International Journal of Security and Its Applications
Vol. 10, No. 6 (2016) pp.215-228
http://dx.doi.org/10.14257/ijsia.2016.10.6.21

On Resolving Key Escrow Problem in HIBE and HIBS

Jian-Wu Zheng[1, 2], Jing Zhao[3] and Xin-Ping Guan[1, 4]

[1]*Institute of Electrical Engineering, Yanshan University, 066004, China*
[2] *School of Transportation, Shijiazhuang Tiedao University, 050043, China*
[3] *School of Civil Engineering, Shijiazhuang Tiedao University, 050043, China*
[4]*Department of Automation, Shanghai Jiao Tong University, 200240, China*
zhengjw@ysu.edu.cn, zhaoj@stdu.edu.cn, xpguan@ysu.edu.cn

Abstract

In traditional hierarchical identity based cryptosystems (HIBC), non-leaf entities as level PKGs are usually capable of deriving private keys for their descendants with use of their private keys, non-leaf entities can therefore act (decrypt or sign) on the behalf of their arbitrary descendants. This is called key escrow problem of HIBC. In order to resolve key escrow problem, a new technique – Identifier Discrimination is proposed in this paper for composing private keys for entities in hierarchy. With the technique, an identity selective secure HIBE scheme is constructed under Decisional Bilinear Diffie-Helleman (DBDH) assumption in standard security model, in which any identity is incapable of deriving private keys for any of its descendants with use of its private key, and the privilege of generating private keys for each individual descendant is delegated by the root PKG through authorization, that we call Authorization Delegation. Moreover, a new hierarchical identity based signature (HIBS) scheme is constructed from our HIBE construction, by applying Naor transformation of an identity-based signature (IBS) out of an IBE. Because of the inability of deriving its descendants' private keys with use its private key, an entity therefore cannot sign messages on behalf of any of its descendants, thus guaranteeing that authenticity and non-repudiation properties are achieved in our HIBS system.

Keywords*: Hierarchical Identity Based Encryption, Identity Based Signature, Authorized Delegation, Identifier Discrimination, Imaginary Identity*

1. Introduction

An Identity Based Encryption (IBE) system [10][8] is a public key system that an entity's public key can be any identifier of the entity, and private key for the entity can be calculated from its identifier (identity) with use of a master key by an authority, called private key generator (PKG). Since the introduction of the concept of Identity-based Encryption (IBE) by Shamir in 1984 [18], some proposals of IBE Schemes had been proposed [11][19][20], however none of them are satisfactory. Precisely, there are no usable IBE constructions until the works by Boneh and Franklin [8], Cocks [10], and Sakai *et. al.*, [17].

Hierarchical Identity Based Encryption (HIBE) [14][12][7] is a generalization of IBE [10][8] that maps institution structure or entity relationship in real world. Gentry and Silverberg [12] presented the first HIBE construction in the random oracle model. Boneh and Boyen [1][5] introduced a selective identity, chosen-plaintext (IND-sID-CPA) secure HIBE scheme BB_1 under Decisional Bilinear Diffie-Hellman (DBDH) assumption in standard model. Later, works by Boneh *et. al.*, [2][6], Waters [21][22] and Lewko *et. al.*, [15] provided some fully secure schemes without random oracles.

ISSN: 1738-9976 IJSIA

Bilinear pairings, *e.g.*, Weil pairing, open new ways of constructing both IBE and IBS [16] [13] schemes since works by Boneh and Franklin [8] and Cocks [10]. As noted by Naor[8], IBS schemes can be steadily constructed from IBE schemes by treating the message intended to be signed as child identifier of signer's identity and extracting a private key for the newly constructed identity as resulting signature. Boneh, Lynn and Shacham [9] and Boneh and Boyen [3] instantiated with IBE schemes by Boneh and Franklin [8] and by Boneh and Boyen [4] respectively to construct notable short signatures. Hierarchical IBS is natural generalization of IBS from HIBE [12].

1.1. Related Work

Although key escrow problem is inherent in Identity-Based Cryptography (IBC) resulting from the mechanism of generating private keys for entities in the system, but it is necessary not to let the problem be exaggerated. However, as of BB_1 system proposed by Boneh and Boyen [5], private key $d_{ID_j} = (d_0^{(ID_j)}, RD_1^{(ID_j)}, \ldots, RD_j^{(ID_j)}) \in \hat{G}^{j+1}$ for identity $ID_j = (I_1, \ldots, I_j) \in (Z_q^*)^j$ can be used to derive private keys $d_{ID_{j+1}}$ for $ID_{j+1} = (ID_j, I_{j+1})$ with $j+1$ random numbers $r_1, \ldots, r_{j+1}$ from Z_q as $(d_0^{(ID_j)} + \sum_{k=1}^{j+1} r_k (I_k \hat{g}_1 + \hat{h}_k), RD_1^{(ID_j)} + r_1 \hat{g}, \ldots, RD_j^{(ID_j)} + r_j \hat{g}, r_{j+1} \hat{g})$. That is, any entity can derive private keys for all of its descendants. That we call unlimited delegation, which undesirably empowers an entity to be able to act on behalf of any of its descendants.

