Signcryption in Hierarchical Identity Based Cryptosystem

Sherman S.M. Chow\textsuperscript{1*}, Tsz Hon Yuen\textsuperscript{2}, Lucas C.K. Hui\textsuperscript{1}, and S.M. Yiu\textsuperscript{1}

\textsuperscript{1} Department of Computer Science
The University of Hong Kong
Hong Kong
\{smchow, hui, smyi\}@cs.hku.hk
\textsuperscript{2} Department of Information Engineering
The Chinese University of Hong Kong
Hong Kong
thuyen4@ie.cuhk.edu.hk

Abstract. In many situations we want to enjoy confidentiality, authenticity and non-repudiation of message simultaneously. A traditional approach to achieve this objective is to “sign-then-encrypt” the message, or we can employ special cryptographic scheme like signcryption. Two open problems about ID-based signcryption were proposed in [15]. The first one is to devise an efficient forward-secure signcryption scheme with public verifiability and public ciphertext authenticity, which is promptly closed by [10]. Another one which still remains open is to devise a hierarchical ID-based signcryption scheme that allows the user to receive signcrypted messages from sender who is under another sub-tree of the hierarchy. This paper aims at solving this problem by proposing two concrete constructions of hierarchical ID-based signcryption.

Key words: Data security, hierarchical identity-based signcryption, bilinear pairings

1 Introduction

In traditional public key infrastructure, certificates leak data and are not easily located. Strict online requirement removes offline capability, and validating policy is time-consuming and difficult to administer. Traditional PKI may not provide a good solution in many scenarios. For example, in tetherless computing architecture (TCA)\cite{20} where two mobile hosts wanting to communicate might be disconnected from each other and also from the Internet. As exchange of public keys is impossible in this disconnected situation, ID-based cryptosystem fits in very well since the public key can be derived from the identity of another party.

In many situations we want to enjoy confidentiality, authenticity and non-repudiation of message simultaneously. A traditional approach to achieve this objective is to “sign-then-encrypt” the message, or we can employ special cryptographic scheme like signcryption. A recent direction is to merge the concept of ID-based cryptography and signcryption. Two open problems about ID-based signcryption were proposed in [15]. The first one is to devise an efficient forward-secure signcryption scheme with public verifiability and public ciphertext authenticity, which is promptly closed by [10]. Another one which still remains open is to devise a hierarchical ID-based signcryption scheme that allows the user to receive signcrypted messages from sender who is under another sub-tree of the hierarchy. This paper aims at solving this problem.

As shown by [7], the integrity checking necessary for security against adaptive adversaries can be obtained from the signature. We employ the same idea here to proposed two concrete constructions of hierarchical ID-based signcryption.

\* corresponding author
1.1 Applications

Identity-based cryptography is suitable for the use of commercial organizations. The inherent key-escrow of property is indeed beneficial in commercial organizations, where the big boss has the power to monitor his/her employees’ Internet communications if necessary. Hierarchical structure is common in nowadays’ organizations, single trusted authority for generation of private key and authentication of users is simply impractical, all these give rise to the hierarchical ID-based cryptosystem.

Moreover, hierarchical ID-based cryptosystem is also useful in other scenarios, such as in TCA, a computing architecture with the concept of “regions”, which can be viewed as a branch of the hierarchy[14].

1.2 Related Work

Malone-Lee gave the first ID-based signcryption scheme [17]. This scheme is not semantically secure as the signcrypted text produced is a concatenation of a signature by a variant of Hess’s ID-based signature [13] and a ciphertext by a simplified version of Boneh and Franklin’s ID-based encryption [4]. In short, the signature of the message is visible in the signcrypted message.

On the other hand, Nalla and Reddy’s ID-based signcryption scheme [19] cannot provide public verifiability as well as public ciphertext authenticity since the verification can only be done with the knowledge of recipient’s private key. Libert and Quisquater proposed three ID-based signcryption schemes [15]. None of them can satisfy the requirements for public verifiability and forward security at the same time.

Boyen’s multipurpose ID-based signcryption scheme [5] is the first scheme that provides public verifiability and forward security and is also provably secure. However, this scheme aims at providing ciphertext unlinkability and anonymity. So, a third party cannot verify the origin of the ciphertext, thus the scheme does not satisfy the requirement of public ciphertext authenticity. We remark that Boyen’s scheme is very useful in applications that require unlinkability and anonymity.

The public verifiability of the signcrypted message usually can only be checked with some ephemeral data computed by the intended recipient of the signcrypted message. The notion of verifiable pairing was introduced in [8] to ensure the non-repudiation property of the ID-based signcryption by disallowing the intended recipient to manipulate the ephemeral data.

In 2004, [18] claimed that they were the first one closing the open problem proposed by [15]; however, the open problem was indeed closed by [10] in 2003. Recently, a simple but secure ID-based signcryption scheme was proposed in [7] and another ID-based signcryption scheme was proposed in [16]. The first blind ID-based signcryption scheme with the security model was proposed in [21]. This scheme offers the option to choose between authenticated encryption and ciphertext unlikability. Moreover, the generic group and pairing model was introduced in this paper. Notice that none of the previously mentioned schemes works with hierarchical ID-based cryptosystem.

2 Preliminaries

Before presenting our results, we give the definition of a hierarchical ID-based signcryption scheme by extending the framework in previous work (e.g. [10, 21]). We also review the definitions of groups equipped with a bilinear pairing and the related complexity assumptions.
2.1 Framework of Hierarchical ID-based Signcryption Schemes

An ID-based signcryption (IDSC) scheme consists of six algorithms: Setup, Extract, Sign, Encrypt, Decrypt and Verify. Setup and Extract are executed by the private key generators (PKGs henceforth). Based on the security level parameter, Setup is executed to generate the master secret and common public parameters. Extract is used to generate the private key for any given identity. The algorithm Sign is used to produce the signature of a signer on a message, it also outputs some ephemeral data; Encrypt takes the message, the signature, the ephemeral data and the recipient’s identity to produce a signcrypted text. Decrypt takes the input of secret key and decrypt the message and the corresponding signature, finally Verify is used by any party to verify the signature of a message.

In the hierarchical ID-based signcryption (HIDSC henceforth), PKGs are arranged in a tree structure, the identities of users (and PKGs) can be represented as vectors. A vector of dimension \( \ell \) represents an identity at depth \( \ell \). Each identity \( ID \) of depth \( \ell \) is represented as an ID-tuple \( ID[\ell] = \{ID_1, \ldots, ID_\ell\} \). The algorithms of HIDSC have similar functions to that of IDSC except that the Extract algorithm in HIDSC will generate the private key for a given identity which is either a normal user or a lower level PKG. The private key for identity \( ID \) of depth \( \ell \) is denoted as \( S_{ID[\ell]} \) or \( S_{ID} \) if the depth of \( ID \) is not important. The functions of Setup, Extract, Sign, Encrypt, Decrypt and Verify in HIDSC are described as follows.

