SIGNCRYPTION IN HIERARCHICAL IDENTITY BASED CRYPTOSYSTEM

(Extended Abstract)

Sherman S.M. Chow[1], Tsz Hon Yuen[2], Lucas C.K. Hui[1], and S.M. Yiu[1]

[1]*Department of Computer Science*
University of Hong Kong
Pokfulam, Hong Kong
{smchow, hui, smyiu}@cs.hku.hk

[2]*Department of Information Engineering*
Chinese University of Hong Kong
Shatin, Hong Kong
thyuen4@ie.cuhk.edu.hk

Abstract: In many situations we want to enjoy confidentiality, authenticity and non-repudiation of message simultaneously. One 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 identity-based (ID-based) signcryption were proposed in [16]. 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: signcryption, hierarchical identity-based cryptosystem, 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. Moreover, traditional PKI may not provide a good solution in many scenarios. For example, in tetherless computing architecture (TCA) [24] 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, identity-based (ID-based) cryptosystem fits in very well since the public key can be derived from the identity of another party [23].

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 which can be more efficient in computation than running encryption and signature separately. A recent direction is to merge the concept of ID-based cryptography [22] and signcryption [26]. Two open problems about ID-based signcryption were proposed in [16]. 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.

1.1 Applications

ID-based cryptography is suitable for the use of commercial organizations. In their settings, the inherent key-escrow of property is indeed beneficial, 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 may be impractical; all these motivated the need of 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 [15,23].

1.2 Related Work

Malone-Lee gave the first ID-based signcryption scheme [18]. 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 [14] 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 [20] 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 [16]. 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, [19] claimed that they were the first one closing the open problem proposed by [16]; 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 an ID-based signcryption scheme with exact security was proposed in [17]. The first blind ID-based signcryption scheme was proposed in [25]. This scheme offers the option to choose between authenticated encryption and ciphertext unlinkability. The generic group and pairing model was also 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. [10,25]). 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

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 for the use of Encrypt; Encrypt takes the message, the signature, the ephemeral data produced by Sign and the recipient's identity to produce a signcrypted text. Decrypt takes the input of secret key and decrypt the signcrypted text to give 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 ℓ represents an identity at depth ℓ. Each identity ID of depth ℓ is represented as an ID-tuple $ID \mid \ell = \{ID_1, \cdots, ID_\ell\}$. The algorithms of HIDSC have similar functions to those 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 ℓ is denoted as $S_{ID|\ell}$ (or S_{ID} if the depth of ID does not related to the discussion). The functions of Setup, Extract, Sign, Encrypt, Decrypt and Verify in HIDSC are described as follows.

- Setup: Based on the input of a unary string 1^k where k is a security parameter, it outputs the common public parameters $params$, which include descriptions of a finite message space, a finite signature space and a finite signcrypted text space. It also outputs the master secret s, which is kept secret by the root private key generator (PKG).
- Extract: Based on the input of an arbitrary identity ID of depth j, it makes use of the secret key $S_{ID|j-1}$ (if $j = 1$, the input of the algorithm is s, which is the master secret of the root PKGs, instead of $S_{ID|j-1}$) to output the private key $S_{ID|j}$ for ID.
- Sign: Based on the input (M, S_{ID}), it outputs a signature σ and some ephemeral data r.
- 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, the corresponding signature σ and the purported signer ID_A.
- Verify: Based on the input (σ, M, ID), it outputs $\top$ for "true" or $\perp$ for "false", depending on whether σ is a valid signature of message M signed by ID or not.

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

2.2 Bilinear Pairing

Let $(G, \cdot)$ and $(G_1, \cdot)$ be two cyclic groups of prime order q and g be a generator of G. The bilinear pairing is given as $\hat{e}: G \times G \to G_1$, which satisfies the following properties:

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

2.3 Diffie-Hellman Problems

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

DEFINITION 2. The bilinear Diffie-Hellman problem (BDHP) in G is defined as follows: Given a 4-tuple $(g, g^a, g^b, g^c) \in G^4$ and a pairing function $\hat{e}(\cdot,\cdot)$, compute $\hat{e}(g, g)^{abc} \in G_1$. We say that the (t, ε)-BDH assumption holds in G if no t-time algorithm has advantage at least ε in solving the BDHP in G.

