans. Comput. **59**(9), 1239–1249 (2010)
15. Fazio, N., Perera, I.M.: Outsider-anonymous broadcast encryption with sublinear ciphertexts. In: Proceedings of the Public Key Cryptography - PKC 2012–15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, May 21–23, 2012, pp. 225–242 (2012)
16. Fiat, A., Naor, M.: Broadcast encryption. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 480–491. Springer, Heidelberg (1994)
17. Gentry, C., Waters, B.: Adaptive security in broadcast encryption systems (with short ciphertexts). In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 171–188. Springer, Heidelberg (2009)
18. He, K., Weng, J., Liu, J.-N., Liu, J.K., Liu, W., Deng, R.H.: Anonymous identity-based broadcast encryption with chosen-ciphertext security. In: Accepted for publication in ASIACCS 2016, January 2016
19. Liang, H., Liu, Z., Cheng, X.: Efficient identity-based broadcast encryption without random oracles. JCP **5**(3), 331–336 (2010)
20. Hur, J., Park, C., Hwang, S.: Privacy-preserving identity-based broadcast encryption. Inf. Fusion **13**(4), 296–303 (2012)
21. Kim, I., Hwang, S.O.: An optimal identity-based broadcast encryption scheme for wireless sensor networks. IEICE Trans. **96–B**(3), 891–895 (2013)
22. Li, H., Pang, L.: Cryptanalysis of wang et al'.s improved anonymous multi-receiver identity-based encryption scheme. IET Inf. Secur. **8**(1), 8–11 (2014)
23. Libert, B., Paterson, K.G., Quaglia, E.A.: Anonymous broadcast encryption: Adaptive security and efficient constructions in the standard model. In: Proceedings of Public Key Cryptography - PKC 2012 - 15th InternationalConference on Practice and Theory in Public Key Cryptography, Darmstadt, May 21-23, 2012, pp. 206–224 (2012)
24. Liu, W., Liu, J., Wu, Q., Qin, B.: Hierarchical identity-based broadcast encryption. In: Susilo, W., Mu, Y. (eds.) ACISP 2014. LNCS, vol. 8544, pp. 242–257. Springer, Heidelberg (2014)
25. Ren, Y., Dawu, G.: Fully CCA2 secure identity based broadcast encryption without random oracles. Inf. Process. Lett. **109**(11), 527–533 (2009)
26. Ren, Y., Niu, Z., Zhang, X.: Fully anonymous identity-based broadcast encryption without random oracles. I. J. Netw. Sec. **16**(4), 256–264 (2014)

27. Rompel, J.: One-way functions are necessary and sufficient for secure signatures. In: Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, May 13–17, 1990, Baltimore pp. 387–394 (1990)
28. Sakai, R., Furukawa, J.: Identity-based broadcast encryption. Cryptology ePrint Archive, Report 2007/217 (2007)
29. Wang, H., Yi-Chun Zhang, H., Xiong, H., Qin, B.: Cryptanalysis and improvements of an anonymous multi-receiver identity-based encryption scheme. IET Inf, Sec. **6**(1), 20–27 (2012)
30. Wang, J., Bi, J.: Lattice-based identity-based broadcast encryption scheme. IACR Cryptology ePrint Archive, 2010/288 (2010)
31. Qing, W., Wang, W.: New identity-based broadcast encryption with constant ciphertexts in the standard model. JSW **6**(10), 1929–1936 (2011)
32. Xie, L., Ren, Y.: Efficient anonymous identity-based broadcast encryption without random oracles. IJDCF **6**(2), 40–51 (2014)
33. Yang, C., Zheng, S., Wang, L., Xiuhua, L., Yang, Y.: Hierarchical identity-based broadcast encryption scheme from LWE. J. Commun. Netw. **16**(3), 258–263 (2014)
34. Zhang, B., Xu, Q.: Identity-based broadcast group-oriented encryption from pairings. In: The Second International Conference on Future Generation Communication and Networking, FGCN 2008, vol. 1, Main Conference, Hainan Island, China, December 13–15, 2008, pp. 407–410 (2008)
35. Zhang, J.H., Cui, Y.B.: Comment an anonymous multi-receiver identity-based encryption scheme. IACR Cryptology ePrint Archive, 2012/201 (2012)
36. Zhang, J., Mao, J.: An improved anonymous multi-receiver identity-based encryption scheme. Int. J. Commun. Syst. **28**(4), 645–658 (2015)
37. Zhang, L., Hu, Y., Mu, N.: An identity-based broadcast encryption protocol for ad hoc networks. In: Proceedings of the 9th International Conference for Young Computer Scientists, ICYCS 2008, Zhang Jia Jie, Hunan, China, November 18–21, 2008, pp. 1619–1623 (2008)
38. Zhang, L., Wu, Q., Mu, Y.: Anonymous identity-based broadcast encryption with adaptive security. In: Wang, G., Ray, I., Feng, D., Rajarajan, M. (eds.) CSS 2013. LNCS, vol. 8300, pp. 258–271. Springer, Heidelberg (2013)
39. Zhang, M., Takagi, T.: Efficient constructions of anonymous multireceiver encryption protocol and their deployment in group e-mail systems with privacy preservation. IEEE Syst. J. **7**(3), 410–419 (2013)
40. Zhao, X., Zhang, F.: Fully CCA2 secure identity-based broadcast encryption with black-box accountable authority. J. Syst. Softw. **85**(3), 708–716 (2012)