- **Setup**: Based on the input of an unary string \( 1^k \) where \( k \) is a security parameter, it outputs the common public parameters \( params \), which include a description of a finite message space together with a description of a finite signature space; and the master secret \( s \), which is kept secret by the private key generator.
- **Extract**: Based on the input of an arbitrary identity \( ID \), it makes use of the master secret \( s \) (for root PKG) or \( S_{ID[j-1]} \) (for lower level PKGs) if \( ID \) is of depth \( j \) to output the private key \( S_{ID[j]} \) for \( ID \) corresponding to \( params \).
- **Sign**: Based on the input \((m, S_{ID})\), it outputs a signature \( \sigma \) and some ephemeral data \( r \), corresponding to \( params \).
- **Encrypt**: Based on the input \((m, S_A, ID_B, \sigma, r)\), it outputs a signcrypted message \( c \).
- **Decrypt**: Based on the input \((c, S_B, ID_B)\), it outputs the message \( m \) and the corresponding signature \( \sigma \).
- **Verify**: Based on the input \((\sigma, m, ID)\), it outputs \( \top \) for “true” or \( \bot \) for “false”, depending on whether \( \sigma \) is a valid signature of message \( m \) signed by \( ID \) or not, corresponding to \( params \).

These algorithms must satisfy the standard consistency constraint of hierarchical ID-based signcryption, i.e. if \( \{\sigma, r\} = \text{Sign}(m, S_A) \) and \( C = \text{Encrypt}(S_A, ID_B, m, \sigma, r) \), we must have \( \{m', ID_{A'}, \sigma'\} = \text{Decrypt}(c, S_B) \), \( m = m' \), \( ID_A = ID_{A'} \) and \( \top = \text{Verify}(\sigma', m, ID_A) \).

2.2 Bilinear Pairing

Let \((\mathbb{G}, \cdot)\) and \((\mathbb{G}_1, \cdot)\) be two cyclic groups of prime order \( p \) and \( g \) be a generator of \( \mathbb{G} \). The bilinear pairing is given as \( \hat{\cdot} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1 \), which satisfies the following properties:

1. **Bilinearity**: For all \( u, v \in \mathbb{G} \) and \( a, b \in \mathbb{Z} \), \( \hat{\cdot}(u^a, v^b) = \hat{\cdot}(u, v)^{ab} \).
2. **Non-degeneracy**: \( \hat{\cdot}(g, g) \neq 1 \).
3. **Computability**: There exists an efficient algorithm to compute \( \hat{\cdot}(u, v) \) \( \forall u, v \in \mathbb{G} \).
2.3 Diffie-Hellman Problems

Definition 1. The computational Diffie-Hellman problem (CDHP) in $\mathbb{G}$ is defined as follows: Given a 3-tuple $(g, g^a, g^b) \in \mathbb{G}^3$, compute $g^{ab} \in \mathbb{G}$. We say that the $(t, \epsilon)$-CDH assumption holds in $\mathbb{G}$ if no $t$-time algorithm has advantage at least $\epsilon$ in solving the CDHP in $\mathbb{G}$.

Definition 2. The bilinear Diffie-Hellman problem (BDHP) in $\mathbb{G}$ is defined as follows: Given a 4-tuple $(g, g^a, g^b, g^c) \in \mathbb{G}^4$ and a pairing $\hat{e}(\cdot, \cdot)$, compute $\hat{e}(g, g)^{abc} \in \mathbb{G}_1$. We say that the $(t, \epsilon)$-BDH assumption holds in $\mathbb{G}$ if no $t$-time algorithm has advantage at least $\epsilon$ in solving the BDHP in $\mathbb{G}$.

Definition 3. The decisional bilinear Diffie-Hellman problem (DBDHP) in $\mathbb{G}$ is defined as follows: Given a 5-tuple $(g, g^a, g^b, g^c, T) \in \mathbb{G}^4 \times \mathbb{G}_1$ and a pairing $\hat{e}(\cdot, \cdot)$, decides whether $T = \hat{e}(g, g)^{abc}$. We say that the $(t, \epsilon)$-DBDH assumption holds in $\mathbb{G}$ if no $t$-time algorithm has advantage at least $\epsilon$ in solving the DBDHP in $\mathbb{G}$.

3 Security model

We present our security model for indistinguishability, existential unforgeability and ciphertext authenticity for HIDSC.

3.1 Indistinguishability

Indistinguishability for HIDSC against adaptive chosen ciphertext attack (IND-CCA2) is defined as in the following IND-CCA2 game. The adversary is allowed to query the random oracles $q_H$ times, the key extraction oracle $q_E$ times, the signcryption oracle $q_S$ times and the Un-signcryption / Recover oracle $q_R$ times. The game is defined as follows:

1. The simulator selects the public parameter and sends the parameter to the adversary.
2. The adversary is allowed to perform a polynomial number of oracle queries adaptively.
3. The adversary generates $m_0, m_1, ID_A, ID_B$, and sends them to the simulator. The simulator randomly chooses $b \in \{0, 1\}$ and delivers the challenge ciphertext $c$ to the adversary where \{\sigma, r\} = Sign(m, S_A) and $C = Encrypt(S_A, ID_B, m_b, \sigma, r)$.
4. The adversary can again perform a polynomial number of oracle queries adaptively.
5. The adversary tries to compute $b$.

The adversary wins the game if he can guess $b$ correctly. The advantage of the adversary is the probability, over half, that he can compute $b$ accurately. The oracles are defined as follows:

- **Key extraction oracle $K\Theta$:** Upon the input of an identity, the key extraction oracle outputs the private key corresponding to this identity, but oracle query to $K\Theta$ with input $ID_B$ is not allowed.
- **Signcryption oracle $S\Theta$:** Upon the input of the message $m$, sender $ID_A$, recipient $ID_B$, the signcryption oracle produces a valid signcryption $\zeta$ but oracle query to $S\Theta$ with input $(m_0/m_1, ID_A, ID_B)$ is not allowed.
- **Unsigncryption oracle $U\Theta$:** Upon the input of the ciphertext $c$, sender $ID_A$ and recipient $ID_B$, the unsigncryption oracle outputs the decryption result and the verification outcome, but oracle query to $U\Theta$ for the challenge ciphertext from the simulator is not allowed.
**Definition 4.** (Indistinguishability) A hierarchical ID-based signcryption scheme is IND-CCA2 secure if no PPT adversary has a non-negligible advantage in the IND-CCA2 game.

