Efficient Identity-based Signcryption without Random Oracles

Peter Hyun-Jeen Lee[1] **Udaya Parampalli**[1] **Shivaramakrishnan Narayan**[2]

[1] Department of Computing and Information Systems
University of Melbourne
Victoria, 3010, Australia
Email: {phjlee, udaya}@csse.unimelb.edu.au

[2] Optimal Payments
1620 27th Avenue NE Calgary
Alberta T2E 8W4 Canada
Email: kris.narayan@optimalpayments.com

Abstract

In this paper, we propose a new Identity-based signcryption (IBSC) scheme in the standard model. Our scheme shows an improvement of approximately 40% reduction in the ciphertext size when compared to the previously proposed IBSC schemes in the standard model. Further, we argue that the previous IBSC schemes do not provide sufficient simulation ability in the security game. We show that with some minor overhead, we are able to correct this. The security reduction of our scheme is based on the hardness of the hashed modified decision bilinear Diffie-Hellman problem and the modified computational Diffie-Hellman problem.

1 Introduction

Signcryption which was initially proposed by Zheng (1997), is a public key cryptographic primitive which combines encryption and signing as a single logical operation. The main motivation is to lower the computational and storage cost compared to performing a sequence of encryption and signing.

Later, Boneh & Franklin (2001) gave the first efficient construction of Identity-based encryption (IBE) in the random oracle model. Its ability to derive a public key from an identity string simplified the inherent public key authentication issue in public key encryption. Thus, this naturally led the movement towards the adaptation of signcryption in IBE setting.

Since the initial work on Identity-based signcryption (IBSC) by Malone-Lee (2002), there have been numerous IBSC schemes proposed in the random oracle model (Barreto et al. 2005, Boyen 2003, Chen & Malone-Lee 2005, Chow et el. 2003, Libert & Quisquator 2003, Libert & Quisquater 2004, McCullagh & Barreto 2004, Nalla & Reddy 2003, Yuen & Wei 2005, Zhang, Gao, Chen & Geng 2009, Zhang, Yang, Zhu & Zhang 2010). Although the random oracle model is an accepted proving methodology and enables efficient constructions, it has also been criticized due to its practical issue that the security of a scheme can be broken when an idealized hash function is replaced with a real world hash function (Goldwasser & Kalai 2003).

However, constructing a secure IBSC scheme in the standard model is non-trivial and many previous attempts have resulted in failures. For instance, Ren & Gu (2007) proposed the first IBSC scheme in the standard model which was later shown to be broken by Wang et al. (2010). Yu et al. (2009) proposed another IBSC scheme in the standard model. Again, Zhang (2010) and Jin et al. (2010) independently showed that Yu et al.'s scheme is broken and attempted at correcting the security flaw. However, it turns out both of these attempts have failed (see Section 2.7 for details). Thus, it still remains as an interesting problem to construct a secure IBSC scheme in the standard model.

1.1 Contribution

In this paper, we propose a new IBSC scheme in the standard model. Our contributions can be divided into *efficiency improvement* and *stronger security result*.

Efficiency improvement: Our scheme performs similarly in terms of computational cost compared to that of Jin et al. (2010) and Zhang (2010). In terms of ciphertext size, we reduce it by approximately 40% compared to the previous schemes. This is due to the complexity assumption that we rely on called the hashed modified decision bilinear Diffie-Hellman assumption which enables us to remove the inclusion of an extension field element from the ciphertext.

Stronger security result: Our security proof shows a stronger result than those of the previously presented IBSC schemes (Jin et al. 2010, Yu et al. 2009, Zhang 2010) in the standard model. In the previous schemes the simulator aborts during the security game when the adversary issues *failing queries*, which are signcrypt/unsigncrypt queries for which the simulator is unable to generate the private keys. This is due to the simulation abort during extract queries in Waters IBE (Waters 2006) which is also used in their schemes. Although the abort does not affect the CPA security of Waters IBE, this allows an adversary to trivially distinguish a simulated envrionment from a real

The work of P. Lee and U. Parampalli was supported in part by the Australia China Special Fund for S&T Cooperation, Department of Innovation, Industry, Science and Research (DIISR) Australia, under Grant CH090262.

environment if used directly to provide CCA security as in the previous IBSC schemes. For instance, the reduction requires the challenge identities fixed at the challenge phase be the ones for which the simulator is unable to generate the private keys. Then, in phase 2 the adversary can simply issue signcrypt/unsigncrypt queries involving the challenged identites which will always cause the simulator to abort. We stress that *failing queries* should be answered and we achieve this at the cost of an additional group operation in each of signcrypt and unsigncrypt, and a group element in the private key.

1.2 Organization

The rest of this paper is organized as follows. In Section 2, we introduce the necessary background material. Then, in Section 3 we present our scheme followed by its security proof in Section 4. Next, we give an efficiency comparison in Section 5 and finally conclude in Section 6.

2 Preliminaries

2.1 Identity Based Signcryption (IBSC) Scheme

An IBSC scheme consists of the following four algorithms (Malone-Lee 2002).

Setup$(1^{\mathcal{K}})$**:** Given $1^{\mathcal{K}}$ for a security parameter $\mathcal{K} \in \mathbb{Z}^+$, outputs the system public key M_{pk} and the secret key M_{sk}.

Exract$(\mathbf{u})$**:** Given an identity $\mathbf{u}$, outputs the private key $d_{\mathbf{u}}$.

Signcrypt$(d_{\mathbf{u}_A}, \mathbf{u}_B, M)$**:** Given a message M, a receiver identity $\mathbf{u}_B$ and the private key of a sender $d_{\mathbf{u}_A}$, outputs the signcryption CT.

Unsigncrypt$(\mathbf{u}_A, d_{\mathbf{u}_B}, \mathsf{CT})$**:** Given a ciphertext CT, the sender identity $\mathbf{u}_A$ and the private key of the receiver $d_{\mathbf{u}_B}$, outputs the original message M or $\perp$.

2.2 Security Model

We restate the two security requirements for an IBSC scheme namely, *message confidentiality* and *unforgeability* which appear in (Malone-Lee 2002).

Confidentiality: In order to achieve confidentiality, an IBSC scheme must provide *indistinguishability of identity-based signcryptions under adaptive chosen ciphertext attack*(IND-IBSC-CCA2), which is a natural adaptation of *indistinguishability of encryptions under adaptive chosen ciphertext attack* for public key encryption schemes. Now, we describe the game which is played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

Setup: $\mathcal{C}$ runs **Setup**$(1^{\mathcal{K}})$ for a security parameter $\mathcal{K} \in \mathbb{Z}^+$ and passes the system public key M_{pk} to the adversary $\mathcal{A}$ and keeps the master secret M_{sk} to himself.

Phase 1: $\mathcal{A}$ may issue a polynomial number of the following queries:

Extraction queries on $\mathbf{u}_i$: Given an identity $\mathbf{u}_i$, $\mathcal{C}$ computes $d_{\mathbf{u}_i}$ = **Extract**$(\mathbf{u}_i)$ and gives the generated private key $d_{\mathbf{u}_i}$ to $\mathcal{A}$.

Signcrypt queries on $(\mathbf{u}_i, \mathbf{u}_j, M)$: Given a sender identity $\mathbf{u}_i$, a receiver identity $\mathbf{u}_j$ and a message M, $\mathcal{C}$ generates the ciphertext CT and passes it to $\mathcal{A}$.

Unsigncrypt queries on $(\mathbf{u}_i, \mathbf{u}_j, \mathsf{CT})$: Given a sender identity $\mathbf{u}_i$, a receiver identity $\mathbf{u}_j$ and a ciphertext CT, $\mathcal{C}$ unsigncrypts it and passes the result to $\mathcal{A}$.

Challenge: $\mathcal{A}$ chooses two messages M_0, M_1 and two identities $\mathbf{u}_A, \mathbf{u}_B^*$ on which he wishes to be challenged on. Note that the choice of $\mathbf{u}_A$ is flexible where as $\mathbf{u}_B^*$ must be an identity for which $\mathcal{A}$ has not asked the private key for.

Phase 2: Same as **Phase 1**, except that $\mathcal{A}$ is not allowed issue the following queries **Extract**$(\mathbf{u}_B^*)$ and **Unsigncrypt**$(\mathbf{u}_A, \mathbf{u}_B^*, \mathsf{CT})$.

Guess: Finally, $\mathcal{A}$ outputs its guess bit b' and wins the game if $\mathsf{b}' = \mathsf{b}$.

Definition 1. We say that an identity-based signcryption scheme is IND-IBSC-CCA2 secure if no polynomially bounded adversary has non-negligible advantage in the game described above.

Unforgeability: Similar to confidentiality, *existential unforgeability of identity based signcryptions under chosen message attack* (EUF-IBSC-CMA) is a natural adaptation of *existential unforgeability under adaptive chosen message attack* for signature schemes.

Again the game is played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

Setup: $\mathcal{C}$ runs **Setup**$(1^{\mathcal{K}})$ for a security parameter $\mathcal{K} \in \mathbb{Z}^+$ and passes the system public key M_{pk} to the adversary $\mathcal{A}$ and keeps the master secret M_{sk} to himself.

Attack: $\mathcal{A}$ may issue a polynomially bounded number of the following queries:

Extraction queries on $\mathbf{u}_i$: Given an identity $\mathbf{u}_i$ runs $d_{\mathbf{u}_i}$ = **Extract**$(\mathbf{u}_i)$ and gives the generated private key $d_{\mathbf{u}_i}$ to $\mathcal{A}$.

Signcrypt queries on $(\mathbf{u}_i, \mathbf{u}_j, M)$: Given a sender identity $\mathbf{u}_i$, a receiver identity $\mathbf{u}_j$ and a message M, generates the ciphertext CT and passes it to $\mathcal{A}$.

Unsigncrypt queries on $(\mathbf{u}_i, \mathbf{u}_j, \mathsf{CT})$: Given a sender identity $\mathbf{u}_i$, a receiver identity $\mathbf{u}_j$ and a ciphertext CT, unsigncrypts it and passes the result to $\mathcal{A}$.

Forge: Finally $\mathcal{A}$ outputs $(\mathsf{CT}^*, \mathbf{u}_A^*, \mathbf{u}_B)$, where $\mathbf{u}_A^*$ is not an identity for which $\mathcal{A}$ issued extract query during Attack. $\mathcal{A}$ wins if **Unsigncrypt**$(\mathbf{u}_A^*, d_{\mathbf{u}_B}, \mathsf{CT}^*)$ does not return $\perp$. Note that there is no restriction on $\mathbf{u}_B$ unlike $\mathbf{u}_A^*$.