As for HIBE systems in [6] and [15], an entity in the system is restricted to be only capable of generating private keys for its descendants of limited depth. Specifically, by distributing a restricted private key to an entity, the root PKG can limit the number of the entity's descendants whose private keys can be derived by the entity with its private key. Private key $d_{ID_j} \in G^{\ell-j+2}$ for identity $ID_j = (I_1, \ldots, I_j) \in (Z_q^*)^j$ is extracted by the root PKG [6] as $(\alpha g_2 + r^{(ID_j)}(g_3 + \sum_{k=1}^{j} I_k h_k), r^{(ID_j)} g, r^{(ID_j)} h_{j+1}, \ldots, r^{(ID_j)} h_\ell)$, where $r^{(ID_j)} h_{j+1}, \ldots, r^{(ID_j)} h_\ell$ are all $\ell - j$ private values for deriving private keys for all descendants of Entity$_j$. To derive a private key for $ID_{j+1} = (ID_j, I_{j+1})$ with use of $d_{ID_j} = (d_0^{(ID_j)}, d_1^{(ID_j)}, RH_{j+1}^{(ID_j)}, \ldots, RH_\ell^{(ID_j)})$, pick a random number r from Z_q, and output $d_{ID_{j+1}} \in G^{\ell-j+1}$ as $(d_0^{(ID_j)} + r(g_3 + \sum_{k=1}^{j+1} I_k h_k) + I_{j+1} RH_{j+1}^{(ID_j)}, d_1^{(ID_j)} + rg, RH_{j+2}^{(ID_j)} + r h_{j+2}, \ldots, RH_\ell^{(ID_j)} + r h_\ell)$.

Actually, by distributing a restricted private key for ID_j with only t components $r^{(ID_j)} h_{j+k}$ for $k = 1, \ldots, t$ to Entity$_j$, Entity$_j$ can only be capable of generating private keys for its descendants of bounded depth t, *i.e.*, descendants at levels between $j+1$ and $j+t$ along the hierarchy tree. That is called limited delegation.

Limited delegation does prevent private keys for descendants at depth beyond the limited depth from being derived. Nevertheless, there is no means to only derive a private key for identity ID_ξ at level ξ in $[j+2, \ell]$ (with ID_j being its prefix) with use of private key for ID_j without revealing private keys for identites at levels between $j+1$

and $\xi - 1$ with ID_j as their prefix. This undesirable breach in privacy is resulted from the need of a parent's private key when deriving a private key for a child.

1.2. Our Results

We construct a selective identity secure HIBE system under DBDH assumption in standard model with authorized delegation and dedicated encryption privacy, where any entity not being authorized does not have the capability of deriving valid private keys for its descendants, however any entity can be authorized to be capable of generating valid private keys for its descendants.

Moreover, basing on Naor transformation of an identity-based signature (IBS) out of an IBE, we build a new hierarchical IBS (HIBS) scheme from our HIBE scheme. Being unable to generating a private key for any of its descendants, an entity cannot sign messages on behalf of any of its descendants, which guarantees that authenticity and non-repudiation properties are achieved in HIBS setting.

Identifier Discrimination. When extracting a private key for identity $ID_j = (I_1, \ldots, I_j) \in (\mathbb{Z}_q^*)^j$ of Entity $_j$, our HIBE construction differentiates between the local identifier I_j and ancestor identifiers (non-local identifiers) I_1, …, I_{j-1}, on which global privacy and dedicated privacy making up of the private key for ID_j are defined respectively, and any entity being unable to generate dedicated privacy for any of its descendants is prevented from deriving valid private keys for the descendant. That we call Identifier Discrimination.

Imaginary Identity. The concept of imaginary identity corresponding to a true identity ID_j is introduced for defining secrets that are private values for deriving private keys for the identity. A secret is originally crafted by the root PKG by randomizing its master key along an imaginary identity hierarchy constructed from ID_j for which private keys are authorized to be derived. The secret from PKG is hierarchically randomized to create secrets level by level along the imaginary hierarchy until generating a secret for the end level of the imaginary hierarchy, *i.e.,* level j or hierarchy depth of ID_j, which is a private key for ID_j in true hierarchy.

2. Preliminaries

2.1. Bilinear Pairings

Definition 1. Let $k \in \mathbb{N}$ be a security parameter and q be a k-bit prime integer. Let $\mathbb{G} = \langle g \rangle$ and $\hat{\mathbb{G}} = \langle \hat{g} \rangle$ be two additively-written groups ($(\mathbb{G},+)$ and $(\hat{\mathbb{G}},+)$)both of order q, $\mathbb{G}_t$ a multiplicatively-written group of order q with identity denoted by 1, and let $e: \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_t$ be a function that maps pairs of elements in $\mathbb{G} \times \hat{\mathbb{G}}$ to elements of a group of $\mathbb{G}_t$. e is a bilinear map (pairing) if following conditions are satisfied.

1. **Bilinearity:** $e(aP, bQ) = e(P, Q)^{ab}$, $\forall P \in \mathbb{G}, Q \in \hat{\mathbb{G}}$ and $\forall a, b \in \mathbb{Z}_q$.

2. **Non-degeneracy:** $e(g, \hat{g}) \neq 1$, g and $\hat{g}$ are generators of $\mathbb{G}$ and $\hat{\mathbb{G}}$ respectively.

3. **Computability:** the group operations in $\mathbb{G}$, $\hat{\mathbb{G}}$, $\mathbb{G}_t$ and the pairing e are all efficiently computable (probabilistic polynomial-time bounded time complexity).

The bilinear pairing e is called symmetric if $\hat{\mathbb{G}}$ is $\mathbb{G}$.

2.2. Definition of HIBE systems

Hierarchical Identity Based Encryption (HIBE). A HIBE system is a tuple of five algorithms $\Pi_{HIBE} = (Setup, Extract, Derive, Encrypt, Decrypt)$. The root PKG runs the *Setup* algorithm to output public and private parameters for HIBE setting, including a bilinear pairing as HIBE context, public parameters and master key only known to the root PKG (at level 0). The *Extract* algorithm generates private keys for all identities in hierarchy with master key, public parameters and identities as input, and distributes private keys to their owners via trusted channel. Algorithm Derive functions alike to Extract. It is used by ancestor entities to generate private keys for their descendants, or delegate private keys along hierarchy. The Encrypt algorithm encrypts a message on the intended recipient's identity. Algorithm Decrypt uses the intended recipient's private key to decrypt a ciphertext.