Our security notion above is a strong one. It incorporates previous security notions including insider-security in [1], indistinguishability in [17]. Notice that if we set the adversary to send the recipient identity $ID_B$ to the simulator before step 1 (say, in an initialization stage) in the game, the security is reduced to the indistinguishability against selective identity, adaptive chosen ciphertext attack (IND-sID-CCA2).

### 3.2 Existential unforgeability

Existential unforgeability against adaptive chosen message attack (EU-CMA2) for HIDSC is defined as in the following EU-CMA2 game. The adversary is allowed to query the random oracles, $\mathcal{KEO}$, $\mathcal{SO}$ and $\mathcal{UO}$, which are defined in the above section. The game is defined as follows:

1. The simulator selects the public parameter and sends it to the adversary.
2. The adversary is allowed to perform a polynomial number of oracle queries adaptively.
3. The adversary delivers a recipient identity $ID_B$ and a ciphertext $c$.

The adversary wins the game if he can produce a valid $(c, ID_B)$ such that $c$ can be decrypted, under the private key of $ID_B$, to a message $m$, sender identity $ID_A$ and a signature $s$ which passes the verification test.

Oracle query to $\mathcal{KEO}$ with input $ID_A$ is not allowed. No $\mathcal{SO}$ request that resulted in a ciphertext $c$, the signcryption of $m$ from $ID_A$ to $ID_B$, whose decryption under the private key of $ID_B$ is the claimed forgery $(\sigma, m, ID_A)$.

**Definition 5.** (Existential Unforgeability) A hierarchical ID-based signcryption scheme is EU-CMA2 secure if no PPT adversary has a non-negligible probability in winning the EU-CMA2 game.

The adversary is allowed to get the private key of the recipient in the adversary’s answer. This gives us an insider-security in [1]. Notice that if we set the adversary to send the sender identity $ID_A$ to the simulator in Step 1 in the game, the security is reduced to the existential unforgeability against selective identity, adaptive chosen ciphertext attack (EU-sID-CMA2).

### 3.3 Ciphertext Authenticity

Ciphertext authenticity against adaptive chosen message attack (AUTH-CMA2) for HIDSC is defined as in the following AUTH-CMA2 game. The adversary is allowed to query the random oracles, $\mathcal{KEO}$, $\mathcal{SO}$ and $\mathcal{UO}$, which are defined in the above section. The game is defined as follows:

1. The simulator selects the public parameter and sends the parameter to the adversary.
2. The adversary is allowed to perform a polynomial number of oracle queries adaptively.
3. The adversary delivers a recipient identity $ID_B$ and a ciphertext $c$.

The adversary wins the game if he can produce a valid $(c, ID_B)$ such that $c$ can be decrypted, under the private key of $ID_B$, to a message $m$, sender identity $ID_A$ and a signature $s$ which passes the verification test.

Oracle query to $\mathcal{KEO}$ with input $ID_A$ and $ID_B$ is not allowed. The adversary’s answer $(c, ID_B)$ should not be computed by $\mathcal{SO}$ before.
Definition 6. (Ciphertext Authenticity) A hierarchical ID-based signcryption scheme is AUTH-CMA2 secure if no PPT adversary has a non-negligible probability in winning the AUTH-CMA2 game.

Outsider-security is considered in this model since the adversary is not allowed to get the private key of the recipient in the adversary’s answer. This model represents the attack where a signature is re-encrypted by using a public key with unknown secret key.

4 Scheme 1

4.1 Construction

Let $H_1$, $H_2$ and $H_3$ be three cryptographic hash functions where $H_1 : \{0,1\}^* \rightarrow G$ and $H_2 : \{0,1\}^* \rightarrow G$, and $H_3 : G_1 \rightarrow \{0,1\}^{k_0+k_1+n}$ where $k_0$ is the number of bits required to represent an element of $G$, $k_1$ is the maximum number of bits required to represent an identity and $n$ is the number of bits of a message to be signcrypted. Our first construction of A hierarchical ID-based signcryption scheme is given below. The construction is based on the idea in [12].

Setup: On the input of a security parameter $k \in \mathbb{N}$, the BDH parameter generator [4] will generate $G$, $G_1$, $p$ and $\hat{e}(\cdot, \cdot)$. Then the PKG executes the following steps.

1. Select an arbitrary generator $P_0$ from $G$.
2. Pick a random $s_0$ from $Z_p$, which is the system’s master secret key.
3. Compute $Q_0 = P_0^{s_0}$.
4. The public system parameters are

   \[ \text{params} = < G, G_1, \hat{e}(\cdot, \cdot), p, P_0, Q_0, H_1(\cdot), H_2(\cdot), H_3(\cdot) >. \]

KeyGen: For an entity with $ID|k-1 = \{ID_1, ID_2, \cdots, ID_{k-1}, ID_k\}$ of depth $k-1$, it uses its secret key $S_{ID|k-1}$ to generate the secret key for a user $ID|k$ (where the first $k-1$ elements of $ID|k$ are those in $ID|k-1$) as follows.

1. Compute $P_k = H_1(ID_1, ID_2, \cdots, ID_{k-1}, ID_k)$.
2. Pick random $s_{k-1}$ from $Z_p$.
3. Set the private key of the user to be $S_{ID|k} = S_{ID|k-1} \cdot P_k^{s_{k-1}} = \prod_{i=1}^{k} P_i^{s_i-1}$, where $S_{ID|0}$ is defined as the identity element in $G$.
4. Send the values of $Q_i = P_0^{s_i}$ for $1 \leq i \leq k-1$ to the user.

Sign: For a user $A|k$ with secret key $S_{A|k} = \prod_{i=1}^{k} P_A^{s_i-1}$ and the points $Q_i = P_0^{s_i}$ for $1 \leq i \leq k$ to sign on a message $M$, he/she follows the steps below.

1. Pick a random number $r$ from $Z_p^*$.
2. Compute $P_M = H_2(M)$.
3. Compute $\sigma = S_{A|k} \cdot P_M r$.
4. Return signature $= \{ r, \sigma, Q_1, Q_2, \cdots, Q_{k-1}, Q_k = P_0^r \}$.

Encrypt: To signcrypt the message $M$ to user $B|l$, the steps below are used.

1. Compute $P_{B|j} = H_1(B_1, B_2, \cdots, B_j)$ for $1 \leq j \leq l$. 

2. Return ciphertext = 
\[ \{ P_{B|2}^{\mathcal{r}}, \ldots, P_{B|l}^{\mathcal{r}}, (M||A|k) \oplus H_3(\hat{g}^{\mathcal{r}}), Q_1, Q_2, \ldots, Q_k \} \]

where \( \hat{g} = \hat{e}(Q_0, P_{B|1}) \in \mathbb{G}_1 \) and \( \oplus \) represents the bitwise XOR.