The advantage of $\mathcal{A}$ is $Adv(\mathcal{A}) = \Pr[\mathcal{A} \text{ wins}]$.

Definition 2. We say that an identity-based signcryption scheme is EUF-IBSC-CMA secure if no polynomially bounded adversary has non-negligible advantage in the above game.

2.3 Bilinear Maps

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two multiplicative cyclic groups of prime order q. Let $\mathbb{Z}_q^*$ denote the set of all non-zero integers modulo prime q. A mapping $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, satisfying the following properties is a bilinear map.

Bilinearity: $\forall g_1, g_2 \in \mathbb{G}, a, b \in \mathbb{Z}_q^*$: $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$.

Non-degeneracy: $e(g_1, g_2) \neq 1$.

Computability: e is efficiently computable.

2.4 Complexity Assumptions

Assumption 1 (Hashed Modified Decision Bilinear Diffie-Hellman (HmDBDH) (Gagné et al. 2010)). Let $H : \mathbb{G}_T \rightarrow \{0,1\}^{n_m+|g|} \times \mathbb{Z}_q^*$ be a hash function. Given the two distributions $\langle g, g^a, g^{a^2}, g^b, g^c, H(e(g,g)^{abc})\rangle \in \mathbb{G}^5 \times \{0,1\}^{n_m+|g|} \times \mathbb{Z}_q^*$ and $\langle g, g^a, g^{a^2}, g^b, g^c, R\rangle \in \mathbb{G}^5 \times \{0,1\}^{n_m+|g|} \times \mathbb{Z}_q^*$, where n_m denotes plaintext length, n_u denotes identity string length, g is a generator of $\mathbb{G}$, $a, b, c \in_R (\mathbb{Z}_q^*)^3$, $R \in_R \{0,1\}^{n_m+|g|} \times \mathbb{Z}_q^*$ and $e(g,g) \in \mathbb{G}_T$. The HmDBDH problem is to distinguish the two distributions. We define the advantage ϵ of an adversary $\mathcal{B}$ in solving the HmDBDH problem as,

$$\Pr[\mathcal{B}(\mathbb{G}, \mathbb{G}_T, e, g, g^a, g^{a^2}, g^b, g^c, H(e(g,g)^{abc})) = 1] - \Pr[\mathcal{B}(\mathbb{G}, \mathbb{G}_T, e, g, g^a, g^{a^2}, g^b, g^c, R) = 1],$$

where the probability is over randomly chosen a, b, c, R. We say the HmDBDH assumption holds if ϵ is negligible for all adversaries $\mathcal{B}$.

Assumption 2 (Modified Computational Diffie-Hellman(mCDH)). Given $\langle g, g^a, g^{a^2}, g^b\rangle \in \mathbb{G}^4$, where g is a generator of $\mathbb{G}$ and $a, b \in_R (\mathbb{Z}_q^*)^2$, the mCDH problem is to compute g^{ab}.

We define the advantage ϵ of an adversary $\mathcal{B}$ in solving the mCDH problem as,

$$\Pr[\mathcal{B}(\mathbb{G}, \mathbb{G}_T, e, g, g^a, g^{a^2}, g^b) = g^{ab})],$$

where the probability is over randomly chosen a, b. We say that the mCDH assumption holds if ϵ is negligible for all adversaries $\mathcal{B}$.

2.5 The Hashed Modified Decision Bilinear Diffie-Hellman (HmDBDH) Assumption

The HmDBDH assumption first appeared in (Gagné et al. 2010) is inspired from the hashed Diffie-Hellman (HDH) problem by Abdalla et al. (Abdalla et al. 2001). The HDH problem states that it is hard to distinguish between the two distributions $\langle g, g^a, g^b, H(g^{ab})\rangle$ and $\langle g, g^a, g^b, R\rangle$, where a, b are random numbers between 1 and the size of the group, and R is a random element in the range of the hash function H.

The HmDBDH assumption is then obtained by directly applying the HDH problem to the modified decision bilinear Diffie-Hellman (mDBDH) problem by Kiltz & Vahlis (2008). As noted in the work of Abdalla et al. (2001), the HDH assumption is weaker than the DDH assumption and analogously, the HmDBDH assumption is weaker than the mDBDH assumption.

Moreover, we assume the existence of the hash function $H : \mathbb{G}_T \rightarrow \{0,1\}^n \times \mathbb{Z}_q^*$, where n denotes a bit-length. This can be realized by taking a cryptographic hash function $H' : \mathbb{G}_T \rightarrow \{0,1\}^n$ in conjunction with a pseudorandom number generator (PRNG). Then, the output of H' can be used as the seed to the PRNG. Note that our scheme requires $n = n_m + |g|$ which is may be larger than what is provided by a standard cryptographic hash function (eg. SHA-2 supports upto 512 bits). Skein (Ferguson et al. 2010), which is one of the finalists in the NIST hash function competition for the SHA-3 standard, supports arbitrary output size and can be useful for our purpose.

2.6 Target Collision Resistant Hash Function (TCR)

Let $\mathbb{M}$ and $\{0,1\}^n$ be finite sets where n is an integer and let $\mathbb{K}$ be a key space. Then, target collision resistant hash functions are a family of keyed hash functions $\{\mathsf{TCR}_K : \mathbb{M} \rightarrow \{0,1\}^n : K \in \mathbb{K}\}$. We say such hash functions are target collision resistant if any polynomial-time adversary $\mathcal{A}$ has only a negligible advantage in the following case: Given a message $M \in \mathbb{M}$, find another message $M' \in \mathbb{M}$ such that $(M' \neq M) \wedge (H_K(M') = H_K(M))$.

We define the advantage ϵ_{TCR} of $\mathcal{A}$ against TCR as

$$\epsilon_{\mathsf{TCR}} = \Pr[\mathcal{A} \text{ finds a collision in } \mathsf{TCR}].$$

Constructing target collision resistant hash functions is considered to be relatively easier than constructing collision resistant hash functions where an attacker is required to find any pair of messages M, M' such that $H_K(M) = H_K(M')$. Although we do not discuss here in detail, it has been shown that target collision resistant hash functions can be built from standard hash functions (Bellare & Rogaway 1997).

2.7 Attacks against IBSC schemes by Zhang and Jin et al.

In the following, we describe how the security of the IBSC schemes by Zhang (Zhang 2010) and Jin et al. (Jin et al. 2010) can be broken. For details of their scheme, please refer to their original papers.

2.7.1 Zhang's scheme

In Zhang's scheme, $\mathcal{A}$ is able to correctly distinguish which message has been encrypted as follows. In the security game, $\mathcal{A}$ submits two messages M_0, M_1. Then, $\mathcal{B}$ randomly chooses a bit b and encrypts M_{b} to generate the challenge ciphertext $\mathsf{CT}^* = \langle \mathsf{CT}_1^*, \mathsf{CT}_2^*, \mathsf{CT}_3^*, \mathsf{CT}_4^*, \mathsf{CT}_5^*, \mathsf{CT}_6^*\rangle$. $\mathcal{A}$ upon receiving CT^*, simply guesses $b = 0$ and computes $R'' = \mathsf{CT}_1/M_0$. Next, $\mathcal{A}$ further computes $t'' = \mathsf{TCR}(M_0 \parallel R'')$ and $m'' = H_2(g^{t''} h^{\mathsf{CT}_6^*})$. Then, $\mathcal{A}$ checks if $e(\mathsf{CT}_4^*, g) = e(g_1, g_2) e(H_u(\mathbf{u}), \mathsf{CT}_5^*) e(H_m(m''), \mathsf{CT}_2^*)$. If the verification succeeds, then the encrypted message was M_0, otherwise M_1.

The fundamental reason why Zhang's scheme is insecure is that the value of R, which is supposedly only computable by using the private key of the intended receiver, is trivially computable by $\mathcal{A}$. Once $\mathcal{A}$ obtains R, then $\mathcal{A}$ has all the necessary components to create a valid signature. Then, $\mathcal{A}$ can use its verification result to distinguish the correct message.

2.7.2 Jin et al.'s scheme

In Jin et al.'s scheme, $\mathcal{A}$ can break the IND-IBSC-CCA security of the scheme as follows. Let $\mathsf{CT}^* = \langle \mathsf{CT}_1^*, \mathsf{CT}_2^*, \mathsf{CT}_3^*, \mathsf{CT}_4^*, \mathsf{CT}_5^* \rangle$ be the challenge ciphertext created given by $\mathcal{B}$. Then, $\mathcal{A}$ successfully creates a forgery by choosing a random $r' \in \mathbb{Z}_q$ then computing $\mathsf{CT}' = \langle \mathsf{CT}'_1, \mathsf{CT}'_2, \mathsf{CT}'_3, \mathsf{CT}'_4 H_u(\mathbf{u})^{r'}, \mathsf{CT}'_5 g^{r'} \rangle$. Since $\mathsf{CT}' \neq \mathsf{CT}^*$, $\mathcal{A}$ may issue an **Unsigncrypt** query on CT' which will cause $\mathcal{A}$ to abnormally abort.

3 Our Scheme

We now describe our IBSC scheme in the standard model. The security of our scheme is based on the hardness of HmDBDH problem and mCDH problem. Note that n_m and n_u denote the maximum length of a plaintext and an identity respectively.

Setup$(1^{\mathcal{K}})$: Given $1^{\mathcal{K}}$ for a security parameter $\mathcal{K} \in \mathbb{Z}^+$, generates the system public key M_{pk} and the master key M_{sk} as follows:

1. Generate two groups $\mathbb{G}, \mathbb{G}_T$ of prime order q and a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$.
2. Choose a secret $s \in_R \mathbb{Z}_q$.
3. Choose three generators $g, g_2, h \in_R \mathbb{G}$
4. Compute $g_1 = g^s, Y = e(g_1, g_2)$.
5. Choose $u', u_1, ..., u_{n_u} \in_R \mathbb{G}$.
6. Choose $m', m_1, ..., m_{n_m} \in_R \mathbb{G}$.
7. Choose a cryptographic hash function which satisfies the HmDBDH assumption $H : \mathbb{G}_T \to \{0,1\}^{n_m + |g|} \times \mathbb{Z}_q^*$.
8. Choose a target collision resistant hash function $\mathsf{TCR} : \mathbb{G} \to \mathbb{Z}_q^*$

Finally, the master public key M_{pk} and the master secret key for the system are as follows

$$M_{pk} = \langle q, \mathbb{G}, \mathbb{G}_T, e, g, g_1, g_2, h, u', u_1, ..., u_{n_u}, m', m_1, ..., m_{n_m}, Y, H, \mathsf{TCR} \rangle$$
$$M_{sk} = \langle s \rangle$$

For notational convenience, we further define the following functions.