DEFINITION 3. The decisional bilinear Diffie-Hellman problem (DBDHP) in G is defined as follows: Given a 5-tuple $(g, g^a, g^b, g^c, T) \in G^4 \times G_1$ and a pairing function $\hat{e}(\cdot,\cdot)$, decides whether $T = \hat{e}(g, g)^{abc}$. We say that the (t, ε)-DBDH assumption holds in G if no t-time algorithm has advantage at least ε in solving the DBDHP in 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.

1. The simulator selects the public parameter and sends the parameter to the adversary.
2. There are three oracles except the random oracles (hash oracles).
   - **Key extraction oracle** KEO: Upon the input of an identity, the key extraction oracle outputs the private key corresponding to this identity.
   - **Signcryption oracle** SO: Upon the input of the message M, the sender ID_A, the recipient ID_B, the signcryption oracle produces a valid signcryption C.
   - **Unsigncryption oracle** UO: Upon the input of the ciphertext C, the sender ID_A and the recipient ID_B, the unsigncryption oracle outputs the decryption result and the verification outcome.

The adversary is allowed to perform a polynomial number of oracle queries adaptively, but oracle query to KEO with input ID_B is not allowed.

3. The adversary generates M_0, M_1, ID_A, ID_B, and sends them to the simulator. The simulator randomly chooses $b \in_R \{0,1\}$ and delivers the challenge ciphertext C to the adversary where $\{\sigma, r\} = \text{Sign}\ (M, S_A)$ and $C = \text{Encrypt}\ (S_A, ID_B, M_b, \sigma, r)$. M_0 and M_1 should be of equal length, and no oracle query have been made and will be made to SO with input (M_0, ID_A, ID_B) and (M_1, ID_A, ID_B) throughout the game.
4. The adversary can again perform a polynomial number of oracle queries adaptively, but oracle query to UO for the challenge ciphertext (defined later) from the simulator is not allowed.
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.

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] and *indistinguishability* in [18].

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, KEO, SO and UO (which are defined above) with the restriction that oracle query to KEO with input ID_A is not allowed.

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, a sender identity ID_A and a signature σ which passes the verification test and no SO request that resulted in a ciphertext C, whose decryption under the private key of ID_B is the claimed forgery (σ, 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* as defined 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, KEO, SO and UO, which are defined above. 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 σ which passes the verification test.

Oracle query to KEO with input ID_A and ID_B is not allowed. The adversary's answer (C, ID_B) should not be computed by 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 ℓ be the number of levels of the hierarchy to be supported. Let H_1, H_2 and H_3 be three cryptographic hash functions where $H_1 : \{0,1\}^* \to G$ and $H_2 : \{0,1\}^* \to G$, and $H_3 : G_1 \to \{0,1\}^{k_0+k_1+n}$ 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 (of depth ℓ) and n is the maximum 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 [13].

`Setup`: On the input of a security parameter $k \in N$, the root PKG uses the BDH parameter generator [4] to generate G, G_1, q and $\hat{e}(\cdot,\cdot)$, where q is the order of groups G and G_1. Then the root 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

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

`KeyGen`: For an entity with $ID \mid k-1 = \{ID_1, ID_2, \cdots, ID_{k-1}\}$ of depth $k-1$ (for root PKG, its depth is defined as 0 and its identity is defined as empty string ε), it uses its secret key $S_{ID|k-1}$ (or the master secret s_0 of the root PKGs, if $k=1$) to generate the secret key for a user $ID \mid k$ (where the first $k-1$ elements of $ID \mid k$ are those in $ID \mid k-1$) as follows.