2.3. Complexity Assumptions

Decisional BDH. The Decisional Bilinear Diffie-Hellman (DBDH) problem in asymmetric bilinear pairing $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_t, e)$ is to output 1 (yes) with 7-tuple $(g, ag, cg, \hat{g}, a\hat{g}, b\hat{g}, T) \in \mathbb{G}^3 \times \hat{\mathbb{G}}^3 \times \mathbb{G}_t$ as input if T equals $e(g, \hat{g})^{abc}$, and output 0 (no) otherwise, for some $a, b, c \in_R \mathbb{Z}_q^*$ and $T \in_R \mathbb{G}_t$. The advantage of any probabilistic polynomial-time (PPT) algorithm $\mathbb{B}$ in solving DBDH problem in $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_t, q, e)$ is defined as

$$Adv^{DBDH}_{e:\mathbb{G}\times\hat{\mathbb{G}}\to\mathbb{G}_t,\mathbb{B}} = \left|\Pr\left[\mathbb{B}(g, ag, cg, \hat{g}, a\hat{g}, b\hat{g}, e(g,\hat{g})^{abc}) = 1\right]\right.$$

$$\left. - \Pr\left[\mathbb{B}(g, ag, cg, \hat{g}, a\hat{g}, b\hat{g}, T) = 1\right]\right|,$$

where the probability is over the random generators g of $\mathbb{G}$ and $\hat{g}$ of $\hat{\mathbb{G}}$, random choices of exponents a, b and c in $\mathbb{Z}_q$, random choice of T in $\mathbb{G}_t$, and random bits used by $\mathbb{B}$. We say that algorithm $\mathbb{B}$ has advantage ε in solving DBDH problem in $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_t, q, e)$ if $Adv^{DBDH}_{e:\mathbb{G}\times\hat{\mathbb{G}}\to\mathbb{G}_t,\mathbb{B}} \geq \varepsilon$.

Definition 2. ***Decisional BDH Assumption****. If there is no t-time algorithm $\mathbb{B}$ that has advantage at least ε in solving decisional BDH problem in asymmetric pairing $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_t, q, e)$, then the (t, ε)-Decisional BDH assumption holds. For simplicity, Decisicional BDH assumption holds if for every PPT algorithm $\mathbb{B}$, $Adv^{DBDH}_{e:\mathbb{G}\times\hat{\mathbb{G}}\to\mathbb{G}_t,\mathbb{B}}$ is negligible.*

3. Our HIBE Construction

An HIBE scheme is a tuple of five algorithms $\Pi_{HIBE} = (Setup, Extract, Derive, Encrypt, Decrypt)$. We now present our HIBE construction of maximum hierarchy

depth ℓ with authorized delegation being. We opt to construct the system in more general asymmetric bilinear pairing $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_t, q, e)$. Our construction is applicable to symmetric bilinear pairing also, and can be easily converted by discarding all hats from the symbols. As for needed preliminaries and definitions of bilinear pairing, DBDH assumption, notions of IND-sID-CPA and IND-sID-CCA2, (t, q_{ID}, ε) -IND-sID-CPA HIBE system and so on, we refer the reader to [5] for more details.

3.1. Construction

• Setup$(\mathbf{1^k}, \ell) \rightarrow$ **{(**$\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_t$**, e), params, mk}**: takes the security parameters 1^k and the maximum hierarchy depth ℓ as input, and outputs a description of asymmetric bilinear pairing $(q, \mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_t, e, g, \hat{g})$, where $q \geq 2^k$, $\mathbb{G}$, $\hat{\mathbb{G}}$, $\mathbb{G}_t$ are all of prime q order with generators g, $\hat{g}$ and $e(g, \hat{g})$ respectively; picks two random numbers α and β from $\mathbb{Z}_q$, sets $g_1 = \alpha g$, $\hat{g}_1 = \alpha \hat{g}$ and $\hat{g}_0 = \alpha\beta\hat{g}$, and calculates $v = e(g, \hat{g}_0) = e(g, \hat{g})^{\alpha\beta}$; randomly selects ℓ numbers $\delta_1, \ldots, \delta_\ell$ from $\mathbb{Z}_q$, and sets $h_i = \delta_i g$ and $\hat{h}_i = \delta_i \hat{g}$ for each $i = 1, \ldots, \ell$; outputs public system parameters $params \in \mathbb{G}^{\ell+2} \times \hat{\mathbb{G}}^{\ell+2} \times \mathbb{G}_t$ and the master secret $mk \in \hat{\mathbb{G}}$ as

$$params = (g, g_1, h_1, \ldots, h_\ell, \hat{g}, \hat{g}_1, \hat{h}_1, \ldots, \hat{h}_\ell, v),$$
$$mk = (\hat{g}_0).$$