- Let $\mathcal{U} \subseteq \{1, ..., n_u\}$ denote the set of all i for which $\mathbf{u}[i] = 1$, where $\mathbf{u}[i]$ is the i-th bit of the identity string $\mathbf{u}$. Then, $H_u : \{0,1\}^{n_u} \to \mathbb{G}$ on $\mathbf{u}$ is computed as $H_u(\mathbf{u}) = u'^{t_1} \prod_{i \in \mathcal{U}} u_i^{t_1}$. For simplicity, we will denote the output of $H_u(\mathbf{u})$ as $g_{\mathbf{u}}$.
- Let $\mathcal{M} \subseteq \{1, ..., n_m\}$ denote the set of all j for which $M[j] = 1$, where $M[j]$ is the j-th bit of the Message M. Then, $H_m : \{0,1\}^{n_m} \to \mathbb{G}$ on M is computed as $H_m(M) = m' \prod_{j \in \mathcal{M}} m_j$. For simplicity, we will denote the output of $H_m(M)$ as g_M.

Extract(u): Given an identity $\mathbf{u}$, generates the corresponding private key $d_{\mathbf{u}}$ as follows:

1. Choose $r_{\mathbf{u}} \in_R \mathbb{Z}_q^*$.
2. $d_{\mathbf{u}} = \{d_{(\mathbf{u},0)} = g_2^s \cdot (g_{\mathbf{u}})^{r_{\mathbf{u}}},\ d_{(\mathbf{u},1)} = g^{r_{\mathbf{u}}}, d_{(\mathbf{u},2)} = h^{r_{\mathbf{u}}}\}$.

Signcrypt$(M, d_{\mathbf{u}_A}, \mathbf{u}_B)$**:** Given a message M, a sender's private key $d_{\mathbf{u}_A}$ and a receiver identity $\mathbf{u}_B$, outputs the signcryption CT as follows:

1. Choose $r, r' \in_R \mathbb{Z}_q^*$.
2. $(h_1, h_2) = H(Y^r)$.
3. $t' = \mathsf{TCR}(g^{r'})$.
4. $Z = g^{h_2} \cdot H_m(M \oplus t')^{r'} \cdot d_{(\mathbf{u}_A,0)}$.
5. $t = \mathsf{TCR}(g^r)$.
6. $\mathsf{CT} = \langle g^r, g^{r'}, (g_{\mathbf{u}_B} \cdot h^t)^r, (M \parallel Z) \oplus h_1, d_{(\mathbf{u}_A,1)} \rangle$

Unsigncrypt$(\mathsf{CT}, \mathbf{u}_A, d_{\mathbf{u}_B})$**:** Given a ciphertext $\mathsf{CT} = \langle \mathsf{CT}_1, \mathsf{CT}_2, \mathsf{CT}_3, \mathsf{CT}_4, \mathsf{CT}_5 \rangle$, a sender identity $\mathbf{u}_A$ and a receiver's private key $d_{\mathbf{u}_B}$, unsigncrypts as follows:

1. $t = \mathsf{TCR}(\mathsf{CT}_1)$.
2. $Y = \frac{e\left(\mathsf{CT}_1, d_{(\mathbf{u}_B,0)} \cdot (d_{(\mathbf{u}_B,2)})^t\right)}{e\left(\mathsf{CT}_3, d_{(\mathbf{u}_B,1)}\right)}$
   $= \frac{e\left(g^r, g_2^s \cdot g_{\mathbf{u}_B}^{r_{\mathbf{u}_B}} \cdot h^{r_{\mathbf{u}_B} t}\right)}{e\left((g_{\mathbf{u}_B} \cdot h^t)^r, g^{r_{\mathbf{u}_B}}\right)}$
   $= e(g^r, g_2^s)$.
3. $(h_1, h_2) = H(Y)$.
4. $(M \parallel Z) = \mathsf{CT}_4 \oplus h_1$.
5. $Z' = Z \cdot g^{-h_2}$.
6. $t' = \mathsf{TCR}(\mathsf{CT}_2)$.
7. Test if $e(Z', g) = Y \cdot e(\mathsf{CT}_2, H_m(M \oplus t')) \cdot e(\mathsf{CT}_5, g_{\mathbf{u}_A})$ and if it holds, output the message M, otherwise $\perp$.

4 Security Proof

In this section we prove the security of our scheme using a series of games. More precisely, we have two sequences of games Game 0 to Game 8 and Game′ 0 to Game′ 8, where we prove confidentiality and unforgeability respectively. Each game (eg. Game 0, Game 1, etc) played is complete in the sense that an adversary will interact with a simulator from Setup phase to Guess phase as defined in the security model. For conciseness however, we will only describe the new changes made in each game. We define $\mathcal{E}_i, \mathcal{E}'_i$ to be the events that $\mathcal{B}$ outputs its guess $\beta' = 1$, in the respective i-th games.

Theorem 4.1. *If there exists a polynomial-time IND-IBSC-CCA2 adversary $\mathcal{A}$ against our scheme, then there exists an algorithm $\mathcal{B}$ which can break the HmDBDH assumption. Specifically, for an adversary $\mathcal{A}$ with an advantage ϵ and running time t which may issue at most Q_E* **Extract** *queries, $\mathcal{B}$ has an advantage of at least ϵ_{HmDBDH} in solving a HmDBDH problem in time at most t'.*

$$\epsilon_{HmDBDH} \geq \frac{\epsilon - \epsilon_{\mathsf{TCR}}}{8Q_E(n_u + 1)},$$
$$t' \leq t + O(\epsilon^{-2} ln(\epsilon^{-1}) \lambda^{-1} ln(\lambda)^{-1}))$$

Proof. The theorem is proved via a series of games from Game 0 to Game 8. To start with, Game 0 where the scheme is simulated exactly as described in Section 3 is presented. Then we transit through the subsequent games based on various events (eg. simulation abort, hash collision, etc). We conclude the proof with the overall probability calculation of the advantage and the running time of our simulation.

Recall that the HmDBDH problem is to distinguish between two probability distributions $\langle g, g^a, g^{a^2}, g^b, g^c, H(e(g,g)^{abc})\rangle \in \mathbb{G}^5 \times \{0,1\}^{n_m+|g|} \times \mathbb{Z}_q^*$ and $\langle g, g^a, g^{a^2}, g^b, g^c, R\rangle \in \mathbb{G}^5 \times \{0,1\}^{n_m+|g|} \times \mathbb{Z}_q^*$. We assume that the secrets a, b, c are known to $\mathcal{B}$ initially. Then, in sequel games, $\mathcal{B}$ will gradually forget the secrets and instead they are available in the forms of g^a, g^{a^2}, g^b, g^c only.

Game 0

Let $\mathcal{A}$ be an adversary and $\mathcal{B}$ be a simulator. We define Game 0 to be an interactive game between $\mathcal{A}$ and $\mathcal{B}$. In short, $\mathcal{B}$ will behave as a KGC in our scheme described in Section 3. Thus $\mathcal{B}$ has no limitation in serving the queries made by $\mathcal{A}$ in Game 0 since it knows the secret exponents a, b, c explicitly. Let $\mathcal{E}_0$ be the event that $\mathsf{b} = \mathsf{b}'$. Then, by definition $\mathcal{A}$'s advantage in Game 0 is $|\Pr[\mathcal{E}_0] - \frac{1}{2}|$.

Game 1 [Transition based on hash collisions]

In Game 1, the simulation is performed identically to Game 0 except for the case when a hash collision occurs. We say that a hash collision has occurred when $(\mathsf{CT}_1 \neq g^c) \wedge (\mathsf{TCR}(\mathsf{CT}_1) = t^*))$. We define $HASHABORT$ to be the event that the simulator aborts due to a hash collision. The simulation environment remains indistinguishable from the view of $\mathcal{A}$ until $HASHABORT$ occurs. Thus due to the difference lemma (Shoup 2004) we have,

$$|\Pr[\mathcal{E}_0] - \Pr[\mathcal{E}_1]| \leq \Pr[HASHABORT] \quad (1)$$

Also, we have an adversary against TCR which succeeds with probability of at least $\Pr[HASHABORT]$. Then,

$$\Pr[HASHABORT] \leq \epsilon_{\mathsf{TCR}} \quad (2)$$

Game 2 [Transition based on change in the system public key 1]

In Game 2, $\mathcal{B}$ modifies the system public key M_{pk} as follows.

Setup: $\mathcal{B}$ sets an integer, $m = 4Q_E$, where Q_E is the number of extract queries, and chooses an integer, k_u, uniformly at random between 0 and n_u. $\mathcal{B}$ defines $x', \vec{x}, y', \vec{y} \in_R \mathbb{Z}_m^*$, three functions $F_u(\mathbf{u}) = (q - mk_u) + x' + \sum_{i\in\mathcal{U}} x_i \pmod q, J_u(\mathbf{u}) = y' + \sum_{i\in\mathcal{U}} y_i \pmod q, K_u(\mathbf{u}) = 0$, if $x' + \sum_{i\in\mathcal{U}} x_i \equiv 0 \pmod m$, otherwise 1.

$\mathcal{B}$ sets $h = g_1 \cdot g^\alpha$, where $\alpha \in_R \mathbb{Z}_q^*$. $\mathcal{B}$ then assigns $u' = g_2^{q-k_u m+x'} \cdot g^{y'} \cdot g_1^{-t^*}$, where $t^* = \mathsf{TCR}(g^c)$ and $u_i = g_2^{x_i} \cdot g^{y_i}$. Finally, $\mathcal{B}$ replaces the parts of the system public key M_{pk} with newly computed $\langle u', u_1, ..., u_{n_u}, m', m_1, ..., m_{n_m}\rangle$ and keeps the functions $F_u, J_u, K_u, F_m, J_m, K_m$ internal to itself.

$\mathcal{B}$ further chooses k_m randomly between 0 and n_m and defines $m' = g_2^{q-k_m m+v'} \cdot g^{w'}$, $m_i = g_2^{v_i} \cdot g^{w_i}$, where $v', \vec{v}, w', \vec{w} \in_R \mathbb{Z}_m^*$. Further $\mathcal{B}$ defines three functions $F_m(M) = (q - mk_m) + v' + \sum_{i\in\mathcal{M}} v_i \pmod q, J_m(M) = w' + \sum_{i\in\mathcal{M}} w_i \pmod q, K_m(M) = 0$, if $v' + \sum_{i\in\mathcal{M}} v_i \equiv 0 \pmod m$ otherwise 1.