1. Compute $P_{ID|k} = H_1(ID_1, ID_2, \cdots, ID_{k-1}, ID_k)$.
2. Pick random s_{k-1} from Z_p (this step is not necessary for the root PKG as s_0 is already defined).
3. Set the private key of the user to be $S_{ID|k} = S_{ID|k-1} \cdot P_{ID|k}{}^{s_{k-1}} = \prod_{i=1}^{k} P_{ID|i}{}^{s_{i-1}}$, where $S_{ID|0}$ is defined as the identity element in G.
4. Send the values of $Q_i = P_0{}^{s_i}$ for $1 \le i \le k-1$ as "verification points" to the user.

`Sign`: For a user $A|k = \{A_1, A_2, \cdots, A_k\}$ with secret key $S_{A|k} = \prod_{i=1}^{k} P_{A|i}{}^{s_{i-1}}$ and the points $Q_i = P_0{}^{s_i}$ for $1 \le i \le k-1$ 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 $\{\sigma, Q_1, Q_2, \cdots, Q_{k-1}, Q_M = P_0{}^r\}$ as the signature and return r as the ephemeral data for Encrypt.

`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 $1 \le j \le l$.
2. Pads the identity A with a chain of zero bits if it is not of depth ℓ.
3. Return ciphertext $C =$

$$\{P_{B|2}{}^r, \cdots, P_{B|l}{}^r, (M \| \sigma \| A) \oplus H_3(\hat{g}^r), Q_1, Q_2, \cdots, Q_M\}$$

where $\hat{g} = \hat{e}(Q_0, P_{B|1}) \in G_1$ and $\oplus$ represents the bitwise XOR.

`Decrypt`: For user $B|l$ with secret key $S_{B|l} = \prod_{i=1}^{l} P_{B|i}{}^{s'_{i-1}}$ and the points $Q'_i = P_0{}^{s'_i}$ for $1 \le i \le l$ to decrypt the signcrypted message c, the steps below are used.

1. Let $C = \{U_2, \cdots, U_l, V, Q_1, Q_2, \cdots, Q_{k-1}, Q_M\}$
2. Compute $V \oplus H_3(\hat{e}(Q_M, S_{B|l}) / \prod_{i=2}^{l} \hat{e}(Q'_{i-1}, U_i)) = M \| \sigma \| A$.
   (for $l = 1$, $\prod_{i=2}^{l} \hat{e}(Q'_{i-1}, U_i)$ is defined as the identity element in G_1.)
3. Return $\{M, \sigma, A, Q_1, Q_2, \cdots, Q_{k-1}, Q_M\}$.

`Verify`: For A's signature $\{\sigma, Q_1, Q_2, \cdots, Q_{k-1}, Q_M\}$, everyone can do the following to verify its validity.

1. Compute $P_M = H_2(M)$.
2. Compute $P_{A|i} = H_1(A_1, A_2, \cdots, A_i)$ for $1 \le i \le k$.
3. Return $\top$ if $\hat{e}(P_0, \sigma) / \prod_{i=2}^{k} \hat{e}(Q_{i-1}, P_{A|i}) = \hat{e}(Q_0, P_{A|1}) \hat{e}(Q_k, P_M)$.
   (for $k = 1$, $\prod_{i=2}^{k} \hat{e}(Q_{i-1}, P_{A|i})$ is defined as the identity element in G_1.)