**Decrypt**: For user \( B|l \) with secret key \( S_{B|l} = \prod_{i=1}^{t} P_{B|i}^{q_{i-1}} \) and the points \( Q'_i = P_0^{q_i} \) for \( 1 \leq i \leq l \) to decrypt the signencrypted message \( C \), the steps below are used.

1. Let \( C = \{ U_2, \ldots, U_l, V, Q_1, Q_2, \ldots, Q_k \} \)
2. Compute \( V \oplus H_3(\hat{e}(Q_k, S_{B|l})^{\prod_{i=2}^{t} Q'_{i-1}, U_i}) = M||A|k. \)
3. Return \( \{ M, \sigma, H_1(ID_{A|k}), Q_1, Q_2, \ldots, Q_k \}. \)

**Verify**: For \( A \)'s signature \( \{ \sigma, Q_1, Q_2, \ldots, Q_k \} \), everyone can do the following to verify its validity.

1. Compute \( P_M = H_2(M) \).
2. Compute \( P_{A|i} = H_1(A_1, A_2, \ldots, A_i) \) for \( 1 \leq i \leq k \).
3. Return \( \top \) if \( \hat{e}(P_0, \sigma) / \prod_{i=2}^{k} \hat{e}(Q_{i-1}, P_{A|i}) = \hat{e}(Q_0, P_{A|1}) \hat{e}(Q_k, P_M). \)

### 4.2 Efficiency Analysis

The signencrypted message is shortened by one \( \mathbb{G}_1 \) element, as compared with using the scheme HIDE and HIDS in [12] together. Moreover, chosen ciphertext secure HIDE requires the transformation in Section 3.2 of [12], while our scheme does not require such transformation as the integrity checking of the ciphertext is obtained from the signature.

### 4.3 Security analysis

**Theorem 1.** Suppose that the \((t, \varepsilon)\)-BDH assumption holds in \( \mathbb{G} \), then the above scheme is \((t', q_s, q_H, q_E, q_R, \varepsilon)\)-adaptive chosen ciphertext (IND-CCA2) secure for arbitrary \( q_s, q_H, q_E, q_R \), and any \( t' < t - o(t) \).

**Proof.** Dealer \( \mathcal{D} \) gives \( (g, g^a, g^b, g^c) \) to Simulator \( \mathcal{S} \) and wants \( \mathcal{S} \) to compute \( \hat{e}(g, g)^{abc} \). Set \( P_0 = g, Q_0 = g^a \). \( \mathcal{S} \) sends the system parameter to \( \mathcal{A} \). \( \mathcal{A} \) randomly picks \( \mu \) with \( 1 \leq \mu \leq q_H \).

**Phase 1:** Query on \( H_1 \) for input \( (A_1, \ldots, A_k) \):

- If \( k = 1 \), the \( \mu \)-th query to \( H_1 \) with \( k = 1 \) is back patched to \( g^b \). The corresponding identity is denoted as \( ID_b \). Adds the entry \( \langle ID_b, g^b \rangle \) to tape \( L_1 \) and returns \( g^b \).
- Otherwise, randomly picks \( \lambda \in \mathbb{Z}_p; \) add \( \langle A_1, \ldots, A_k, \lambda \rangle \) to \( L_1 \) and returns \( g^\lambda \).

When there is a query on \( H_2 \) for input \( M \), randomly picks \( \lambda \in \mathbb{Z}_p; \) adds \( \langle M, \lambda \rangle \) to \( L_2 \) and returns \( (g^a)^\lambda \). Query on \( H_3 \) is handled by producing a random element from the codomain, and adding both query and answer to tape \( L_3 \).

**Key Extraction Oracle (\( \mathcal{KE} \)):** For input identity \( ID = (I_1, \ldots, I_k) \in \mathbb{Z}_p^k \) where \( k \leq \ell \).

- If \( I_1 = ID_b \), then abort the simulation.
Otherwise, look up at the tape \( L_K = \langle ID_1, \cdots, ID_u, \alpha_1, \cdots, \alpha_{u-1} \rangle \) which stores the previously extracted keys. Let \( y \) be the maximal values such that \((I_1, \cdots, I_y) = (ID_{j_1}, \cdots, ID_{j_y})\) for some tuple \((ID_{j_1}, \cdots, ID_{j_u}, \alpha_{j_1}, \cdots, \alpha_{j(u-1)}) \in L_K\). Then:

- For \( 1 \leq i \leq y \), set \( \alpha_i = \alpha_{j_i}, Q_i = g^{\alpha_i} \). Get \( P_i = H_i(A_1, \cdots, A_i) \) from \( L_1 \) and also get \( \lambda \) from \((A_1, \lambda) \in L_1\).
- For \( y < i \leq k \), query the value of \( P_i \) from \( H_1 \). Randomly generate \( \alpha_i \in \mathbb{Z}_p \).
- Put \((I_1, \cdots, I_k, \alpha_1, \cdots, \alpha_{k-1}) \in L_K \). Set the private key as \( s_{ID|k} = \prod_{i=1}^k P_i^{\alpha_i -1} = (g^a)^\lambda \cdot P_2^{a_1} \cdots P_k^{a_{k-1}} \). Returns \( s_{ID|k} \) and \( Q_i = g^{\alpha_i} \) for \( 1 \leq i \leq k-1 \).

Note that the private key satisfies the required form.

Signcryptions Oracle (SO): For input message \( M \), sender \( ID_{A|k} = \{I_{A1}, \cdots, I_{Ak}\} \), and recipient \( ID_{B|l} = \{I_{B1}, \cdots, I_{Bl}\} \).

- If \( I_{A1} = ID_b \), query \( P_M \) from \( H_2 \) and obtain \( \lambda_M \) from \((M, \lambda_M) \in L_2 \). Query \( P_{A|k} \) from \( H_1 \) and obtain \( \lambda_i \) from \((I_{A1}, \cdots, I_{Ai}, \lambda_i) \in L_1 \), for \( 1 \leq i \leq k \). Randomly generate \( \alpha_i \in \mathbb{Z}_p \) for \( 1 \leq i \leq k \). Compute \( \sigma = (g^a)^{(\alpha_1 \lambda_M)} \prod_{i=2}^k g^{\lambda \alpha_{i-1}}, Q_i = g^{\alpha_i} \) for \( 1 \leq i \leq k-1 \), \( Q_k = (g^a)^{(b)^{-1}/\lambda_M} \). Query \( P_{B|l} \) from \( H_1 \) and obtain \( \lambda_{B|l} \) from \((I_{B1}, \cdots, I_{Bl}, \lambda_{Bl}) \in L_1 \), for \( 1 \leq i \leq l \). Compute \( U_i = (g^{\alpha_k}) (g^b)^{-\lambda_{Bl}/\lambda_M} \) for \( 2 \leq i \leq l \), \( V = (M||\sigma||A|k) \oplus H_3(e(g^a, (g^{\alpha_k})(g^b)^{-\lambda_{Bl}/\lambda_M})) \). Return the ciphertext \( C = \{U_2, \cdots, U_l, V, Q_1, \cdots, Q_k\} \). \( S \) puts \((ID_{A|k}, ID_{B|l}, M, C) \in L_S \). It is easy to see that the signature will pass the verification test:

\[
\hat{e}(P_0, \sigma) / \prod_{i=2}^k \hat{e}(Q_{i-1}, P_{A|k})
= \hat{e}(g, (g^{(\alpha_k \lambda_M)}) \prod_{i=2}^k g^{\lambda \alpha_{i-1}} / \prod_{i=2}^k \hat{e}(g, g^{\lambda \alpha_{i-1}})
= \hat{e}(g, g^{(\alpha_k \lambda_M)}) \hat{e}(g, \prod_{i=2}^k g^{\lambda \alpha_{i-1}}) / \prod_{i=2}^k \hat{e}(g, g^{\lambda \alpha_{i-1}})
= \hat{e}(g^{\alpha_k}, g^{(\alpha_M)}) \prod_{i=2}^k \hat{e}(g, g^{\lambda \alpha_{i-1}}) / \prod_{i=2}^k \hat{e}(g, g^{\lambda \alpha_{i-1}})
= \hat{e}(g^{\alpha_k}, g^b) \hat{e}(g^{\alpha_k}, g^{(\alpha_M)}) \hat{e}(g^{(\alpha_M)} (g^b)^{-1/\lambda_M})
= \hat{e}(g^{\alpha_k}, g^b) \hat{e}(g^{\alpha_k}, g^{(\alpha_M)}) \hat{e}(g^{(\alpha_M)} (g^b)^{-1/\lambda_M})
= \hat{e}(Q_0, P_{A|k}) \hat{e}(Q_k, P_M)
\]

- Otherwise, \( S \) retrieves the private key of \( ID_{A|k} \) using the same way as \( KEQ \) and then uses it to run signcryption and gets ciphertext \( c \). \( S \) puts \((ID_{A|k}, ID_{B|l}, M, C) \in L_S \).

Un-signcryptions / Recover Oracle (UD): For input sender \( ID_{A|k} = \{I_{A1}, \cdots, I_{Ak}\} \), recipient \( ID_{B|l} = \{I_{B1}, \cdots, I_{Bl}\} \) and ciphertext \( C = \{U_2, \cdots, U_l, V, Q_1, \cdots, Q_k\} \).

- For the case \( ID_{B|l} = ID_b \), \( S \) finds if \((ID_{A|k}, ID_{B|l}, M, C) \) is in \( L_S \). If so, returns \( M \). Otherwise, \( S \) searches for all combinations \((M, \sigma)\) such that \((M, h_2) \in L_2, (g', h_3) \in L_3,\) for some \( h_2, h_3 \), under the constraints that \( h_3 \oplus V = M||\sigma||A|k \), and \( \hat{e}(g, \sigma) = \)
\[ \hat{e}(g^a, P_{A\|}) \hat{e}(Q_k, h_2) \prod_{i=2}^k \hat{e}(Q_{i-1}, P_{A\|}). \] 

\[ S \text{ simply picks one of the valid message } M \text{ from the above and return it as answer. If no such tuple is found, the oracle signals that the ciphertext is invalid.} \]

- For other cases, \( S \) retrieves the private key of \( ID_{B|} \) using the same way as \( KEO \) and then uses it to decrypt and verify.

**Witness Extraction:** As in the IND-CCA2 game, at some point \( A \) chooses to test \( m_0, m_1 \), and sends \( ID_{A|k} \) on which he wishes to be challenged. \( S \) retrieves the private key of \( ID_{A|k} \) and \( Q_1, \cdots, Q_k \) using the same way as \( KEO \). \( S \) queries \( P_{B|i} \) from \( H_1 \) and obtain get \( \lambda_{Bi} \) from \( \langle I_{B1}, \cdots, I_{Bi}, \lambda_{Bi} \rangle \in L_1 \), for 2 \( \leq i \leq k \). \( S \) randomly picks \( V \in \{0,1\}^{k_0+k_1+n} \) and responds with challenge ciphertext \( C = \{(g^c)^{\lambda_{m2}}, \cdots, (g^c)^{\lambda_{m1}}, V, Q_1, \cdots, Q_{k-1}, g^c\} \). All further queries by \( A \) are processed adaptively as in the oracles above, with no private key extraction of \( ID_{B|} \). Finally, \( A \) returns its final guess \( \theta \). \( S \) ignores the answer from \( A \), randomly picks an entry \( \langle g', h_3 \rangle \) on \( L_3 \), and returns \( g' \) as the solution to the BDH problem.

If the recipient identity is \( ID_{B|} = \{I_{B1}, \cdots, I_{Bi}\} \) with \( I_{Bi} = ID_{bi} \), to recognize the challenge ciphertext is incorrect, \( A \) needs to query random oracle \( H_3 \) with \( g' = \hat{e}(Q_0, P_{B|i})^c = \hat{e}(g, g)^{abc} \). It will leave an entry \( \langle g', h_3 \rangle \) on \( L_3 \), from which \( S \) can extract \( g' = \hat{e}(g, g)^{abc} \). \( \square \)

**Theorem 2.** Suppose that the \((t, e)\)-CDH assumption holds in \( \mathbb{G} \), then the above scheme is \((t', qS, qH, qE, qR, e)\)-adaptive chosen message (EU-CMA2) secure for arbitrary \( qS, qH, qE, qR \), and any \( t' < t - o(t), e' > \frac{e}{c qS qE} \).

**Proof.** Dealer \( D \) gives \((g, g^a, g^b)\) to Simulator \( S \) and wants \( S \) to compute \( g^{ab} \). Set \( g_1 = g^a, g_2 = g^b \). The initialization, setup and the simulation of oracles are similar to those in the proof in Theorem 1. The difference is that probabilistic simulations are used in the simulation of two hash oracles: the one for hashing the identity \( H_1(\cdot) \) and the one for hashing the message \( (H_2(\cdot)) \).