The changes made in M_{pk} as above does not affect the view of $\mathcal{A}$ and hence the simulation remains indistinguishable from Game 1. Therefore,

$$\Pr[\mathcal{E}_1] = \Pr[\mathcal{E}_2] \quad (3)$$

Game 3 [Transition based on simulation abort]

Let Q_E be the maximum number of Extract queries $\mathcal{A}$ may issue. Further, let F_1 denote the event that $\mathcal{A}$ issues an Extract query on an identity $\mathbf{u}$ such that $K_u(\mathbf{u}) = 0$ and let F_2 denote the event that $\mathcal{A}$ chooses the challenge identity $\mathbf{u}_B^*$ such that $F_u(\mathbf{u}_B^*) \neq 0$. Then, we define the event forced abort $F_{for} : F_1 \vee F_2$ and

$$\Pr[\neg F_{for}] = \Pr\left[\bigwedge_{i=1}^{Q_E} K_u(\mathbf{u}_i) = 1\right] \cdot \Pr\left[F_u(\mathbf{u}_B^*) = 0 \,\middle|\, \bigwedge_{i=1}^{Q_E} K_u(\mathbf{u}_i) = 1\right]$$

We also define $\eta = \Pr[\neg F_{for}]$ and put λ as a lower bound on η.

Lemma 4.2. *The probability of simulator not aborting by the guess phase is at least* $\lambda = \frac{1}{8(n_u+1)Q_E}$.

The proof of this lemma is postponed until Section 4.1.

As discussed by Waters (2006), artificial abort, denoted as F_{art}, is required to ensure that the simulation abort occurs with almost same probability $(1 - \lambda)$ over all possible sets of Extract queries made by $\mathcal{A}$. Let $\vec{\mathbf{u}} = \mathbf{u}_1, ..., \mathbf{u}_{Q_E}$ be the set of identities queried for Extract during Phase 1 and Phase 2. We define the function $\tau(X', \vec{\mathbf{u}}, \mathbf{u}^*)$, where X' is a set of simulation values $x', x_1, ..., x_{n_u}$, as $\tau(X', \vec{\mathbf{u}}, \mathbf{u}^*) = 0$, if $\neg F$, otherwise 1. We consider the probability over the simulation values for a given set of queries, $\vec{\mathbf{u}}, \mathbf{u}^*$, as $\eta = \Pr_{X'}[\tau(X', \vec{\mathbf{u}}, \mathbf{u}^*) = 0]$. $\mathcal{B}$ estimates η' by sampling $O(\epsilon^{-2}\ln(\epsilon^{-1})\lambda^{-1}\ln(\lambda)^{-1}))$ times the probability η by choosing a random X'. Then, if $\eta' \geq \lambda$, $\mathcal{B}$ will abort with probability $\frac{\eta'-\lambda}{\eta'}$ and take a random guess. Otherwise, $\mathcal{B}$ will continue to Guess phase as usual. Note that fixing $X', \vec{\mathbf{u}}, \mathbf{u}^*$ gives the adversary the fixed view of the simulation.

Lemma 4.3. *If the simulator takes* $O(\epsilon^{-2}ln(\epsilon^{-1})\lambda^{-1}ln(\lambda^{-1}))$ *samples when computing the estimate* η'*, then*

$$\left|\frac{Pr[\mathcal{E}_2] - \frac{1}{2}}{\lambda} - Pr[\mathcal{E}_3] - \frac{1}{2}\right| \leq \frac{\epsilon}{2}$$

The proof of the above lemma is postponed until Section 4.2. Note that readers who are familiar with the work by Kiltz & Galindo (2009) may skip this proof as this is identical to the proof of Lemma A.3 in their work.

Game 4 [Transition based on private key derivation]

$\mathcal{B}$ answers private key queries made by $\mathcal{A}$ as follows.

Extract Queries: Given an identity $\mathbf{u}$, $\mathcal{B}$ chooses $r_{\mathbf{u}} \in_R \mathbb{Z}_q^*$ and computes $d_{\mathbf{u}}$ as follows :

$$d_{\mathbf{u}} = \Big\{ d_{(\mathbf{u},0)} = g_1^{\frac{-J_u(\mathbf{u})}{F_u(\mathbf{u})}} \cdot g_{\mathbf{u}}^{r_{\mathbf{u}}}, d_{(\mathbf{u},1)} = g_1^{\frac{-1}{F(\mathbf{u})}} \cdot g^{r_{\mathbf{u}}},$$
$$d_{(\mathbf{u},2)} = (A_2 \cdot g_1^{\alpha})^{\frac{-1}{F_u(\mathbf{u})}} \cdot (g_1 \cdot g^{\alpha})^{r_{\mathbf{u}}} \Big\}.$$

Letting $\tilde{r}_{\mathbf{u}} = r_{\mathbf{u}} - \frac{a}{F_u(\mathbf{u})}$ gives us

$$\begin{aligned}
d_{(\mathbf{u},0)} =& g_1^{\frac{-J_u(\mathbf{u})}{F_u(\mathbf{u})}} \cdot A_2^{\frac{t^*}{F_u(\mathbf{u})}} \cdot g_{\mathbf{u}}^{r_{\mathbf{u}}} \\
=& g_1^{\frac{-J_u(\mathbf{u})}{F_u(\mathbf{u})}} \cdot g_1^{\frac{at^*}{F_u(\mathbf{u})}} \cdot \left(g_2^{F_u(\mathbf{u})} \cdot g^{J_u(\mathbf{u})} \cdot g_1^{-t^*} \right)^{r_{\mathbf{u}}} \\
=& g_2^a \cdot \left(g_2^{F_u(\mathbf{u})} \cdot g^{J_u(\mathbf{u})} \cdot g_1^{-t^*} \right)^{-\frac{a}{F_u(\mathbf{u})}} \\
& \cdot \left(g_2^{F_u(\mathbf{u})} \cdot g^{J_u(\mathbf{u})} \cdot g_1^{-t^*} \right)^{r_{\mathbf{u}}} \\
=& g_2^a \cdot g_{\mathbf{u}}^{r_{\mathbf{u}} - \frac{a}{F_u(\mathbf{u})}} \\
=& g_2^a \cdot g_{\mathbf{u}}^{\tilde{r}_{\mathbf{u}}}, \\
d_{(\mathbf{u},1)} =& g_1^{\frac{-1}{F_u(\mathbf{u})}} \cdot g^{r_{\mathbf{u}}} = g^{r_{\mathbf{u}} - \frac{a}{F_u(\mathbf{u})}} = g^{\tilde{r}_{\mathbf{u}}}, \\
d_{(\mathbf{u},2)} =& (A_2 \cdot g_1^{\alpha})^{\frac{-1}{F_u(\mathbf{u})}} \cdot (g_1 \cdot g^{\alpha})^{r_{\mathbf{u}}} \\
=& (g_1 \cdot g^{\alpha})^{\frac{-a}{F_u(\mathbf{u})}} \cdot (g_1 \cdot g^{\alpha})^{r_{\mathbf{u}}} \\
=& (g_1 \cdot g^{\alpha})^{r_{\mathbf{u}} - \frac{a}{F_u(\mathbf{u})}} \\
=& h^{\tilde{r}_{\mathbf{u}}}.
\end{aligned}$$

$\mathcal{B}$ can perform this computation if and only if $F_u(\mathbf{u}) \neq 0$. Since we choose q, m, k_u such that $q \gg mk_u$, the only condition that $F_u(\mathbf{u}) = 0$ can occur is when $mk_u = x' + \vec{x}$. Notice that $K_u(\mathbf{u}) \neq 0$ is the sufficient condition for $F_u(\mathbf{u}) \neq 0$, since $K_u(\mathbf{u}) \neq 0$ implies $mk_u \neq x' + \vec{x}$. Thus the simulator will only continue when $K_u(\mathbf{u}) \neq 0$.

Game 4 remains indistinguishable from Game 3 and hence,

$$\Pr[\mathcal{E}_3] = \Pr[\mathcal{E}_4] \tag{4}$$

Game 5 [Transition based on Signcrypt/Unsigncrypt computation]

In this game, $\mathcal{B}$ answers **Signcrypt/Unsigncrypt** queries made by $\mathcal{A}$ as follows. Note that $\mathcal{B}$ is able to answer the queries without the explicit knowledge of $a, b \in \mathbb{Z}_q^*$.

Signcrypt queries on $(\mathbf{u}_A, \mathbf{u}_B, M)$**:** There are two cases:

$K_u(\mathbf{u}_A) \neq 0$**:** $\mathcal{B}$ runs **Extract**$(\mathbf{u}_A)$ to generate the private key for $\mathbf{u}_A$ and signcrypts M as usual.

Otherwise: $\mathcal{B}$ signcrypts M as follows :

1. Choose $r, r'r'' \in_R \mathbb{Z}_q^*$.
2. $(h_1, h_2) = H(Y^r)$.
3. $t' = \mathsf{TCR}(g^{r'})$.
4. Repick r' and restart from Step 3 until $K_m(M') \neq 0$, where $M' = M \oplus t'$.
5. Computes the signature Z as follows:

$$\begin{aligned}
Z =& g^{h_2} \cdot g_1^{\frac{-J_m(M')}{F_m(M')}} \cdot \left(g_2^{F_m(M')} \cdot g^{J_m(M')} \right)^{r'} \\
& \cdot \left(g^{J_u(\mathbf{u}_A)} \cdot g_1^{-t^*} \right)^{r''} \\
=& g^{h_2} \cdot g_2^a \cdot \left(g_2^{F_m(M')} \cdot g^{J_m(M')} \right)^{\frac{-a}{F_m(M')}} \\
& \cdot \left(g_2^{F_m(M')} \cdot g^{J_m(M')} \right)^{r'} \cdot \left(g^{J_u(\mathbf{u}_A)} \cdot g_1^{-t^*} \right)^{r''} \\
=& g^{h_2} \cdot g_2^a \cdot \left(g_2^{F_m(M')} \cdot g^{J_m(M')} \right)^{r' - \frac{a}{F_m(M')}} \\
& \cdot \left(g^{J_u(\mathbf{u}_A)} \cdot g_1^{-t^*} \right)^{r''} \\
=& g^{h_2} \cdot g_2^a \cdot H_m(M')^{\tilde{r}} \cdot \left(g^{J_u(\mathbf{u}_A)} \cdot g_1^{-t^*} \right)^{r''}, \\
& \text{where } \tilde{r} = r' - \frac{a}{F_m(M')}.
\end{aligned}$$

$g^{\tilde{r}}$ is computed as follows:

$$g_1^{\frac{-1}{F_m(M')}} \cdot g^{r'} = g^{\frac{-a}{F_m(M')}} \cdot g^{r'} = g^{r' - \frac{a}{F_m(M')}} = g^{\tilde{r}}.$$

6. $t = \mathsf{TCR}(g^r)$.
7. $\mathsf{CT} = \langle g^r, g^{\tilde{r}_{M'}}, (g_{\mathbf{u}_B} \cdot h^t)^r, M \oplus h_1, Z, g^{r''} \rangle$

Remark 4.4. $g^{r''}$ must be fixed for each identity since it corresponds to a part of a user's private key in the actual scheme.