4.2 Efficiency Analysis

We first consider the communication efficiency of the scheme. The signcrypted message is shortened by one G_1 element, as compared with using the schemes HIDE and HIDS in [13] together. Moreover, the size of the signcrypted message can be further reduced if the sender and the receiver have a common low-level PKG ancestor. The modification incurred includes using a fixed s_{k-1} instead of a random one for each invocation of KeyGen. For verification side, since the sender and the receiver share some common "verification points", these points can be omitted from the transmission. For encryption side, the ciphertext size can be reduced by using the concept of "Dual-HIDE" in [13], which can be seen as an extension of the concept of non-interactive key sharing in [22]. The basic idea behind non-interactive key sharing is that a same value can be computed either from the sender's private key and the recipient's public key or from the recipient's private key and the sender's public key. The sender is required to get his/her private key before the encryption can be done, but there is no practical difference in the case of signcryption since the sender who are going to sign the message must have his/her private key ready anyway. In our proposed construction, the "non-interactive agreed secret key" created by the sender ID whose the common ancestor with the receipt is at level m is $\hat{e}(S_{ID|m}, P_0) = \hat{e}(P_0, S_{ID}) / \prod_{i=m+1}^{l} \hat{e}(Q_{i-1}, P_{ID|i})$. To utilizing it, simply replace $\hat{g}$ with this agreed secret key.

For the computational efficiency, chosen ciphertext secure HIDE requires the transformation in Section 3.2 of [13], while our scheme does not require such transformation as the integrity checking of the ciphertext is obtained from the signature. Notice that the above modification from the concept of "Dual-HIDE" distributes the computational effort of the sender and that of the recipient in a more even way.

4.3 Security Analysis

THEOREM 1. Suppose that the (t,ε)-BDH assumption holds in G, then the above scheme is $(t', q_S, q_H, q_E, q_R, \varepsilon)$-adaptive chosen ciphertext (IND-CCA2) secure for any $t' < t - o(t)$.

THEOREM 2. Suppose that the (t,ε)-CDH assumption holds in G, then the above scheme is $(t', q_S, q_H, q_E, q_R, \varepsilon)$-adaptive chosen message (EU-CMA2) secure for any $t' < t - o(t)$, $\varepsilon' > \varepsilon / e^2 q_S q_E$.

THEOREM 3. Suppose that the (t,ε)-CDH assumption holds in G, then the above scheme is $(t', q_S, q_H, q_E, q_R, \varepsilon)$-adaptive chosen message (AUTH-CMA2) secure for any $t' < t - o(t)$.

Proofs are omitted due to the length constraint. Please refer to the full version of this paper [11].

5. SCHEME 2

5.1 Construction

Let H be a cryptographic hash function where $H:\{0,1\}^* \rightarrow Z_p$. We use $H(\cdot)$ to hash the string representing the identity into an element in $Z_p{}^k$, the same hash function will be used in the signing algorithm too. Similar to [3], H is not necessarily a full domain hash function. Notice that the identity string is hashed to Z_p instead G in scheme 1, so we use I_i to denote $H(ID_i)$ for $1 \le i \le \ell$, where ℓ is the number of levels of the hierarchy to be supported. Our second construction of HIDSC, based on the ideas in [9] and [3], is given below.

`Setup`: On the input of a security parameter $k \in N$, the root PKG uses the BDH parameter [4] to generate G, G_1, q and $\hat{e}(\cdot,\cdot)$, where q is the order of groups G and G_1. Then the root PKG executes the following steps.

1. Select α from Z_p^*, $h_1, h_2, \cdots, h_\ell$ from G and two generators g, g_2 from G^*, where ℓ is the number of levels of the hierarchy to be supported.
2. The public parameters are: $\{g, g_1 = g^\alpha, g_2, h_1, h_2, \cdots, h_\ell, \hat{e}(g_1, g_2)\}$.
3. The master secret key is $d_{ID|0} = g_2{}^\alpha$.

`KeyGen`: For a user $ID|k-1 = \{ID_1, ID_2, \cdots, ID_{k-1}\}$ 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 Z_p.
2. $d_{ID|k} = \{d_0 F_k(I_k)^{r_k}, d_1, \cdots, d_{k-1}, g^{r_k}\}$, where $F_k(x)$ is defined as $g_1{}^x h_k$.