**Queries on oracle \( H_1 \) for identity \((A_1, \cdots, A_k)\):** If \( k = 1 \), \( S \) embeds part of the challenge \( g^b \) in the answer of many \( H_1 \) queries [11]. \( S \) picks \( \lambda \in_R \mathbb{F}_q^* \) and repeats the process until \( \lambda \) is not in the list \( L_1 \). \( S \) then flips a coin \( W_1 \in \{0,1\} \) that yields 0 with probability \( \zeta_1 \) and 1 with probability \( 1 - \zeta_1 \). (\( \zeta_1 \) will be determined in the probability analysis shortly afterward.) If \( W_1 = 0 \) then the hash value \( H_1(A_1) \) is defined as \( g^\lambda \); else if \( W_1 = 1 \) then returns \( H_1(A_1) = (g^b)^\lambda \). In either case, \( S \) stores \( \langle A_1, \lambda, W_1 \rangle \) in the list \( L_1 \).

On the other hand, if \( k > 1 \), \( S \) performs the simulation as that in the proof of Theorem 1.

**Queries on oracle \( H_2 \) for message \( m \):** In this case, \( S \) embeds the remaining part of the challenge \( g^a \) in the answer of many \( H_2 \) queries. \( S \) picks \( \beta \in_R \mathbb{F}_q^* \) and repeats the process until \( \beta \) is not in the list \( L_2 \). \( S \) then flips a coin \( W_2 \in \{0,1\} \) that yields 0 with probability \( \zeta_2 \) and 1 with probability \( 1 - \zeta_2 \). (\( \zeta_2 \) will be determined later.) If \( W_2 = 0 \) then the hash value \( H_2(m) \) is defined as \( (g^a)^\beta \); else if \( W_2 = 1 \) then returns \( H_2(m) = g^\beta \). In either case, \( S \) stores \( \langle m, \beta, W_2 \rangle \) in the list \( L_2 \).

**Witness Extraction** After such probabilistic behaviour is introduced to the simulation, \( S \) will fail for the \( KEO \) query of \((A_1, \cdots, A_k)\) if \( W_1 = 1 \) is found in the corresponding entry of \( A_1 \) in \( L_1 \). The \( SO \) query for the signcryption of message \( m \) done by \((A_1, \cdots, A_k)\) will fail too when \( W_1 = 1 \) and \( W_2 = 1 \) are found in the corresponding entry of \( A_1 \) in \( L_1 \) and \( m \) in \( L_2 \) respectively.

At the end of the game, \( A \) returns a forgery \( C = \{U_2, \cdots, U_1, V, Q_1, Q_2, \cdots, Q_k\} \) which is the signcryption of message \( m \) done by \((A_1, \cdots, A_k)\). \( S \) cannot solve the CDH problem.
if the forgery is not related to the problem instance at all, i.e. when $W_1 = 0$ is found in the corresponding entry of $A_1$ in the list $L_1$ and $W_1 = 1$ and $W_2 = 0$ are found in the corresponding entry of $A_1$ in $L_1$ and $m$ in $L_2$ respectively.

For successful cases, $S$ gets the forged signature $\{\sigma, Q_1, Q_2, \ldots, Q_k\}$ by the decryption of the signcrypted text. Suppose that $\lambda_i$ is the corresponding entry of $P_i$ in the list $L_1$ and $\beta$ is the corresponding entry of $P_M$ in the list $L_2$, since $\sigma = \prod_{i=1}^{k} (P_i^{\lambda_i}) \cdot P_M^\beta = g^{\alpha_{11}} \prod_{i=2}^{k} (P_i^{\lambda_i})$. $P_M^\beta \in \mathcal{C}$ can compute the solution of the CDH problem by $\sigma/\prod_{i=2}^{k} (Q_{i-1}^{\lambda_i}) \cdot Q_k^\beta$.

**Probability Analysis:** The probability that $S$ answers to all private key extraction queries is $\zeta_1 q_s$. $S$ can answer all signcrypted queries for users $H_i(A_1, \ldots, A_k)$ where $\langle A_1, \lambda, 0 \rangle$ is in the list $L_1$. So the worst case for $S$ to answer all signcrypted queries correctly happens when all signcrypted requests are for users $H_i(A_1, \ldots, A_k)$ where $\langle A_1, \lambda, 1 \rangle$ is in the list $L_1$. For these class of users, $S$ can still signcrypted given the message is $M$ where $\langle M, \beta, 0 \rangle$ can be found in the list $L_2$. So the probability for $S$ to successfully answer all signcrypted requests is $\zeta_2 q_s$.

Finally, the probability that $A$ makes a forged signature for user $H_i(A_1, \ldots, A_k)$ where $\langle A_1, \lambda, 1 \rangle$ is in the list $L_1$ is $1 - \zeta_1$ and the probability that $A$ makes a forged signature on message $M$ where $\langle M, \beta, 1 \rangle$ is in the list $L_2$ is $1 - \zeta_2$.

Hence the probability for $S$ to solve CDH problem successfully is $f_{qe}(\zeta_1) f_{qs}(\zeta_2)$ where $f_{\zeta}(\zeta) = \zeta^2 (1-\zeta)$. Simple differentiation shows that $f_{\zeta}(\zeta)$ is maximized when $\zeta = 1 - (x+1)^{-1}$, and the corresponding probability is $\frac{1}{2} (1 - \frac{1}{x+1})^2$. So the maximum probability for $S$ to solve CDH problem successfully is

$$\frac{1}{q_s q_e} \left(1 - \frac{1}{q_s + 1}\right)^{q_s+1} \left(1 - \frac{1}{q_e + 1}\right)^{q_e+1}$$

For large $q_s$ and $q_e$, this probability is approximately equal to $1/e^2 q_s q_e$.

\[\square\]

5 Scheme 2

5.1 Construction

Let $H$ be a cryptographic hash function where $H : \{0,1\}^* \rightarrow \mathbb{Z}_p$. We use $H(\cdot)$ to hash the string representing the identity into an element in $\mathbb{Z}_p^\kappa$, the same hash function will be used in the signing algorithm too. Similar to [3], $H$ is not necessarily a full domain hash function. Our second construction of HIDSC, based on the ideas in [9] and [3], is given below.

**Setup:** On the input of a security parameter $k \in \mathbb{N}$, the BDH parameter generator [4] will generate $\mathbb{G}$, $\mathbb{G}_1$, $p$ and $\hat{\epsilon}(\cdot, \cdot)$. Then the PKG executes the following steps.

1. Select $\alpha$ from $\mathbb{Z}_p^*$, $h_1, h_2, \ldots, h_\ell$ from $\mathbb{G}$ and two generators $g$, $g_2$ from $\mathbb{G}^*$, where $\ell$ is the number of levels of the hierarchy that our scheme supports.
2. The public parameters are: $\{g, g_1 = g^\alpha, g_2, h_1, h_2, \ldots, h_\ell, \hat{\epsilon}(g_1, g_2)\}$.
3. The master secret key is $d_{ID}[0] = g_2^\alpha$.