Unsigncrypt queries on $(\mathbf{u}_B, \mathsf{CT} = \langle \mathsf{CT}_1, ..., \mathsf{CT}_6 \rangle)$**:** There are three cases:

$(\mathsf{CT}_1 \neq \mathsf{CT}_1^* = C^{t_3}) \wedge (\mathsf{TCR}(\mathsf{CT}_1) = \mathsf{TCR}(C))$**:** $\mathcal{B}$ aborts due a hash collision. Note that we have bounded the probability of this abort in Game 1.

$K(\mathbf{u}_B) \neq 0$**:** Runs **Extract**$(\mathbf{u}_B)$ and unsigncrypts CT' as usual.

Otherwise: $\mathcal{B}$ unsigncrypts as follows:

1. Computes Y as follows:

$$\begin{aligned}
Y =& e\left(\frac{\mathsf{CT}_3}{\mathsf{CT}_1^{J_u(\mathbf{u}_B)} \cdot \mathsf{CT}_1^{\alpha t}}, g_2 \right)^{(t-t^*)^{-1}} \\
=& e\left(\frac{\left(g_1^{-t^*} \cdot g^{J_u(\mathbf{u}_B)} \right)^r \cdot h^{tr}}{g^{rJ_u(\mathbf{u}_B)} \cdot g^{r\alpha t}}, g_2 \right)^{(t-t^*)^{-1}} \\
=& e\left(\frac{g_1^{-t^* r} \cdot g^{J_u(\mathbf{u}_B) r} \cdot g_1^{tr} \cdot g^{\alpha t r}}{g^{rJ_u(\mathbf{u}_B)} \cdot g^{r\alpha t}}, g_2 \right)^{(t-t^*)^{-1}} \\
=& e\left(g_1^{-t^* r} \cdot g_1^{tr} \right)^{(t-t^*)^{-1}} = e\left(g_1^r, g_2 \right)
\end{aligned}$$

2. $(h_1, h_2) = H(Y)$.
3. $Z = \mathsf{CT}_5 \cdot g^{-h_2}$.
4. $M = \mathsf{CT}_4 \oplus h_1$.
5. $t' = \mathsf{TCR}(\mathsf{CT}_2)$.
6. Test if $e(g, Z) = Y \cdot e(\mathsf{CT}_2, H_m(M \oplus t')) \cdot e(g_{\mathbf{u}_A}, \mathsf{CT}_6)$ and if it holds, outputs the message M, otherwise $\perp$.

Remark 4.5. The importance of the simulator being able to answer signcrypt/unsigncrypt queries when $F_u(\mathbf{u}) = 0$ has been overlooked in many previous attempts (Jin et al. 2010, Yu et al. 2009, Zhang 2010). For a security reduction to go through, given the challenge identity $\mathbf{u}_B^*$ it is required that $F_u(\mathbf{u}_B^*) = 0$. However, the simulators in the mentioned papers are not able to answer any sigincrypt/unsigncrypt queries involving $\mathbf{u}_B^*$ and simply abort when such cases occur. This behaviour of the simulator clearly enables an attacker to distinguish the simulated environment from the real environment.

Game 5 remains indistinguishable from Game 4 and hence,

$$\Pr[\mathcal{E}_4] = \Pr[\mathcal{E}_5] \tag{5}$$

Game 6 [Transition based on change in the system public key 2]

We now assume that $a, b \in \mathbb{Z}_q^*$ are no longer available to the simulator $\mathcal{B}$ as plain integers. Instead, they are available in the form of $A_1 = g^a, A_2 = g^{a^2}, B = g^b$.

Setup: $\mathcal{B}$ sets $g_1 = A_1, g_2 = B$ and $Y = e(g_1, g_2)$. Then, $\mathcal{B}$ replaces the parts of the system public key M_{pk} with newly computed $\langle g_1, g_2, Y\rangle$.

The changes made in M_{pk} as above does not affect the view of $\mathcal{A}$. Therefore,

$$\Pr[\mathcal{E}_5] = \Pr[\mathcal{E}_6] \tag{6}$$

Game 7 [Transition based on challenge ciphertext computation]

We now assume that $c \in \mathbb{Z}_q^*$ is no longer available to the simulator $\mathcal{B}$ as a plain integer. Instead, it is available in the form of $C = g^c$, in addition to $(z_1, z_2) = H(e(g,g)^{abc})$. Then, we show how $\mathcal{B}$ constructs the challenge ciphertext as follows.

Challenge: $\mathcal{A}$ commits the challenge identities $(\mathbf{u}_A, \mathbf{u}_B^*)$ and a message M. If $(F_u(\mathbf{u}_B^*) \neq 0)$ then $\mathcal{B}$ aborts and outputs a random guess as the solution. Else, $\mathcal{B}$ returns the challenge ciphertext CT^* as:

$$r' \in_R \mathbb{Z}_q^*,$$
$$t' = \mathsf{TCR}(g^{r'}),$$
$$Z = g^{z_2} \cdot H_m(M_\mathsf{b} \oplus t')^{r'} \cdot d_{(\mathbf{u}_A,0)},$$
$$\mathsf{CT}^* = \Big\langle C, g^{r'}, \Big(g^{J_u(\mathbf{u}_B^*)} \cdot g_1^{-t^*} \cdot h^{t^*}\Big)^c, M_\mathsf{b} \oplus z_1, Z, d_{(\mathbf{u}_A,1)}\Big\rangle.$$

Note that we can compute $\mathsf{CT}_3 = \Big(g^{J_u(\mathbf{u}_B^*)} \cdot g_1^{-t^*} \cdot h^{t^*}\Big)^c$ since $\mathsf{CT}_3 = \Big(g^{J_u(\mathbf{u}_B^*)} \cdot g_1^{-t^*} \cdot g_1^{t^*} \cdot g^{\alpha t^*}\Big)^c = \big(g^{J_u(\mathbf{u}_B^*)} \cdot g^{\alpha t^*}\big)^c$. $d_{(\mathbf{u}_A,0)}$ and $d_{(\mathbf{u}_A,1)}$ are obtained by running **Extract**$(\mathbf{u}_A)$ assuming that $F_u(\mathbf{u}_A) \neq 0$. Otherwise, we can use the same technique as how we answer **Signcrypt** queries in Game 5.

Game 7 remains indistinguishable from Game 6 and hence,

$$\Pr[\mathcal{E}_6] = \Pr[\mathcal{E}_7] \tag{7}$$

Game 8 [Transition based on challenge ciphertext replacement]

$\mathcal{B}$ simply replaces CT_4^* and CT_5^* with random bit strings. Thus we have,

$$\Pr[\mathcal{E}_8] = \frac{1}{2} \tag{8}$$

The only difference between Game 7 and Game 8 is the computation of $\mathsf{CT}_4^*, \mathsf{CT}_5^*$. It is easy to see that this is equivalent to distinguishing between a well formed HmDBDH instance and a random instance. Hence,

$$|\Pr[\mathcal{E}_7] - \Pr[\mathcal{E}_8]| \leq \epsilon_{HmDBDH} \tag{9}$$

Analysis

We have computed partial probabilities of indistinguishability between games. We now combine the these probabilities to compute the overall advantage ϵ of an adversary $\mathcal{A}$ running in time t, which is at most,

$$\epsilon = \left|\Pr[\mathcal{E}_0] - \frac{1}{2}\right| \text{(by definition)} \tag{10}$$
$$\leq \left|\Pr[\mathcal{E}_1] + \epsilon_{\mathsf{TCR}} - \frac{1}{2}\right| \text{(from equations 1, 2)} \tag{11}$$
$$= \left|\Pr[\mathcal{E}_2] + \epsilon_{\mathsf{TCR}} - \frac{1}{2}\right| \text{(from equation 3)} \tag{12}$$
$$\leq \left|\frac{\Pr[\mathcal{E}_3] - \frac{1}{2}}{\lambda} + \epsilon_{\mathsf{TCR}}\right| \text{(from Lemma 4.3)} \tag{13}$$
$$= \left|\frac{\Pr[\mathcal{E}_4] - \frac{1}{2}}{\lambda} + \epsilon_{\mathsf{TCR}}\right| \text{(from equation 4)} \tag{14}$$
$$= \left|\frac{\Pr[\mathcal{E}_5] - \frac{1}{2}}{\lambda} + \epsilon_{\mathsf{TCR}}\right| \text{(from equation 5)} \tag{15}$$
$$= \left|\frac{\Pr[\mathcal{E}_6] - \frac{1}{2}}{\lambda} + \epsilon_{\mathsf{TCR}}\right| \text{(from equation 6)} \tag{16}$$
$$= \left|\frac{\Pr[\mathcal{E}_7] - \frac{1}{2}}{\lambda} + \epsilon_{\mathsf{TCR}}\right| \text{(from equation 7)} \tag{17}$$
$$\leq \left|\frac{\Pr[\mathcal{E}_8] + \epsilon_{HmDBDH} - \frac{1}{2}}{\lambda} + \epsilon_{\mathsf{TCR}}\right| \text{(from equation 9)} \tag{18}$$
$$= \left|\frac{\epsilon_{HmDBDH}}{\lambda} + \epsilon_{\mathsf{TCR}}\right| \text{(from equation 8)} \tag{19}$$
$$= \left|\frac{\epsilon_{HmDBDH}}{\frac{1}{8Q_E(n_u+1)}} + \epsilon_{\mathsf{TCR}}\right| \text{(from Lemma 4.2)} \tag{20}$$
$$= |8Q_E(n_u+1)\,(\epsilon_{HmDBDH}) + \epsilon_{\mathsf{TCR}}| \tag{21}$$

Since ϵ_{HmDBDH} and ϵ_{TCR} are negligible, $\mathcal{A}$ has only negligible advantage in breaking our scheme.