`Sign`: For a user $ID|k$ with secret key $\{g_2{}^\alpha \prod_{j=1}^k F_j(I_j)^{r_j}, g^{r_1}, \cdots, g^{r_k}\}$ to sign on a message M, he/she follows the steps below.

1. Pick a random number s from 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 $\{s, y_1, y_2, \cdots, y_k, z\}$ as the signature.

`Encrypt`: To signcrypt a message $M \in G_1$ to user $ID|l = \{ID_1, ID_2, \cdots, ID_l\}$, the ciphertext to be generated is

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

`Decrypt`: For a user $ID'|l$ with secret key $\{d'_0 = g_2{}^\alpha \prod_{j=1}^l F_j(I'_j)^{r'_j}, d'_1 = g^{r'_1}, \cdots, d'_l = g^{r'_l}\}$ to decrypt the signcrypted text $\{u_1, \cdots, u_l, v, w, y_1, y_2, \cdots, y_k, z\}$, he/she follows the steps below.

1. Compute $\sigma = \hat{e}(g_1, g_2)^s$ by $\hat{e}(w, d'_0)/\prod_{j=1}^{l} \hat{e}(u_j, d'_j)$.
2. Obtain the message M by $v \cdot \sigma^{-1}$

`Verify:` For $ID|k = \{ID_1, ID_2, \cdots, ID_k\}$'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 $\hat{e}(g, z) = \sigma \cdot \hat{e}(g_1, g_2{}^h \prod_{j=1}^{k} y_j^{I_j}) \prod_{j=1}^{k} \hat{e}(y_j, h_j)$, $\perp$ otherwise.

5.2 Efficiency Analysis

We first analyze the computational efficiency. For the proposed scheme 1, admissible encoding scheme [4] are required for the hash function H_1 and H_2, which is computationally expensive as such scheme requires $\log_2(q/p)$ -bit scalar multiplication in $E(F_q)$ where F_q is the field on which G is based and p is the size of the group G. Using the example from [21], if $\log_2 p = 512$ and the embedding degree of pairing is 6, then $\log_2 q$ should be at least 2560 and hence 2048-bit scalar multiplication is needed. Scheme 2's hash function does not rely on such admissible encoding scheme. 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.

For the communication efficiency of the scheme, the signcrypted message is shortened by one G_1 element, as compared with using the scheme in [9] and [3] together.

5.3 Security Analysis

THEOREM 4. Suppose that the (t, ε)-Decision BDH assumption holds in G, then the above scheme is $(t', q_S, q_H, q_E, q_R, \varepsilon)$ -selective identity, adaptive chosen ciphertext (IND-sID-CCA2) secure for arbitrary q_S, q_H, q_E, q_R, and any $t' < t - o(t)$.

THEOREM 5. Suppose that the (t, ε)-CDH assumption holds in G, then the above scheme is $(t', q_S, q_H, q_E, q_R, \varepsilon')$ -selective identity, adaptive chosen message (EU-sID-CMA) secure for any $t' < t - o(t)$, $\varepsilon' > \varepsilon \cdot (1 - q_S(q_H + q_S)/q)$.

THEOREM 6. Suppose that the (t, ε)-CDH assumption holds in G, then the above scheme is $(t', q_S, q_H, q_E, q_R, \varepsilon)$-selective identity, adaptive chosen message (AUTH-sID-CMA2) secure for any $t' < t - o(t)$.

Proofs are omitted due to the length constraint. Please refer to the full version of this paper [11].

6. CONCLUSION

Two concrete constructions of hierarchical identity based signcryption are proposed, which closed the open problem proposed by [16]. Our schemes are provably secure under the random oracle model [2]. Moreover, our schemes do 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 ([10,16]) or ciphertext anonymity ([5]).