**KeyGen:** For a user $ID|k-1 = \{I_1, I_2, \ldots, I_{k-1}\}$ of depth $k - 1$, he/she uses his/her secret key $d_{ID|k-1}$ to generate the secret key for a user $ID|k$ (where the first $k - 1$ elements of $ID|k$ are those in $ID|k-1$) as follows.

1. Pick random $r_k$ from $\mathbb{Z}_p$. 

2. \(d_{ID[k]} = \{d_0 F_k(ID_k)^{r_k}, d_1, \cdots, d_{k-1}, g^{r_k}\}\), where \(F_k(x)\) is defined as \(g_1^x h_k\).

**Sign:** For a user \(ID[k]\) with secret key \(\{g_2^a \prod_{j=1}^{k} F_j(ID_j)^{r_j}, g^r, \cdots, g^{r_k}\}\) to sign on a message \(m\), he/she follows the steps below.

1. Pick a random number \(s\) from \(\mathbb{Z}_p^*\).
2. Compute \(h = H(m, \hat{e}(g_1, g_2)^s)\).
3. Repeat Steps 1-3 in case the unlikely event \(s + h = 0\) occurs.
4. For \(j = \{1, 2, \cdots, k\}\), compute \(y_j = d_j^{s+h}\).
5. Compute \(z = d_0^{s+h}\).
6. Return signature \(\{s, y_1, y_2, \cdots, y_k, z\}\).

**Encrypt:** To signcrypt a message \(M \in \mathbb{G}_1\) under the public key \(ID[l] = \{I_1, I_2, \ldots, I_l\}\), the ciphertext is

\[\{\hat{e}(g_1, g_2)^s \cdot M, g^s, F_1(I_1)^s, F_2(I_2)^s, \cdots, F_l(I_l)^s, y_1, y_2, \cdots, y_k, z\}\]

**Decrypt:** For a user \(ID[l]\) with secret key \(\{g_2^a \prod_{j=1}^{l} F_j(ID_j)^{r_j}, g^{r_1}, \cdots, g^{r_l}\}\) to decrypt the signcrypted text \(\{A, B, C_1, \cdots, C_l, y_1, y_2, \cdots, y_k, z\}\), he/she follows the steps below.

1. Compute \(\sigma = \hat{e}(g_1, g_2)^s \cdot \frac{\hat{e}(B, d_0)}{\prod_{j=1}^{l} \hat{e}(C_j, d_j)}\).
2. Obtain the message \(M\) by \(A \cdot \sigma^{-1}\).

**Verify:** For \(ID[k] = \{I_1, I_2, \cdots, I_k\}\)'s signature \(\{\sigma, y_1, y_2, \cdots, y_k, z\}\), everyone can do the following to verify its validity.

1. Compute \(h = H(m, \sigma)\).
2. Return \(\top\) if \(\hat{e}(g, z) = \sigma \cdot \hat{e}(g_1, g_2)^s \prod_{j=1}^{k} F_j(ID_j)^{y_j} \prod_{j=1}^{k} \hat{e}(y_j, h_j)\), \(\bot\) otherwise.

### 5.2 Efficiency Analysis

The signcrypted message is shortened by one \(\mathbb{G}_1\) element, as compared with using the scheme in [9] and [3] together. Moreover, chosen ciphertext secure HIDE requires the transformation in Section 4 of [6], while our scheme does not require such transformation as the integrity checking of the ciphertext is obtained from the signature.

### 5.3 Security Analysis

**Theorem 3.** Suppose that the \((t, e)\)-Decision BDH assumption holds in \(\mathbb{G}\), then the above scheme is \((t', q_5, q_H, q_E, q_R, e)\)-selective identity, adaptive chosen ciphertext (IND-sID-CCA2) secure for arbitrary \(q_5, q_H, q_E, q_R\), and any \(t' < t - o(t)\).

**Proof.** Dealer \(D\) gives \((g, g^a, g^b, g^c, T)\) to Simulator \(S\) and wants \(S\) to output 1 if \(T = \hat{e}(g, g)^{abc}\) or output 0 otherwise. Set \(g_1 = g^a, g_2 = g^b, g_3 = g^c\).

**Initialization:** Adversary \(A\) sends an identity \(ID^* = (I_1^*, \cdots, I_k^*) \in \mathbb{Z}_p^k\) of depth \(k \leq \ell\) that it intends to attack to \(S\).
**Setup:** $S$ randomly picks $\alpha_1, \ldots, \alpha_\ell \in \mathbb{Z}_p$ and defines $h_j = g_1^{-I_j^*} g^{\alpha_j} \in \mathbb{G}$ for $j = 1, \ldots, \ell$. $S$ sends the system parameter $(g, g_1, g_2, h_1, \ldots, h_\ell, \hat{e}(g_1, g_2))$ to $A$.

**Phase 1:** Query on $H$ for input $(m, \sigma)$:
- If $(m, \alpha, h) \in L$ for some $h$, return $h$.
- Otherwise, randomly picks $h \in \mathbb{Z}_p$; add $(m, \alpha, h)$ to $L$ and returns $h$.

**Key Extraction Oracle (KEO):** For input identity $ID = (I_1, \ldots, I_u) \in \mathbb{Z}_p^u$ where $u \leq \ell$.
- If $ID = ID^*$ or $ID$ is a prefix of $ID^*$, then abort the simulation.
- Otherwise, let $j$ be the smallest index such that $I_j \neq I_j^*$. $S$ firstly derives a private key for identity $(I_1, \ldots, I_j)$ from which it then construct a private key for $ID$. $S$ randomly picks $r_1, \ldots, r_j \in \mathbb{Z}_p$ and sets:

$$d_0 = g_2^{-a_j} \prod_{v=1}^{j-1} F_v(I_v)^{r_v}, d_1 = g^{r_1}, \ldots, d_{j-1} = g^{r_{j-1}}, d_j = g_2^{-a_j} g_j$$

We now show that $(d_0, d_1, \ldots, d_j)$ is a valid random private key for $(I_1, I_2, \ldots, I_j)$. Let $\bar{r}_j = r_j - b/(I_j - I_j^*)$ and then we have:

$$g_2^{-a_j} F_j(I_j)^{\bar{r}_j} = g_2^{-a_j} F_j(I_j)^{r_j} = g_2^{a}(g_1 I_j^{-I_j^* - I_j^*} g^{\alpha_j})^{r_j - I_j^* - I_j^* - I_j^* - I_j^*} = g_2^{a} F_j(I_j)^{\bar{r}_j}$$

So the private key satisfies the required form.