The running time t' of $\mathcal{B}$ is linear in the running time of $\mathcal{A}$. Moreover, $\mathcal{B}$ requires additional running time for sampling. Hence, $t' = t + O(\epsilon^{-2}\ln(\epsilon^{-1})\lambda^{-1}\ln(\lambda)^{-1}))$. This completes the proof for the IND-IBSC-CCA2 security of our scheme. □

4.1 Proof of Lemma 4.2

Proof. We now show the lower bound on the probability of the simulation not aborting.

$$\Pr[\neg F] = \Pr[\bigwedge_{i=1}^{Q_E} K_u(\mathbf{u}_i) = 1] \cdot \Pr[F_u(\mathbf{u}_B^*) = 0 | \bigwedge_{i=1}^{Q_E} K_u(\mathbf{u}_i) = 1] \quad (22)$$

$$= (1 - \Pr[\bigvee_{i=1}^{Q_E} K_u(\mathbf{u}_i) = 0]) \cdot \Pr[F_u(\mathbf{u}_B^*) = 0 | \bigwedge_{i=1}^{Q_E} K_u(\mathbf{u}_i) = 1] \quad (23)$$

$$= (1 - \sum_{i=1}^{Q_E} \Pr[K_u(\mathbf{u}_i) = 0]) \cdot \Pr[F_u(\mathbf{u}_B^*) = 0 | \bigwedge_{i=1}^{Q_E} K_u(\mathbf{u}_i) = 1] \quad (24)$$

$$= (1 - \frac{Q_E}{m}) \cdot \Pr[F_u(\mathbf{u}_B^*) = 0 | \bigwedge_{i=1}^{Q_E} K_u(\mathbf{u}_i) = 1] \quad (25)$$

$$= (1 - \frac{Q_E}{m}) \cdot \frac{1}{n_u + 1} \cdot \Pr[K_u(\mathbf{u}_B^*) = 0 | \bigwedge_{i=1}^{Q_E} K_u(\mathbf{u}^*) = 1] \quad (26)$$

$$= (1 - \frac{Q_E}{m}) \cdot \frac{1}{n_u + 1} \cdot \frac{\Pr[K_u(\mathbf{u}^*) = 0]}{\Pr[\bigwedge_{i=1}^{Q_E} K_u(\mathbf{u}_i) = 1]} \cdot \Pr[\bigwedge_{i=1}^{Q_E} K_u(\mathbf{u}_i) = 1 | K_u(\mathbf{u}^*) = 0] \quad (27)$$

$$\geq (1 - \frac{Q_E}{m}) \cdot \frac{1}{(n_u + 1)} \cdot \frac{1}{m} \cdot \Pr[\bigwedge_{i=1}^{Q_E} K_u(\mathbf{u}_i) = 1 | K_u(\mathbf{u}^*) = 0] \quad (28)$$

$$= (1 - \frac{Q_E}{m}) \cdot \frac{1}{(n_u + 1)m} \cdot (1 - \Pr[\bigvee_{i=1}^{Q_E} K_u(\mathbf{u}_i) = 0 | K_u(\mathbf{u}^*) = 0]) \quad (29)$$

$$\geq (1 - \frac{Q_E}{m}) \cdot \frac{1}{(n_u + 1)m} \cdot (1 - \sum_{i=1}^{Q_E} \Pr[K_u(\mathbf{u}_i) = 0 | K_u(\mathbf{u}^*) = 0]) \quad (30)$$

$$= (1 - \frac{Q_E}{m})^2 \cdot \frac{1}{(n_u + 1)m} \quad (31)$$

$$\geq (1 - \frac{2Q_E}{m}) \cdot \frac{1}{(n_u + 1)m} \quad (32)$$

$$= (1 - \frac{2Q_E}{4Q_E}) \cdot \frac{1}{(n_u + 1)4Q_E} \quad (33)$$

$$= \frac{1}{(n_u + 1)8Q_E} \quad (34)$$

Equations 24 and 30 come from the fact that for any pair of $\mathbf{u}$ and $\mathbf{u}'$, the probabilities that $K_u(\mathbf{u}) = 0$ and $K_u(\mathbf{u}')$ are independent. Equations 25 and 28 come from the probability of $K_u(\mathbf{u}) = 0$ being $\frac{1}{m}$ for any $\mathbf{u}$. Equation 26 hold since $F_u(\mathbf{u}) = 0$ implies $K_u(\mathbf{u}) = 0$ as well as the existence of a unique k_u such that $0 \leq k_u \leq n_u$. Finally, equation 33 is obtained by setting $m = 4Q_E$ which optimizes the equation. □

4.2 Proof of Lemma 4.3

Proof. We first compute the probability distribution of $\Pr[\mathcal{E}_3] - \frac{1}{2}$ as follows.

$$\Pr[\mathcal{E}_3] - \frac{1}{2} = \Pr[\beta' = 1|F]\Pr[F] + \Pr[\beta' = 1|\neg F]\Pr[\neg F] - \frac{1}{2} \quad (35)$$

$$= \frac{1}{2}\Pr[F] + \Pr[\beta' = 1|\neg F]\Pr[\neg F] - \frac{1}{2} \quad \text{(random guess taken if } F \text{ occurs)} \quad (36)$$

$$= \frac{1}{2}\Pr[F] + \Pr[\mathsf{b}' = \mathsf{b}|\neg F]\Pr[\neg F] - \frac{1}{2} \quad (\beta' = 1 \text{ if } \mathsf{b}' = \mathsf{b}) \quad (37)$$

$$= \frac{1}{2}(1 - \Pr[\neg F]) + \Pr[\mathsf{b}' = \mathsf{b}|\neg F]\Pr[\neg F] - \frac{1}{2} \quad (38)$$

$$= -\frac{1}{2}\Pr[\neg F]) + \Pr[\mathsf{b}' = \mathsf{b}|\neg F]\Pr[\neg F] \quad (39)$$

$$= -\frac{1}{2}\Pr[\neg F]) + \Pr[\neg F|\mathsf{b}' = \mathsf{b}]\Pr[\mathsf{b}' = \mathsf{b}] \quad \text{(Bayes' theorem)} \quad (40)$$

$$= \frac{1}{2}(\Pr[\neg F|\mathsf{b}' = \mathsf{b}]\Pr[\mathsf{b}' = \mathsf{b}] - \Pr[\neg F|\mathsf{b}' \neq \mathsf{b}]\Pr[\mathsf{b}' \neq \mathsf{b}]) \quad (41)$$

$$= \frac{1}{2}(\Pr[\neg F|\mathsf{b}' = \mathsf{b}]\Pr[\mathcal{E}_2] - \Pr[\neg F|\mathsf{b}' \neq \mathsf{b}](1 - \Pr[\mathcal{E}_2])) \quad (\Pr[\mathcal{E}_2] = \Pr[\mathsf{b}' = \mathsf{b}]) \quad (42)$$

Let F be the event such that $F : F_{art} \vee F_{for}$. Then we make the following claim.

Claim 4.6. *For any fixed view of $\mathcal{A}$, $|Pr[\neg F] - \lambda| \leq \frac{\lambda\epsilon}{4}$.*

Let us assume the claim holds for now. Since the claim holds for any fixed view of $\mathcal{A}$, the claim should also hold in the following cases conditioned on $\mathsf{b}' = \mathsf{b}$ and $\mathsf{b}' \neq \mathsf{b}$.

$$|\Pr[\neg F|\mathsf{b}' = \mathsf{b}] - \lambda| \leq \frac{\lambda\epsilon}{4}, |\Pr[\neg F|\mathsf{b}' \neq \mathsf{b}] - \lambda| \leq \frac{\lambda\epsilon}{4} \quad (43)$$

Then, combining equations 42 and 43 gives,

$$\left|\Pr[\mathcal{E}_3] - \frac{1}{2} - \lambda\left(\Pr[\mathcal{E}_2] - \frac{1}{2}\right)\right| \leq \Pr[\mathcal{E}_2]\frac{\lambda\epsilon}{4} + \frac{\lambda\epsilon}{4} \leq \frac{\lambda\epsilon}{2},$$

which trivially leads to

$$\left|\frac{\Pr[\mathcal{E}_3]-\frac{1}{2}}{\lambda}-\left(\Pr[\mathcal{E}_2]-\frac{1}{2}\right)\right|\leq\frac{\epsilon}{2}\ \square$$

Proof of Claim 4.6

Proof. Since two events are independent of each other,

$$\Pr[\neg F]=\Pr[\neg F_{for}]\Pr[\neg F_{art}]=\eta\Pr[\neg F_{art}]$$

Let us fix $0<\epsilon'=\frac{\epsilon}{8}\leq\frac{1}{8}$. Then, by using Chernoff's bound for the estimate η' of η we obtain

$$\Pr[\eta'-\eta]>\eta\epsilon']<\lambda\epsilon'.$$

This gives us

$$\begin{aligned}\Pr[\neg F_{art}] =&\Pr[\neg F_{art}||\eta'-\eta|>\eta\epsilon']\Pr[|\eta'-\eta|>\eta\epsilon']\\ &+\Pr[\neg F_{art}||\eta'-\eta|\leq\eta\epsilon']\Pr[|\eta'-\eta|\leq\eta\epsilon']\\ \leq&\lambda\epsilon'+\Pr[\neg F_{art}||\eta'-\eta|\leq\eta\epsilon']\\ =&\lambda\epsilon'+\frac{\lambda}{\eta'}.\end{aligned}$$

The last equality is true since for fixed η' with $|\eta'-\eta|\geq\eta\epsilon'$ we have $\eta'>\eta(\epsilon'+1)\leq\lambda(\epsilon'+1)\leq\lambda$ and therefore $\Pr[\neg F_{art}]=\frac{\lambda}{\eta'}$. Further we have,

$$\begin{aligned}\Pr[\neg F] =&\Pr[\neg F_{for}]\Pr[\neg F_{art}]\\ \leq&\eta\lambda\epsilon'+\frac{\eta\lambda}{\eta'}\\ \leq&\lambda\epsilon'+\frac{\lambda}{1-\epsilon'}\\ \leq&\lambda(1+2\epsilon').\end{aligned}$$

For all fixed η' with $|\eta'-\eta|\leq\eta\epsilon'$ we have $\Pr[\neg F_{art}]=\min\left\{1,\frac{\lambda}{\eta'}\right\}>\frac{\lambda}{\eta(1+\epsilon')}$ (since $\eta>\lambda$ and hence $\eta(1+\epsilon')>\lambda$). Therefore,

$$\begin{aligned}\Pr[\neg F] =&\eta\Pr[\neg F_{art}]\\ \geq&\eta\Pr[\neg F_{art}||\eta'-\eta|\leq\eta\epsilon']\Pr[|\eta'-\eta|\leq\eta\epsilon']\\ \geq&\eta\frac{\lambda}{\eta(1+\epsilon')}(1-\lambda\epsilon')\\ \geq&\lambda(1-\epsilon')^2\\ \geq&\lambda(1-2\epsilon').\end{aligned}$$

Since $\lambda(1-2\epsilon')\leq\Pr[\neg F]\leq\lambda(1+2\epsilon')$, this implies $|\Pr[\neg F]-\lambda|\leq\lambda 2\epsilon'<\frac{\lambda\epsilon}{4}$ as required. $\square$

Theorem 4.7. *If there exists a polynomial-time EUF-IBSC-CMA adversary $\mathcal{A}$ against our scheme, then there exists an algorithm $\mathcal{B}$ which can break the mCDH assumption. Specifically, for an adversary $\mathcal{A}$ with an advantage ϵ and running time t which may issue at most Q_E extract queries, $\mathcal{B}$ has an advantage of at least ϵ_{mCDH} in solving a mCDH problem in time at most t'.*

$$\begin{aligned}&\epsilon_{mCDH}\geq\frac{\epsilon-\epsilon_{\mathsf{TCR}}}{32Q_E^2(n_u+1)(n_m+1)},\\ &t'\leq t+O(\epsilon^{-2}ln(\epsilon^{-1})\lambda^{-1}ln(\lambda)^{-1}))\end{aligned}$$

Proof. We now prove the EUF-IBSC-CMA security of our scheme. The proof runs from Game′ 0 to Game′ 7.