• Extract$(\mathbf{mk, params, ID_j}) \rightarrow (\mathbf{d_0^{(ID_j)}}, \mathbf{RD_1^{(ID_j)}}, \ldots, \mathbf{RD_j^{(ID_j)}})$ (denoted d_{ID_j}): takes identity $ID_j = (I_1, \ldots, I_j) \in (\mathbb{Z}_q^*)^j$ ($j \leq \ell$), mk and $params$ as input, picks j random numbers $r_1, \ldots, r_j$ from $\mathbb{Z}_q$, and generates a private key $d_{ID_j} \in \hat{\mathbb{G}}^{j+1}$ for ID_j as

$$\left(\hat{g}_0 + \sum_{k=1}^{j-1} r_k \left((I_k - I_j)\hat{g}_1 + \hat{h}_k \right) + r_j (I_j \hat{g}_1 + \hat{h}_j), r_1 \hat{g}, \ldots, r_j \hat{g} \right), \quad (1)$$

where $\hat{g}_0$ is the origin of the privacy, and $\sum_{k=1}^{j} r_k (I_k \hat{g}_1 + \hat{h}_k)$ randomizes $\hat{g}_0$ to create global privacy pertaining to hierarchy $I_1 \rightarrow \ldots \rightarrow I_j$, while $-\sum_{k=1}^{j-1} r_k I_j \hat{g}_1$ defines the dedicated privacy specific to ID_j on local identifier I_j with random values $r_1, \ldots, r_{j-1}$ corresponding to $I_1, \ldots, I_{j-1}$ in defining global privacy.

• Derive$(\mathrm{i}, \mathrm{ID_j}, \mathrm{S_{(i,ID_j)}}) \rightarrow \mathrm{S_{(i+1,ID_j)}}$. The authorized entity being informed the needed information by the root PKG can derive private keys for some of its descendants with algorithm Derive. Algorithm Derive takes as input an index i, an identity $ID_j = (I_1, \ldots, I_j)$, and a secret $S_{(i,ID_j)} \in \hat{\mathbb{G}}^{j+1}$ for identity $ID_j[1:i]$, and outputs a secret for identity $ID_j[1:i+1]$, where i is used to specify the identity as a prefix of ID_j to which

$S_{(i,ID_j)}$ belongs, $ID_j[1:k]$ $(1 \le k \le j)$ is an identity of depth k and a prefix of ID_j, and $ID_j[1:j]$ is ID_j. $S_{(i,ID_j)}$ is a secret specific to identity pair ($ID_j[1:i]$, ID_j), which is used to derive secrets specific to identity pairs ($ID_j[1:i+1]$, ID_j), …, ($ID_j[1:j]$, ID_j). How the root PKG composes secret $S_{(i,ID_j)}$ is detailed in Section 4.

Let $S_{(i,ID_j)} = (S_0^{(i,ID_j)}, RD_1^{(i,ID_j)}, \ldots, RD_j^{(i,ID_j)})$ be secret specific to the identity pair ($ID_j[1:i]$, ID_j), then secret $S_{(i+1,ID_j)} \in \hat{G}^{j+1}$ corresponding to ($ID_j[1:i+1]$, ID_j) is calculated as follows.

- If $i+1$ is less than j, to derive $S_{(i+1,ID_j)}$ with using $S_{(i,ID_j)}$, pick $i+1$ random numbers $r_1, \ldots, r_{i+1}$ from $\mathbb{Z}_q$, and output

$$\Big(S_0^{(i,ID_j)} + \sum_{k=1}^{i+1} r_k \left((I_k - I_j)\hat{g}_1 + \hat{h}_k \right), RD_1^{(i,ID_j)} + r_1\hat{g}, \ldots, RD_{i+1}^{(i,ID_j)} + r_{i+1}\hat{g}, RD_{i+2}^{(i,ID_j)}, \ldots, RD_j^{(i,ID_j)} \Big). \quad (2)$$

- If $i+1$ equals j, $S_{(j,ID_j)}$ is calculated by randomizing $S_{(j-1,ID_j)}$ with j random numbers $r_1, \ldots, r_j$ from $\mathbb{Z}_q$ as

$$\Big(S_0^{(j-1,ID_j)} + \sum_{k=1}^{j-1} r_k \left((I_k - I_j)\hat{g}_1 + \hat{h}_k \right) + r_j \left(I_j\hat{g}_1 + \hat{h}_j \right), RD_1^{(j-1,ID_j)} + r_1\hat{g}, RD_j^{(j-1,ID_j)} + r_j\hat{g} \Big), \quad (3)$$

where the secret $S_{(j,ID_j)}$ is a private key for identity ID_j as defined in (1).

• Encrypt$(\mathbf{params, ID_j, M}) \rightarrow (\mathbf{C_0^{(ID_j)}, C_1^{(ID_j)}, RE_1^{(ID_j)}, \ldots, RE_j^{(ID_j)}})$ (denoted C_{ID_j}). To encrypt a given message $M \in \mathbb{G}_t$ on identity $ID_j = (I_1, \ldots, I_j) \in (\mathbb{Z}_q^*)^j$, the Encrypt algorithm picks a random value $s \in \mathbb{Z}_q^*$ and outputs the ciphertext $C_{ID_j} \in \mathbb{G}_t \times \mathbb{G}^{j+1}$ as

$$(Mv^s, sg, s\left((I_1 - I_j)g_1 + h_1\right), \ldots, s\left((I_{j-1} - I_j)g_1 + h_{j-1}\right), s(I_j g_1 + h_j)). \quad (4)$$

• Decrypt$(\mathbf{params, d_{ID_j}, C_{ID_j}}) \rightarrow \mathbf{M}$. To decrypt ciphertext C_{ID_j} encrypted on $ID_j = (I_1, \ldots, I_j)$, algorithm Decrypt uses private key d_{ID_j} for ID_j, and calculates a message M as

$$\left(C_0^{(ID_j)}\prod_{k=1}^{j}e\left(RE_k^{(ID_j)},RD_k^{(ID_j)}\right)\right)/e\left(C_1^{(ID_j)},d_0^{(ID_j)}\right) \quad (5)$$