**Sign-cryption Oracle (SO):** For input message $m$, sender $ID_{A[k]} = \{I_{A1}, \ldots, I_{Ak}\}$, and recipient $ID_{B[\ell]} = \{I_{B1}, \ldots, I_{B\ell}\}$.
- If $ID_{A[k]}$ equals $ID^*$ or a prefix of $ID^*$, then $S$ randomly chooses $h \in \mathbb{Z}_p$, and computes $\sigma = \hat{e}(g_1, g_2)^{-h}$. Then $S$ randomly picks $r_1, \ldots, r_k \in \mathbb{Z}_p$, computes $y_{h} = g_2^{r_v}$ for $1 \leq v \leq k$ and $z = \prod_{v=1}^{k} g_2^{r_v} \alpha_v$. Then $S$ adds the tuple $(m, \sigma, h)$ to $L$ to force the random oracle $H(m, \sigma) = h$. Finally, $S$ returns the ciphertext $C = \{\sigma \cdot m, g^{h^{-1}} F_1(I_{B1})^{-1}, g^{h^{-1}} F_2(I_{B2})^{-1}, \ldots, F_l(I_{B_l})^{-1}, y_1, y_2, \ldots, y_k, z\}$. $S$ puts $(ID_{A[k]}, ID_{B[\ell]}, m, C, \sigma, h)$ in $L_S$.
- Otherwise, $S$ retrieves the private key of $ID_{A[k]}$ using the same way as KEO and then uses it to run signcryption and gets ciphertext $c$. $S$ puts $(ID_{A[k]}, ID_{B[\ell]}, m, C, s, h)$ in $L_S$.

**Unsign-cryption / Recover Oracle (UO):** For input sender $ID_{A[k]} = \{I_{A1}, \ldots, I_{Ak}\}$, recipient $ID_{B[\ell]} = \{I_{B1}, \ldots, I_{B\ell}\}$ and ciphertext $C = \{A, B, C_1, \ldots, C_i, y_1, \ldots, y_k, z\}$.
- For the case $ID_{B[\ell]} = ID^*$, $S$ finds if $(ID_{A[k]}, ID_{B[\ell]}, m, C, s, h)$ is in $L_S$. If so, returns $m$. Otherwise, $S$ searches for a valid $m$ in all entries $(m, \sigma, h) \in L$, under the constraints that $\sigma \cdot m = A, \sigma = \hat{e}(g, z)/(\hat{e}(g_1, g_2^{h} \prod_{j=1}^{k} y_j^{ID_{A[k]}}) \prod_{j=1}^{l} \hat{e}(y_j, h_j))$ and $\hat{e}(B, F_j(I_{Bj})) = \hat{e}(g, C_j)$ for $1 \leq j \leq l$. $S$ simply picks a message in one of the valid $m$ in the above and return it as the answer. If no such tuple is found, the oracle signals that the ciphertext is invalid.
- For other cases, $S$ retrieves the private key of $ID_{A[k]}$ using the same way as KEO and then uses it to decrypt and verify.

**Witness Extraction:** As in the IND-sID-CCA2 game, at some point $A$ chooses plaintext $m_0, m_1$, and sender $ID_{A[k]}$ on which he wishes to be challenged. $S$ picks a random bit $b \in \{0, 1\}$ and responds with challenge ciphertext $C = \{T, M_b, g_3, g_3^{a_1}, \ldots, g_3^{a_l}, y_1, \ldots, y_k, z\}$.
where \((y_1, \ldots, y_k, z)\) is a valid signature from \(ID_{A|k}\). All further queries by \(A\) are processed adaptively as in the oracles above. Finally, \(A\) returns its final guess \(b'\). If \(b = b'\), then \(S\) outputs 1 meaning \(T = \hat{e}(g, g)^{abc}\). Otherwise it outputs 0 meaning \(T \neq \hat{e}(g, g)^{abc}\).

If the recipient identity is \(ID^*\), then the value of \(\hat{e}(g_1, g_2)^s\) is equal to \(\hat{e}(g^a, g^b)^c = \hat{e}(g, g)^{abc}\). If \(A\) has the advantage \(\epsilon\) to guess \(b\) correctly, then \(S\) has the advantage \(\epsilon\) to solve the DBDH.

**Theorem 4.** Suppose that the \((t, \epsilon)\)-CDH assumption holds in \(G\), then the above scheme is \((t', qs, qH, qE, qR, \epsilon')\)-selective identity, adaptive chosen message (EU-ID-CMA) secure for arbitrary \(qs, qH, qE, qR\), and any \(t' < t - o(t), \epsilon' > \epsilon \cdot (1 - \frac{qs(qH + qS)}{q})\).

**Proof.** Dealer \(D\) gives \((g, g^a, g^b)\) to Simulator \(S\) and wants \(S\) to compute \(g^{ab}\). Set \(g_1 = g^a, g_2 = g^b\). The initialization, setup and the simulation of oracles are the same as the proof of Theorem 3. At the end of the game, \(A\) returns a forgery \(C = \{A, B, C_1, \ldots, C_i, y_1, \ldots, y_k, z\}\) using \(h\) from \(H\) query. By forking lemma, we rewind \(A\) to the time when the \(H\) query was issued and get \(C' = \{A, B', C'_1, \ldots, C'_i, y'_1, \ldots, y'_k, z'\}\) using \(h'\) from \(H\) query. We can get \(d_j = \frac{(y_j y'_j)^{(h-h')^{-1}}}{(y_{j+1} y'_{j+1})^{(h-h')^{-1}}} \) for \(1 \leq j \leq k\). Then we can calculate \(d_0 = (z / z')^{(h-h')^{-1}}\). Finally we can get \(g^{a}_2 = d_0 / \prod_{j=1}^{k} d_j^{a_j}\) which is the solution to the CDH problem.

Let us consider the possibility for \(S\) to fail. The only possibility for introducing an error is in defining \(H(m, \sigma)\) which is already defined. Since \(\sigma\) takes its value uniformly at random in \(G\), the chance for the occurrence of one of these events is at most \((qH + qS)/q\) for each query. Therefore over the whole simulation, the chance of an error is at most \(qs(qH + qS)/q\). Hence \(S\) succeeds with probability at least \(\epsilon \cdot (1 - \frac{qs(qH + qS)}{q})\).

**6 Conclusion**

Two concrete constructions of hierarchical identity based signcryption are proposed, which closed the open problem proposed by [15]. Our schemes are provably secure under the random oracle model [2]. Moreover, our schemes does not require transformation which is necessary for the case of hierarchical identity based encryption as the integrity checking of the ciphertext is obtained from the signature. We believe that hierarchical identity based signcryption schemes are useful in nowadays commercial organization and also in new network architecture such as tetherless computing architecture. Future research directions include further improvement on the efficiency of hierarchical identity based signcryption schemes and achieving other security requirements such as public ciphertext authenticity ([10, 15]) or ciphertext anonymity ([5]).

**References**