ACKNOWLEDGEMENT

This research is supported in part by the Areas of Excellence Scheme established under the University Grants Committee of the Hong Kong Special Administrative Region (HKSAR), China (Project No. AoE/E-01/99), grants from the Research Grants Council of the HKSAR, China (Project No. HKU/7144/03E and HKU/7136/04E), and grants from the Innovation and Technology Commission of the HKSAR, China (Project No. ITS/170/01 and UIM/145).

REFERENCES

[1] Jee Hea An, Yevgeniy Dodis, and Tal Rabin. On the Security of Joint Signature and Encryption. In Lars R. Knudsen, editor, Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings, volume 2332 of Lecture Notes in Computer Science, pages 83–107. Springer-Verlag Heidelberg, 2002.

[2] Mihir Bellare and Phillip Rogaway. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In Proceedings of the 1st ACM Conference on Computer and Communications Security, pages 62–73, 1993.

[3] Dan Boneh and Xavier Boyen. Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In Christian Cachin and Jan Camenisch, editors, Advances in

Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings, volume 3027 of Lecture Notes in Computer Science, pages 223–238. Springer, 2004.

[4] Dan Boneh and Matt Franklin. Identity-Based Encryption from the Weil Pairing. In Joe Kilian, editor, Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings, volume 2139 of Lecture Notes in Computer Science, pages 213–229. Springer-Verlag Heidelberg, 2001.

[5] Xavier Boyen. Multipurpose Identity-Based Signcryption : A Swiss Army Knife for Identity-Based Cryptography. In Dan Boneh, editor, Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings, volume 2729 of Lecture Notes in Computer Science, pages 382–398. Springer, 2003.

[6] Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-Ciphertext Security from Identity-Based Encryption. In Christian Cachin and Jan Camenisch, editors, Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings, volume 3027 of Lecture Notes in Computer Science, pages 207–222. Springer, 2004.

[7] Liqun Chen and John Malone-Lee. Improved Identity-Based Signcryption. In Serge Vaudenay, editor, Public Key Cryptography - PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23-26, 2005. Proceedings, volume 3386 of Lecture Notes in Computer Science, pages 362–379. Springer, 2005. Also available at Cryptology ePrint Archive, Report 2004/114.

[8] Sherman S.M. Chow. Verifiable Pairing and Its Applications. In Chae Hoon Lim and Moti Yung, editors, Information Security Applications: 5th International Workshop, WISA 2004, Jeju Island, Korea, August 23-25, Revised Selected Papers, volume 3325 of Lecture Notes in Computer Science, pages 170–187. Springer-Verlag, 2004.

[9] Sherman S.M. Chow, Lucas C.K. Hui, S.M. Yiu, and K.P. Chow. Secure Hierarchical Identity Based Signature and its Application. In Javier Lopez, Sihan Qing, and Eiji Okamoto, editors, Information and Communications Security, 6th International Conference, ICICS 2004, Malaga, Spain, October 27-29, 2004, Proceedings, volume 3269 of Lecture Notes in Computer Science, pages 480–494. Springer-Verlag, 2004.

[10] Sherman S.M. Chow, S.M. Yiu, Lucas C.K. Hui, and K.P. Chow. Efficient Forward and Provably Secure ID-Based Signcryption Scheme with Public Verifiability and Public Ciphertext Authenticity. In Jong In Lim and Dong Hoon Lee, editors, Information Security and Cryptology - ICISC 2003, 6th International Conference Seoul, Korea, November 27-28, 2003, Revised Papers, volume 2971 of Lecture Notes in Computer Science, pages 352–369. Springer, 2003.

[11] Sherman S.M. Chow, Tsz Hon Yuen, Lucas C.K. Hui, and S.M. Yiu. Signcryption in Hierarchical Identity Based Cryptosystem, 2004. Extended abstract appeared in Security and Privacy in the Age of Ubiquitous Computing, IFIP TC11 20th International Conference on Information Security (SEC 2005), May 30 - June 1, 2005, Chiba, Japan. Full version available at Cryptology ePrint Archive, Report 2004/244.