3.2. Correctness

With private key d_{ID_j} for $ID_j=(I_1,\ldots,I_j)$ extracted as in (1) and a ciphertext C_{ID_j} encrypted on ID_j as in (4), $\prod_{k=1}^{j}e(RE_k^{(ID_j)},RD_k^{(ID_j)})$ is calculated as

$$\begin{aligned}&\prod_{k=1}^{j-1}e\left(s\left((I_k-I_j)g_1+h_k\right),r_k\hat{g}\right)\cdot e\left(s(I_jg_1+h_j),r_j\hat{g}\right)\\&=e\left(sg,\sum_{k=1}^{j-1}r_k\left((I_k-I_j)\hat{g}_1+\hat{h}_k\right)+r_j(I_j\hat{g}_1+\hat{h}_j)\right)\\&=e\left(C_1^{(ID_j)},d_0^{(ID_j)}-\hat{g}_0\right)\end{aligned}$$

That is, our HIBE system is consistent.

4. Authorized Delegation: Secret Derivation along Imaginary Identity Hierarchy

Different from previous constructions [12][1][5] where unlimited delegation is possible, and constructions [6][15] with limited delegation, where private keys for descendants of limited depth can be derived, any entity is unable to derive valid private keys for its descendants in our construction with only knowledge of its private key and some public information, including system parameters and identities of descendants, such as by randomizing its private key along the hierarchy.

Let Δd_0 be the difference of first components of private keys $d_{ID_{j+1}}$ and d_{ID_j} for ID_{j+1} and ID_j respectively, Δd_0 is calculated as

$$\begin{aligned}\Delta d_0 &= \sum_{k=1}^{j}\left(r_k^{(ID_{j+1})}-r_k^{(ID_j)}\right)\left(I_k\hat{g}_1+\hat{h}_k\right)\\&\quad+r_{j+1}^{(ID_{j+1})}\left(I_{j+1}\hat{g}_1+\hat{h}_{j+1}\right)\\&\quad+I_j\hat{g}_1\sum_{k=1}^{j-1}r_k^{(ID_j)}-I_{j+1}\hat{g}_1\sum_{k=1}^{j}r_k^{(ID_{j+1})}.\end{aligned}$$

Let's consider the simplest case that $r_k^{(ID_{j+1})}$ equals $r_k^{(ID_j)}$ for each $k\in\{1,\ldots,j\}$, then

$$\begin{aligned}\Delta d_0 &= r_{j+1}^{(ID_{j+1})}\left(I_{j+1}\hat{g}_1+\hat{h}_{j+1}\right)\\&\quad-\left(I_{j+1}\hat{g}_1\sum_{k=1}^{j}r_k^{(ID_j)}-I_j\hat{g}_1\sum_{k=1}^{j-1}r_k^{(ID_j)}\right).\end{aligned}$$

Obviously, at least both values of $\sum_{k=1}^{j} r_k^{(ID_j)} \hat{g}_1$ and $\sum_{k=1}^{j-1} r_k^{(ID_j)} \hat{g}_1$ can be calculated, it is possible to derive $d_{ID_{j+1}}$ with d_{ID_j} through randomization. The truth is the two required values is unavailable with only knowledge of private key for ID_j as defined in (1).

Our construction does provide a means for the root PKG to authorize an entity to be capable of deriving private keys for any of its descendants through randomization along a virtual identity hierarchy specific to identity of the descendant. Virtual here means that an imaginary identity is constructed from the real identity for which privilege of generating private keys is delegated.

Definition 3. An imaginary identity $ID_{k|Im(ID_j)} \in (\mathbb{Z}_q)^k$ for each k in $\{1,\ldots, j\}$ related to true identity $ID_j = (I_1, \ldots, I_j) \in (\mathbb{Z}_q^*)^j$ in HIBE is defined as

$$ID_{k|Im(ID_j)} = \left(I_{1|Im(ID_j)},\ldots, I_{k|Im(ID_j)}\right), \tag{6}$$

where $I_{k|Im(ID_j)}$ is $I_k - I_j$ for each $k \in \{1,\ldots, j-1\}$, and $I_{j|Im(ID_j)}$ is I_j.

With definition of Imaginary Identity above, a private key for identity ID_j expressed in (1) can be rephrased as

$$d_{ID_j} = \left(\hat{g}_0 + \sum_{k=1}^{j} r_k \left(I_{k|Im(ID_j)} \hat{g}_1 + \hat{h}_k\right), r_1 \hat{g}, \ldots, r_j \hat{g} \right) \in \hat{\mathbb{G}}^{j+1}. \tag{7}$$

Therefore, the root PKG can authorize an ancestor of Entity$_j$ with identity ID_j, Entity$_i$ at depth i with identity $ID_i = ID_j[1:i]$ which is prefix of ID_j, to be capable of generating private keys for ID_j through randomization along virtual hierarchy $I_{1|Im(ID_j)} \rightarrow \ldots I_{i|Im(ID_j)} \rightarrow \ldots I_{j|Im(ID_j)}$ by distributing Entity$_i$ a secret corresponding to $ID_{i|Im(ID_j)}$ (or specific to identity pair (ID_i, ID_j)) as

$$S_{(i,ID_j)} = (\hat{g}_0 + r_j^{(i,ID_j)} \left(I_{j|Im(ID_j)} \hat{g}_1 + \hat{h}_j\right) + \sum_{k=1}^{i} r_k^{(i,ID_j)} \left(I_{k|Im(ID_j)} \hat{g}_1 + \hat{h}_k\right),$$

$$r_1^{(i,ID_j)} \hat{g}, \ldots, r_i^{(i,ID_j)} \hat{g}, 0, \ldots, 0, r_j^{(i,ID_j)} \hat{g}) \in \hat{\mathbb{G}}^{j+1}, \tag{8}$$

where $r_j^{(i,ID_j)} (I_j \hat{g}_1 + \hat{h}_j)$ is required for restricting the entity being authorized to derive private keys only for the descendant at depth j of which local identifier is I_j, and $r_k^{(i,ID_j)}$ for k in $\{1,\ldots,i\} \cup \{j\}$ are random numbers in $\mathbb{Z}_q$.