Recall that the mCDH problem is to compute g^{ab} given $\langle g,g^a,g^{a^2},g^b\rangle\in\mathbb{G}^4$, where g is a generator of $\mathbb{G}$ and $a,b\in_R(\mathbb{Z}_q^*)^2$. We assume that the secrets a,b are known to $\mathcal{B}$ initially. Then, in sequel games, $\mathcal{B}$ will gradually forget the secrets and instead they are available in the forms of g^a,g^{a^2},g^b only.

Game′ 0

$\mathcal{B}$ is simulating the real environment as in Game 0. Then by definition, the advantage of $\mathcal{A}$ is

$$|\Pr[\mathcal{E}_0']| \tag{44}$$

Game′ 1 [Transition based on hash collisions]

This game is identical to Game 1. Thus we have,

$$|\Pr[\mathcal{E}_0']-\Pr[\mathcal{E}_1']|\leq\Pr[HASHABORT] \tag{45}$$

And recall that,

$$\Pr[HASHABORT]\leq\epsilon_{\mathsf{TCR}} \tag{46}$$

Game′ 2 [Transition based on change in the system public key 1]

This game is identical to Game 2. Thus we have,

$$\Pr[\mathcal{E}_1'']=\Pr[\mathcal{E}_2''] \tag{47}$$

Game′ 3 [Transition based on simulation abort]

This game is almost identical to Game 3 except for one change. We now introduce an additional failure event $F_3:F_m(M'')\neq 0$. Then, the new probability of simulation abort F' is

$$\begin{aligned}&F'=F\vee F_3\\ &\Pr[\neg F']=\Pr[\neg F]\Pr[F_m(M'')\neq 0]\end{aligned}$$

Then, we have the following lemma whose proof will be postponed until Section 4.3

Lemma 4.8. *The probability of simulator not aborting is at least $\lambda'=\frac{1}{32Q_E^2(n_m+1)(n_u+1)}$.*

Apart from the additional failure case, the rest of Game′ 3 is identical to Game 3. Therefore,

$$\left|\frac{\Pr[\mathcal{E}_2']-\frac{1}{2}}{\lambda'}-\Pr[\mathcal{E}_3']-\frac{1}{2}\right|\leq\frac{\epsilon}{2} \tag{48}$$

Game′ 4 [Transition based on key derivation]

This game is identical to Game 4. Thus we have,

$$\Pr[\mathcal{E}_3']=\Pr[\mathcal{E}_4'] \tag{49}$$

Game′ 5 [Transition based on Signcrypt/Unsigncrypt computation]

This game is identical to Game 5. Hence,

$$\Pr[\mathcal{E}_4']=\Pr[\mathcal{E}_5'] \tag{50}$$

Game′ 6 [Transition based on change in the system public key 2]

We now assume that $a, b \in \mathbb{Z}_q^*$ are no longer available to the simulator $\mathcal{B}$ as plain integers. Instead, they are available in the form of $A_1 = g^a, A_2 = g^{a^2}, B = g^b$.

Setup: $\mathcal{B}$ sets $g_1 = A_1, g_2 = B$ and $Y = e(g_1, g_2)$. Then, $\mathcal{B}$ replaces the parts of the system public key M_{pk} with newly computed $\langle g_1, g_2, Y\rangle$.

As in Game′ 2, the changes made in M_{pk} as above does not affect the view of $\mathcal{A}$. Therefore,

$$\Pr[\mathcal{E}'_5] = \Pr[\mathcal{E}'_6] \tag{51}$$

Game′ 7 [Transition based on challenge abort]

In Game′ 7, as long as the simulation does not abort, $\mathcal{B}$ is able to solve a mCDH problem as follows.

Forge: Eventually, $\mathcal{A}$ returns a signcrypted message $\mathsf{CT}^* = \langle \mathsf{CT}_1, \mathsf{CT}_2, \mathsf{CT}_3, \mathsf{CT}_4, \mathsf{CT}_5, \mathsf{CT}_6\rangle$. $\mathcal{B}$ unsigncrypts CT^* to get M^*. If CT^* is invalid, **Extract**$(\mathbf{u}_A^*)$ query has previously been made, $F_u(\mathbf{u}_A^*) \neq 0$ or $F_m(M') \neq 0$ where $M' = M \oplus \mathsf{TCR}(\mathsf{CT}_2)$, $\mathcal{B}$ aborts. If $F_u(\mathbf{u}_A^*) = 0$ and $F_m(M') = 0$, $\mathcal{B}$ obtains g^{ab} as follows:

$$\begin{aligned}\mathsf{CT}_5 =& g^{h_2} \cdot H_m(M \oplus \mathsf{TCR}(\mathsf{CT}_2))^{r'} \cdot g_2^a \cdot g_{\mathbf{u}_A}^{r_{\mathbf{u}_A}} \\ =& g^{h_2} \cdot g^{J_m(M\oplus \mathsf{TCR}(\mathsf{CT}_2))r'} \cdot g^{ab} \cdot g_{\mathbf{u}_A}^{r_{\mathbf{u}_A}}.\end{aligned}$$

So,

$$\frac{\mathsf{CT}_5}{g^{h_2} \cdot \mathsf{CT}_2^{J_m(\mathsf{CT}_4 \oplus \mathsf{TCR}(\mathsf{CT}_2))} \cdot \mathsf{CT}_6^{J_u(\mathbf{u}_A)}} = \frac{g^{h_2} \cdot g^{J_m(M\oplus \mathsf{TCR}(\mathsf{CT}_2))r'} \cdot g^{ab} \cdot g_{\mathbf{u}_A}^{r_{\mathbf{u}_A}}}{g^{h_2} \cdot (g^{r'})^{J_m(M\oplus \mathsf{TCR}(\mathsf{CT}_2))} \cdot g_{\mathbf{u}_A}^{r_{\mathbf{u}_A}}} = g^{ab}.$$

Game′ 7 remains indistinguishable from Game′ 6. Hence,

$$\Pr[\mathcal{E}'_6] = \Pr[\mathcal{E}'_7] \tag{52}$$

$\mathcal{B}$ is able to obtain the mCDH output g^{ab} as long as $\neg F'$ holds. This gives us

$$\Pr[\mathcal{E}'_7] = \epsilon_{mCDH} \tag{53}$$

Analysis

The overall advantage ϵ of an adversary $\mathcal{A}$ running in time t is at most,

$$\begin{aligned}\epsilon =& |\Pr[\mathcal{E}'_0]| \text{ (by definition)} \\ \leq& |\Pr[\mathcal{E}'_1] + \epsilon_{\mathsf{TCR}}| \text{ (from equations 45, 46)} \\ =& |\Pr[\mathcal{E}'_2] + \epsilon_{\mathsf{TCR}}| \text{ (from equation 47)} \\ \leq& \left|\frac{\Pr[\mathcal{E}'_3]}{\lambda'} + \epsilon_{\mathsf{TCR}}\right| \text{ (from equation 48)} \\ =& \left|\frac{\Pr[\mathcal{E}'_4]}{\lambda'} + \epsilon_{\mathsf{TCR}}\right| \text{ (from equation 49)} \\ =& \left|\frac{\Pr[\mathcal{E}'_5]}{\lambda'} + \epsilon_{\mathsf{TCR}}\right| \text{ (from equation 50)} \\ =& \left|\frac{\Pr[\mathcal{E}'_6]}{\lambda'} + \epsilon_{\mathsf{TCR}}\right| \text{ (from equation 51)} \\ =& \left|\frac{\Pr[\mathcal{E}'_7]}{\lambda'} + \epsilon_{\mathsf{TCR}}\right| \text{ (from equation 52)} \\ =& \left|\frac{\epsilon_{mCDH}}{\lambda'} + \epsilon_{\mathsf{TCR}}\right| \text{ (from equation 53)} \\ =& \left|\frac{\epsilon_{mCDH}}{\frac{1}{32Q_E^2(n_m+1)(n_u+1)}} + \epsilon_{\mathsf{TCR}}\right| \text{ (from Lemma 4.8)} \\ =& \left|32Q_E^2(n_m+1)(n_u+1)\epsilon_{mCDH} + \epsilon_{\mathsf{TCR}}\right|\end{aligned}$$

Since $\epsilon_{mCDH}, \epsilon_{\mathsf{TCR}}$ are negligible, $\mathcal{A}$ has only negligible advantage in breaking our scheme.

The running time t' of $\mathcal{B}$ is linear in the running time of $\mathcal{A}$. Moreover, $\mathcal{B}$ requires additional running time for sampling. Hence,

$$t' = t + O(\epsilon^{-2}\ln(\epsilon^{-1})\lambda^{-1}\ln(\lambda)^{-1}))$$

This completes the proof for EUF-IBSC-CMA security of our scheme. □

4.3 Proof of Lemma 4.8

Proof. We first compute the probability of the event F_3 not occurring.

$$\begin{aligned}\Pr[\neg F_3] =& \Pr[F_m(M'') = 0] \\ =& \frac{1}{n_m+1}\Pr[K_m(M'') = 0] \\ =& \frac{1}{n_m+1}\frac{1}{m}\end{aligned}$$

Then,

$$\begin{aligned}\Pr[\neg F'] =& \Pr[\neg F \wedge \neg F_3] \\ \geq& \frac{\lambda}{m(n_m+1)} \\ =& \frac{\frac{1}{8(n_u+1)Q_E}}{4Q_E(n_m+1)} \\ =& \frac{1}{32Q_E^2(n_m+1)(n_u+1)}\end{aligned}$$

□

5 Efficiency

We compare the efficiency of our scheme against the other schemes (Jin et al. 2010, Zhang 2010) in terms of the computational cost involved and the ciphertext size. Although these two schemes are broken,

nevertheless the comparison would show the relative performance of our scheme. Table 1 shows that the schemes under the comparison perform similarly in terms of computation overhead.