[12] Jean-Sébastien Coron. On the Exact Security of Full Domain Hash. In Mihir Bellare, editor, Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings, volume 1880 of Lecture Notes in Computer Science, pages 229–235. Springer, 2000.

[13] Craig Gentry and Alice Silverberg. Hierarchical ID-Based Cryptography. In Yuliang Zheng, editor, Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings, volume 2501 of Lecture Notes in Computer Science, pages 548–566. Springer, 2002. Available at http://eprint.iacr.org.

[14] Florian Hess. Efficient Identity Based Signature Schemes based on Pairings. In Kaisa Nyberg and Howard M. Heys, editors, Selected Areas in Cryptography, 9th Annual International Workshop, SAC 2002, St. John's, Newfoundland, Canada, August 15-16, 2002. Revised Papers, volume 2595 of Lecture Notes in Computer Science, pages 310–324. Springer, 2003.

[15] Berkeley. Intel Research. Identity Based Cryptosystem for Secure Delay Tolerant Networking.

[16] Benoît Libert and Jean-Jacques Quisquater. New Identity Based Signcryption Schemes from Pairings. In IEEE Information Theory Workshop, pages 155–158, 2003. Full Version Available at http://eprint.iacr.org.

[17] Benoît Libert and Jean-Jacques Quisquater. The Exact Security of an Identity Based Signature and its Applications. Cryptology ePrint Archive, Report 2004/102, 2004. Available at http://eprint.iacr.org.

[18] John Malone-Lee. Identity Based Signcryption. Cryptology ePrint Archive, Report 2002/098, 2002. Available at http://eprint.iacr.org.

[19] Noel McCullagh and Paulo S. L. M. Barreto. Efficient and Forward-Secure Identity-Based Signcryption. Cryptology ePrint Archive, Report 2004/117, 2004. Available at http://eprint.iacr.org.

[20] Divya Nalla and K.C. Reddy. Signcryption Scheme for Identity-Based Cryptosystems. Cryptology ePrint Archive, Report 2003/066, 2003. Available at http://eprint.iacr.org.

[21] Dong Jin Park, Kihyun Kim, and Pil Joong Lee. Public Key Encryption with Conjunctive Field Keyword Search. In Chae Hoon Lim and Moti Yung, editors, Information Security Applications: 5th International Workshop, WISA 2004, Jeju Island, Korea, August 23-25, Revised Selected Papers, volume 3325 of Lecture Notes in Computer Science, pages 73–86. Springer-Verlag, 2004.

[22] Ryuichi Sakai, Kiyoshi Ohgishi, and Masao Kasahara. Cryptosystems based on Pairing over Elliptic Curve. In Proceedings of Symposium on Cryptography and Information Security (SCIS 2000) C-20, 2000.

[23] Aaditeshwar Seth. Personal Communication, September 2004.

[24] Aaditeshwar Seth, Patrick Darragh, and Srinivasan Keshav. A Generalized Architecture for Tetherless Computing in Disconnected Networks. Manuscript.

[25] Tsz Hon Yuen and Victor K. Wei. Fast and Proven Secure Blind Identity-Based Signcryption from Pairings. In A. J. Menezes, editor, Topics in Cryptology - CT-RSA 2005, The Cryptographers' Track at the RSA Conference 2005, San Francisco, CA, USA, Febrary 14-18, 2005, Proceedings, volume 3376 of Lecture Notes in Computer Science, San Francisco, CA, USA, February 2005. Springer. To Appear. Also available at Cryptology ePrint Archive, Report 2004/121.

[26] Yuliang Zheng. Digital Signcryption or How to Achieve Cost (Signature & Encryption) $<<$ Cost(Signature) + Cost(Encryption). In Burton S. Kaliski Jr., editor, Advances in Cryptology: Proceedings of CRYPTO 1997 5th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, volume 1294 of Lecture Notes in Computer Science, pages 165–179. Springer-Verlag, 1997.