Actually, the root PKG does not need to additionally distribute secret $S_{(i,ID_j)}$ to Entity$_i$ in addition to distributing private key $d_{ID_i} = (\hat{g}_0 + \sum_{k=1}^{i} r_k (I_k \hat{g}_1 + \hat{h}_k) - \sum_{k=1}^{i-1} r_k I_i \hat{g}_1, r_1 \hat{g}, \ldots, r_i \hat{g})$; a two-tuple below is distributed as authorization credential

to Entity$_i$, with which a secret $S_{(i,ID_j)}$ is constructed by updating d_{ID_i}. The two-tuple specific to identity pair (ID_i, ID_j) is

$$\left(r_j \hat{g}, I_i \sum_{k=1}^{i-1} r_k \hat{g}_1 - I_j \sum_{k=1}^{i} r_k \hat{g}_1 + r_j (I_j \hat{g}_1 + \hat{h}_j) \right).$$

where r_k for $k = 1, \ldots, i$ are random values used in extracting d_{ID_i}, and r_j is a newly selected random number from $\mathbb{Z}_q$.

$S_{(i,ID_j)}$ is neither a private key for $ID_i = (I_1, \ldots, I_i)$, nor a private key for $ID_{i|Im(ID_j)} = (I_{1|Im(ID_j)}, \ldots, I_{i|Im(ID_j)})$, but a private value for $ID_{i|Im(ID_j)}$ that can only be used to derive secrets $S_{(i+1,ID_j)}$, …, $S_{(j,ID_j)}$ for $ID_{i+1|Im(ID_j)}$, …, $ID_{j|Im(ID_j)}$ hierarchically along $I_{1|Im(ID_j)} \rightarrow \ldots \rightarrow I_{j|Im(ID_j)}$. Specifically, with algorithm Derive (Section 3.1), the entity being authorized with a secret $S_{(i,ID_j)}$ can hierarchically randomized the secret to derive a secret $S_{(j,ID_j)}$ for $ID_{j|Im(ID_j)}$ which is a private key for identity ID_j.

5. Selective-Message HIBS Construction

In this section, we build a selectively secure HIBS scheme against adaptive chosen-message attacks in the standard model from the selective identity secure HIBE construction in Section 3 based on Naor transformation. As of selectively secure signature [5], the adversary is required to announce the message on which it intends to forge a signature prior to HIBS setting being set by the challenger, which reduces security analysis of HIBS to that of HIBE.

5.1. Construction

Our HIBS scheme is a 4-tuple of algorithms $\Pi_{HIBS} = (Setup, Extract, Sign, Verify)$ defined as follows.

• Setup$(\mathbf{1^k}, \ell) \rightarrow$ **Λ, params, mk}**. As defined in HIBE constrution in Section 3.1.

• Extract$(\mathbf{mk, params, ID_j}) \rightarrow (\mathbf{s_0^{(ID_j)}, s_1^{(ID_j)}, SD_1^{(ID_j)}}, \ldots, \mathbf{SD_{j+1}^{(ID_j)}})$ (denoted SK_{ID_j}): takes identity $ID_j = (I_1, \ldots, I_j) \in (\mathbb{Z}_q^*)^j$ ($j \le \ell - 1$), *mk* and *params* as input, picks $j+1$ random numbers r_1, …, r_j from $\mathbb{Z}_q$ and r_{j+1} from $\mathbb{Z}_q^*$, and generates a signing key $SK_{ID_j} \in \hat{\mathbb{G}}^{j+3}$ for ID_j as

$$\left(\hat{g}_0 + \sum_{k=1}^{j} r_k \left(I_k \hat{g}_1 + \hat{h}_k \right) + r_{j+1} \hat{h}_{j+1}, (r_{j+1} - \sum_{k=1}^{j} r_k) \hat{g}_1, r_1 \hat{g}, \ldots, r_{j+1} \hat{g} \right), \quad (9)$$

• Sign $(\mathbf{params, ID_j, SK_{ID_j}, M}) \rightarrow (\mathbf{d_0^{(ID_j|M)}, RD_1^{(ID_j|M)}}, \ldots, \mathbf{RD_{j+1}^{(ID_j|M)}})$ (denoted $\sigma_{(M,ID_j)}$). To sign a message $M \in \mathbb{Z}_q$ (however, the message space is $\mathbb{G}_t$ in HIBE) under identity $ID_j = (I_1, \ldots, I_j) \in (\mathbb{Z}_q^*)^j$ with signing key

$SK_{ID_j} = (s_0^{(ID_j)}, s_1^{(ID_j)}, SD_1^{(ID_j)}, \ldots, SD_{j+1}^{(ID_j)})$, the signer randomly selects $j+1$ random values r_1, …, r_{j+1} from $\mathbb{Z}_q$, and generates a signature $\sigma_{(m,ID_j)}$ being a private key in HIBE for identity $ID_j \| M$ as

$$\left(s_0^{(ID_j)} + Ms_1^{(ID_j)} + \sum_{k=1}^{j} r_k \left((I_k - M)\hat{g}_1 + \hat{h}_k \right) + r_{j+1}(M\hat{g}_1 + \hat{h}_{j+1}), \right.$$

$$\left. SD_1^{(ID_j)} + r_1\hat{g}, \ldots, SD_{j+1}^{(ID_j)} + r_{j+1}\hat{g} \right). \quad (10)$$