Table 1: Efficiency Comparison

	Ours			Jin et al.			Zhang		
	$\mathbb{G}$ ex.	$\mathbb{G}_T$ ex.	P	$\mathbb{G}$ ex.	$\mathbb{G}_T$ ex.	P	$\mathbb{G}$ ex.	$\mathbb{G}_T$ ex.	P
Extract	2	0	0	2	0	0	2	0	0
Sign-crypt	6	1	0	3	1	0	5	1	0
Unsign-crypt	2	0	5	2	0	5	0	2	5
Cipher-text size	$\mathbb{G}^5 \times \lvert M \rvert$			$\mathbb{G}^4 \times \mathbb{G}_T$			$\mathbb{G}^4 \times \mathbb{Z}_q^* \times \mathbb{G}_T$		
Security	CCA2 CMA			Broken			Broken		

$\mathbb{G}$ ex.: number of exponentiations in $\mathbb{G}$
$\mathbb{G}_T$ ex.: number of exponentiations in $\mathbb{G}_T$
P: number of pairings
CCA2: IND-IBSC-CCA2
CMA: EUF-IBSC-CMA

Now we compare the ciphertext size by considering the implementation over different types of pairings (see the work by (Galbraith et el. 2008) for more details on the different pairing types). In case the schemes are implemented over a supersingular curve of embedding degree 2, then $|\mathbb{G}| = 512$ bits, $|\mathbb{G}_T| = 1024$ bits and typically $n_m = n_u = 160$ bits. Thus, our ciphertext size will be $512 \times 5 + 160 = 2720$ bits compared to $512 \times 4 + 1024 = 3072$ bits by Jin et al.'s and $512 \times 4 + 160 + 1024 = 3232$ bits by Zhang's.

It is trivially possible to convert our symmetric pairing based scheme to Type 2 pairing version (asymmetric pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ with efficient isomorphism). In a crude way, we may define every group element in our scheme as $\mathbb{G}_2$ element. Then, due to the presence of isomorphic map which efficiently maps elements in $\mathbb{G}_2$ to the corresponding elements in $\mathbb{G}_1$, we obtain Type 2 pairing version of our scheme.

In case where a Type 2 pairing of embedding degree 6 is used, for $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2$ and $h \in \mathbb{G}_T$, $|g_1| = 160$ bits, $|g_2| = 480$ bits and $|h| = 960$ bits (Chatterjee & Menezes 2009). Thus, our ciphertext size will be $480 \times 5 + 160 = 2560$ bits instead of $480 \times 4 + 960 = 2880$ bits for Jin et al.'s and $480 \times 4 + 960 = 3040$ bits for Zhang's.

We can further improve the efficiency with a slightly more effort. If a shorter private key size is desired, then we may define private keys to be of elements from $\mathbb{G}_1$. This will force the ciphertext elements to be from $\mathbb{G}_2$ since each private key component is used in pairing with each ciphertext element for unsigncrypting. If a shorter ciphertext size is of primary concern, then we may define the ciphertext elements to be from $\mathbb{G}_1$ and the private keys from $\mathbb{G}_2$. If this is the case, then our ciphertext size will be $160 \times 5 + 160 = 960$ bits compared to $160 \times 4 + 960 = 1600$ bits by Jin et al.'s and $160 \times 4 + 160 + 960 = 1760$ bits by Zhang's. Thus we see a significant reduction of approximately 40% in the ciphertext size.

6 Conclusion

We have proposed a fully secure IBSC scheme in the standard model under HmDBDH and mCDH assumptions. We note that previously proposed IBSC schemes in the standard model are not secure and many schemes ignore the importance of being able to answer signcrypt/unsigncrypt simulation queries for which the private key generation algorithm fails. Moreover, we have shown that our scheme provide a short ciphertext size by avoiding the inclusion of a target group element in the ciphertext.

References

Boneh, D. & Franklin, M. K. (2001), Identity-Based Encryption from the Weil Pairing, *in* 'Advances in Cryptology - CRYPTO 2001', Vol. 2139, Springer, pp. 213–229.

Zheng, Y. (1997), Digital Signcryption or How to Achieve Cost (Signature & Encryption) $\ll$ Cost(Signature) + Cost(Encryption), *in* 'Advances in Cryptology – CRYPTO 1997', Vol. 1294, Springer, pp. 165–179.

Barreto, P. S.L.M., Libert, B., McCullagh N. & Quisquater, J. (2005), Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps, *in* 'Advances in Cryptology – ASIACRYPT 2005', Vol. 3788, Springer, pp. 515–532.

Chen, L. & Malone-Lee, J. (2005), Improved Identity-Based Signcryption, *in* 'Public Key Cryptography – PKC 2005', Vol. 3386, Springer, pp. 362–379.

Shoup, V. (2004), Sequences of Games: A Tool for Taming Complexity in Security Proofs, *Cryptology ePrint Archive Report Report 2004/332*.

Bellare, M. & Rogaway, P. (1997), Collision-Resistant hashing: Towards making UOWHFs practical, *in* 'Advances in Cryptology – CRYPTO '97', Vol. 1294, Springer, pp. 470–484.

Zhang, B. (2010), 'Cryptanalysis of an Identity Based Signcryption Scheme without Random Oracles', *Journal of Computational Information Systems* **6**(6), 1923–1931.

Ren, Y. & Gu, D. (2007), Efficient Identity Based Signature/Signcryption Scheme in the Standard Model, *in* 'International Symposium on Data, Privacy, and E-Commerce', IEEE, pp. 133–137.

Wang, X. A., Zhong, W. & Luo, H. (2010), Cryptanalysis of Efficient Identity Based Signature/Signcryption Schemes in the Standard Model, *in* Intelligence Information Processing and Trusted Computing (IPTC), 2010 International Symposium on, IEEE, pp. 622-625.

Yu, Y., Yang, B., Sun, Y. & Zhu, S. 'Identity based signcryption scheme without random oracles', *Computers Standards & Interfaces* **31**(1), 56–62.

Jin, Z., Wen, Q. & Du, H. 'An improved semantically-secure identity-based signcryption scheme in the standard model', *Computers & Electrical Engineering* **36**(3), 545–552.

Waters, B. (2006), Efficient Identity-Based Encryption Without Random Oracles, *in* 'Advances in Cryptology – EUROCRYPT 2005', Vol. 4058, Springer, pp. 114–127.

Malone-Lee, J. (2002), Identity-based signcryption, *Cryptology ePrint Archive Report 2002/098*.

Gagné, M., Narayan, S. & Safavi-Naini, R. (2010), Threshold Attribute-Based Signcryption, *in* 'Security and Cryptography for Networks', Vol. 6280, Springer, pp. 154–171.

Ferguson, N., Lucks, S., Schneier, B., Whiting, D., Bellare, M., Kohno, T., Calls, J. & Walker, J. The Skein Hash Function Family, *Submission to the NIST SHA-3 Competition (Finalists)*.

Abdalla, M. Bellare, M. & Rogaway, P. (2001), The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES, *in* 'Topics in Cryptology – CT-RSA 2001', Vol. 2020, Springer, pp. 143–158

Kiltz, E. & Vahlis, Y. (2008), CCA2 secure IBE: standard model efficiency through authenticated symmetric encryption, *in* 'Topics in Cryptology – CT-RSA 2008', Springer, pp. 221–238.

Goldwasser, S. & Kalai, Y. T. (2003), On the (In)security of the Fiat-Shamir Paradigm, *in* 'FOCS '03: Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science', IEEE Computer Society, pp. 102–115.

Boyen, X. (2003)2003, A Swiss Army Knife for Identity-Based Cryptography, *in* 'Advances in Cryptology – CRYPTO 2003', Springer, Vol. 2729, pp. 383–399.

Libert, B. & Quisquater, J.J. (2003), A new identity based signcryption scheme from pairings, *in* 'Information Theory Workshop', IEEE, pp. 155–158.

Chow, S. S. M., Yiu, M., Hui, L. C. K. & Chow, K. P. (2003), Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity, *in* 'International Conference on Information Security and Cryptology – ICISC 2003', Springer, Vol. 2971, pp. 352–369.

Nalla, D. & Reddy, K. C. (2003), Signcryption scheme for identity-based cryptosystems, *Cryptology ePrint Archive Report 2003/066*.

McCullagh, N. & Barreto, P. S. L. M. (2004), Efficient and forward-secure identity-based signcryption, *Cryptology ePrint Archive Report 2004/117*.

Libert, B. & Quisquater, J.J. (2004), Efficient Signcryption with Key Privacy from Gap Diffie-Hellman Groups, *in* 'Public Key Cryptography – PKC 2004', Springer, Vol. 2947, pp. 187–200.

Yuen, T. H. & Wei, V. K. (2005), Fast and Proven Secure Blind Identity-Based Signcryption from Pairings, *in* 'Topics in Cryptology – CT-RSA 2005', Springer, Vol. 3376, pp. 305–322.

Zhang, J., Gao, S., Chen, H. & Geng, Q. (2009), A Novel ID-Based Anonymous Signcryption Scheme, *in* 'Advances in Data and Web Management', Springer, Vol. 5446, pp. 604–610.

Zhang, M., Yang, B., Zhu, S. & Zhang, W. (2010), Efficient Secret Authenticatable Anonymous Signcryption Scheme with Identity Privacy, *in* 'Intelligence and Security Informatics', Springer, Vol. 5075, pp. 126–137.

Chatterjee, S. & Menezes, A. (2009), On Cryptographic Protocols Employing Asymmetric Pairings - The Role of Ψ Revisited, *http://eprint.iacr.org/2009/480*.

Kiltz, E. & Galindo, D. (2009), 'Direct chosen-ciphertext secure identity-based key encapsulation without random oracles', *Theoretical Computer Science* **410**(47-49), 5093–5111.

Galbraith, S. D., Paterson, K. G. & Smart, N. P. (2008), 'Pairings for cryptographers', *Discrete Applied Mathematics*, **156**(16), 3113–3121.