• Verify $\mathbf{(params, ID_j, M, \sigma)} \rightarrow 1$ or 0. To verify a message-signature (M, σ) pair under $ID_j = (I_1, \ldots, I_j)$, the Verify algorithm first picks a random value $s \in \mathbb{Z}_q^*$ and outputs the verification credential $VC_{ID_j \| M} = (v_0^{(ID_j \| M)}, v_1^{(ID_j \| M)}, VE_1^{(ID_j \| M)}, \ldots, VE_{j+1}^{(ID_j \| M)}) \in \mathbb{G}_t \times \mathbb{G}^{j+2}$ as

$$(v^s, sg, s((I_1 - M)g_1 + h_1), \ldots, s((I_j - M)g_1 + h_j), s(Mg_1 + h_{j+1})), \quad (11)$$

parses σ as $(d_0, RD_1, \ldots, RD_{j+1})$, and checks the following equality,

$$e\left(c_1^{(ID_j \| M)}, d_0\right) = v_0^{(ID_j \| M)} \prod_{k=1}^{j+1} e\left(VE_k^{(ID_j \| M)}, RD_k\right) \quad (12)$$

If the equality follows, which implies that the signature σ is a valid signature of the identity ID_j on message M, algorithm *Verify* returns 1 or 0, otherwise.

5.2. Signing Key vs. Private Key

Actually, the root PKG does not need to generate a signing key SK_{ID_j} from scratch and distribute it to Entity $_j$ independently with respect to the generation and distribution of private key d_{ID_j} for ID_j.

Because signature $\sigma_{(\mathrm{M},ID_j)}$ is a private key for identity $ID_j \| \mathrm{M}$ actually, the first element of a private key for $ID_j \| \mathrm{M}$ is represented as,

$$d_0^{(ID_j \| \mathrm{M})} = \hat{g}_0 + \sum_{k=1}^{j} r_k (I_k \hat{g}_1 + \hat{h}_k) + r_{j+1}\hat{h}_{j+1} + (r_{j+1} - \sum_{k=1}^{j} r_k)\mathrm{M}\hat{g}_1$$

where M is a placeholder for messages intended to be signed under ID_j, and r_1, …, r_{j+1} are random values in $\mathbb{Z}_q$ with restriction that r_{j+1} cannot be zero.

With reference to Eqn. (1) and Eqn. (9), an intermediate secret can be generated by the PKG for updating a private key for ID_j to compose a signing key for ID_j. Let $d_{ID_j} = (d_0^{(ID_j)}, RD_1^{(ID_j)}, \ldots, RD_j^{(ID_j)})$ be a private key for ID_j, r_1, …, r_j be random values as defined in (1), and r_{j+1} a newly selected random value from $\mathbb{Z}_q^*$, it is no hard for

the root PKG to conclude a intermediate secret $IS_{ID_j} = (IS_0^{(ID_j)}, IS_1^{(ID_j)}, IS_2^{(ID_j)})$ as follows,

$$(\sum_{k=1}^{j-1} r_k I_j \hat{g}_1 + r_{j+1}\hat{h}_{j+1}, (r_{j+1} - \sum_{k=1}^{j} r_k)\hat{g}_1, r_{j+1}\hat{g}), \tag{13}$$

and a signing key SK_{ID_j} for ID_j can be generated by updating private key d_{ID_j} for ID_j with the secret IS_{ID_j} as

$$SK_{ID_j} = (d_0^{(ID_j)} + IS_0^{(ID_j)}, IS_1^{(ID_j)}, RD_1^{(ID_j)}, \ldots, RD_j^{(ID_j)}, IS_2^{(ID_j)}). \tag{14}$$

6. Conclusion

As far as identity based cryptosystems are concerned, it is rational to viewed the root PKG as a trusted party or being unconditionally trusted, but those level PKGs should be treated suspiciously in hierarchical identity based setting. On the other word, from a security point of view, convention that level PKGs, being able to derive private keys for their descendants, are capable of decrypting or signing on behalf of their descendants is unjustifiable from the beginning.

In order to resolve key escrow problem in HIBE schemes, Identifier Discrimination technique is proposed in this paper, and a selective identity secure HIBE system is constructed. With the technique, any entity is not capable of deriving private keys for its descendants with only knowledge of its private key, thus preventing the entity from behaving (decrypting, signing and so on) on behalf of its descendants, and key delegation is fullfilled through independent authorization per descendant (authorized delegation).

Different from IBS schemes constructed from HIBE schemes with unlimited delegation (and also limited delegation), where the private key for an identity is the certain signing key for the identity, the HIBS scheme constructed in this paper is logically independent to the HIBE scheme from which it is built, *i.e.*, the signing key is independent to the private key for an identical identity.

References

[1] D. Boneh and X. Boyen, "Efficient selective-id secure identity-based encryption without random oracles", In: Cachin, C., Camenisch, J. (eds.) Advances in Cryptology - EUROCRYPT 2004, LNCS, Springer Berlin Heidelberg, vol. 3027, **(2004)**, pp. 223–238.

[2] D. Boneh and X. Boyen, "Secure identity based encryption without random oracles", In: Franklin, M. (ed.) Advances in Cryptology - CRYPTO 2004, LNCS, Springer Berlin Heidelberg, vol. 3152, **(2004)**, pp. 443–459.

[3] D. Boneh and X. Boyen, "Short signatures without random oracles", In: Cachin, C., Camenisch, J. (eds.) Advances in Cryptology - EUROCRYPT 2004, LNCS, Springer Berlin Heidelberg, vol. 3027, **(2004)**, pp. 56–73.

[4] D. Boneh and X. Boyen, "Short signatures without random oracles and the sdh assumption in bilinear groups", Journal of Cryptology, vol. 21, no. 2, **(2007)**, pp. 149–177.

[5] D. Boneh and X. Boyen, "Efficient selective identity-based encryption without random oracles", Journal of Cryptology, vol. 24, no. 4, **(2011)**, pp. 659–693.

[6] D. Boneh, X. Boyen and E. J. Goh, "Hierarchical identity based encryption with constant size ciphertext", In: Cramer, R. (ed.) Advances in Cryptology - EUROCRYPT 2005, LNCS, Springer Berlin Heidelberg, vol. 3494, **(2005)**, pp. 440–456.

[7] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing", SIAM J. Comput., vol. 32, no. 3, **(2003)**, pp. 586–615.

[8] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing", In: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, CRYPTO'01, Springer-Verlag, London, UK, UK, **(2001)**, pp. 213–229.

[9] D. Boneh, B. Lynn and H. Shacham, "Short signatures from the weil pairing", Journal of Cryptology, vol. 17, no. 4, **(2004)**, pp. 297–319.
[10] C. Cocks, "An identity based encryption scheme based on quadratic residues", In: Honary, B. (ed.) Proceedings of the 8th IMA International Conference on Cryptography and Coding, LNCS, Springer Berlin Heidelberg, vol. 2260, **(2001)**, pp. 360–363.
[11] Y. Desmedt and J. J. Quisquater, "Public-key systems based on the difficulty of tampering (is there a difference between des and rsa?)", In: Proceedings on Advances in cryptology—CRYPTO'86, Springer-Verlag, London, UK, UK. **(1987)**, pp. 111–117.
[12] C. Gentry and A. Silverberg, "Hierarchical id-based cryptography", In: Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, ASIACRYPT'02, Springer-Verlag, London, UK, UK. **(2002)**, pp. 548–566.
[13] F. Hess, "Efficient identity based signature schemes based on pairings", In: Nyberg, K., Heys, H. (eds.) Selected Areas in Cryptography, Lecture Notes in Computer Science, Springer Berlin Heidelberg, vol. 2595, **(2003)**, pp. 310–324.
[14] J. Horwitz and B. Lynn, "Toward hierarchical identity-based encryption", In: Knudsen, L. (ed.) Advances in Cryptology - EUROCRYPT 2002, LNCS, Springer Berlin Heidelberg, vol. 2332, **(2002)**, pp. 466–481.
[15] A. Lewko and B. Waters, "New techniques for dual system encryption and fully secure hibe with short ciphertexts", In: Micciancio, D. (ed.) Theory of Cryptography, LNCS, Springer Berlin Heidelberg, vol. 5978, **(2010)**, pp. 455–479.
[16] K. Paterson, "Id-based signatures from pairingson elliptic curves", Electronics Letters 38, no. 1, **(2002)**, pp. 1025–1026.
[17] K. O. Ryuichi Sakai and M. Kasahara, "Cryptosystems based on pairings", Symposium on Cryptography and Information Security 2000 - SCIS2000, **(2000)**.
[18] A. Shamir, "Identity-based cryptosystems and signature schemes", In: Blakley, G., Chaum, D. (eds.) Advances in Cryptology, LNCS, Springer Berlin Heidelberg, vol. 196, **(1985)**, pp. 47–53.
[19] H. Tanaka, "A realization scheme for the identity-based cryptosystem", In: A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology, CRYPTO'87, Springer-Verlag, London, UK, UK. **(1988)**, pp. 340–349.
[20] S. Tsujii and T. Itoh, "An id-based cryptosystem based on the discrete logarithm problem", Selected Areas in Communications, IEEE Journal on, vol. 7, no. 4, **(1989)**, pp. 467–473
[21] B. Waters, "Efficient identity-based encryption without random oracles", In: Cramer, R. (ed.) Advances in Cryptology - EUROCRYPT 2005, LNCS, Springer Berlin Heidelberg, vol. 3494, **(2005)**, pp. 114–127.
[22] B. Waters, "Dual system encryption: Realizing fully secure ibe and hibe under simple assumptions", In: Halevi, S. (ed.) Advances in Cryptology - CRYPTO 2009, LNCS, Springer Berlin Heidelberg, vol. 5677, **(2009)**, pp. 619–636.

Authors

Jian-Wu Zheng, received the B.E. and M.E. degrees from Fuzhou University, China, in 1995 and 1998 respectively. He is currently an Associate Professor with the School of Transportation, Shijiazhuang Tiedao University, China. His current research interests include applied cryptography, security and privacy in wireless networks and VANETs.

Jing Zhao, received the B.E. degree from Hebei Institute of Science and Technology, China, in 1996, and M.E degree from Fuzhou University, China, in 1996 respectively. She is currently an Associate Professor with the Collaborative Innovation Center, Shijiazhuang Tiedao University, China. Her current research interests are Internet of Things, wireless network security and complex systems.

Xin-Ping Guan, received the Ph.D. degree in control and systems from the Harbin Institute of Technology, Harbin, China, in 1999. In 2007, he joined the Department of Automation, Shanghai Jiao Tong University, Shanghai, China, where he is currently a Distinguished University Professor, and the Director of the Key Laboratory of Systems Control and Information Processing with the Ministry of Education, Beijing, China. His current research interests include cyber-physical systems, multiagent systems, wireless networking and applications in smart city and smart factory, and underwater sensor networks.