International Journal of Security and Its Applications
Vol. 10, No. 8 (2016), pp.225-238
http://dx.doi.org/10.14257/ijsia.2016.10.8.20

Differentiating Technique: Constructing Efficient HIBE with Constant Size Ciphertext and Authorized Delegation

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

As Hierarchical Identity Based Encryption (HIBE) system usually maps the true institutional structure of an organization or entity relationship between objects in real world, It is important that computation & communication complexity of private key, ciphertext, cryptographic computations and so on related to an entity in the hierarchy is independent to the hierarchy depth of the entity. Moreover, key escrow problem that any non-leaf entity in a hierarchical identity based cryptosystem can derive private keys for its descendants with use of its private key should be resolved, in order to prevent any entity from behaving on behalf of its descendants. In this paper, a new technique is introduced for composing a private key for each individual entity in HIBE system by differentiating between non-local identifiers and local identifiers of the identity of the entity. That we call Identifier Discrimination. With the technique, A selective identity secure HIBE system is constructed under Decisional Bilinear Diffie-Hellman (DBDH) assumption without using random oracles, where the private key and the ciphertext consist of constant number of group elements, and decryption requires only three bilinear map computations, regardless of the identity hierarchy depth. Moreover, in contrast to previous HIBE constructions, where private key for an entity can be derived by its ancestors with direct use of their private keys, key escrow problem inherent in identity based cryptosystems is resolved in our HIBE construction. Privilege of deriving private keys for an entity can be delegated to any of its ancestors through authorization by distributing specifically crafted values to the ancestor in our HIBE system, that we call Authorized Delegation.

Keywords*: Identity-Based Encryption, Bilinear Diffie-Hellman Assumption, Constant Size Ciphertext, Identifier Discrimination, Authorized Delegation*

1. Introduction

An Identity Based Encryption (IBE) system [6,5] 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 IBE, there are no usable IBE constructions until the works by Boneh and Franklin [5] and Cocks [6]. Cocks built an IBE scheme from Quadratic Residuosity, while Boneh and Frankin constructed their IBE scheme from bilinear pairing, which has ignited a storm of research interest in building identity based cryptosystems from pairings.

Hierarchical Identity Based Encryption (HIBE) [8,7,1] is a generalization of IBE [6] [5] that maps institution structure or entity relationship in real world. Gentry and Silverberg [7] presented the first HIBE construction in the random oracle model. Boneh and Boyen [1,3] introduced a selective identity, chosen-plaintext (IND-sID-CPA) secure

ISSN: 1738-9976 IJSIA

HIBE scheme BB_1 under Decisional Bilinear Diffie-Hellman (DBDH) assumption in standard model. Later, works by Boneh *et. al.,* [2,4], Waters [10,11] and Lewko *et. al.,* [9] provided some fully secure schemes without random oracles.

1.1. Problem Formulation

Efficiency of HIBE systems. Different from One-PKG characterized Identity Based Encryption (IBE) system, where the unique PKG manages only one level of identities, Hierarchical IBE (HIBE) system accommodates level-oriented PKG configuration, where the root PKG (at level zero) maintains a hierarchy tree of which non-leaf nodes are level PKGs, and entities should be treated differently from logically hierarchical relationship point of view. Although, an entity at upper-level may have certain privileges than the other entity at lower-level in the hierarchy with respect to the institution structure they should respect, there should be no difference in requirements challenging entities at different hierarchy levels in HIBE system, such as computation complexity, communication complexity, capability assumption (such as using random bits) and so on, as far as completing cryptographic computations and related operations are concerned. In previous constructions [7,3,11], size of private keys and ciphertexts grows linearly in identity hierarchy depth, and decryption time consequently keeps linearly with the hierarchy depth.

Key Escrow Problem. Furthermore, in identity based cryptosystems, any identity's private key (despite of its usage, *e.g.*, decryption or signing) can be generated by the root PKG being with the knowledge of the master key, then the root PKG can recover messages being encrypted under arbitrary identities valid in the hierarchy, generate signatures of any identity on arbitrary messages and so on. Moreover, non-leaf entities in hierarchical context being as level PKGs are usually capable of deriving private keys for their descendants, non-leaf-entities can therefore behave (decrypt or sign) on the behalf of their arbitrary descendants. This is called inherent key escrow problem of IBC [7].

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 context. It is therefore important to restrict the power of level PKGs from being able to derive private keys for their descendants, and decrypting or signing on behalf of their descendants.

1.2. Related Work

Reducing Complexity of Computation and Communication. A HIBE system should be efficient enough in dealing with cryptographic operations to be useful and practical. Particularly, key information such as public and private key pair and ciphertext should be frugal in consuming storage space, and encryption and decryption should be efficient in finishing related cryptographic computations.

As for BB^1 system presented in [3], to encrypt a given message $M \in \mathbb{G}_T$ (image group of the bilinear pairing $\Lambda = (\mathbb{G}, \mathbb{G}_1, \mathbb{G}_T, q, e)$) on Entity j 's identity $ID_j = (I_1, \ldots, I_j) \in (\mathbb{Z}_q^*)^j$, pick a random number $s \in \mathbb{Z}_q^*$, output tuple below as resulted ciphertext,

$$C = \left(Mv^s, sg, s(I_1 g + h_1), \ldots, s(I_j g + h_j)\right) = \left(C_0, C_1, RE_1, \ldots, RE_j\right) \in \mathbb{G}_T \times \mathbb{G}^{j+1}.$$

Moreover, private key for Entity j is expressed as:

$$d_{ID_j} = \left(\hat{g}_0 + \sum_{k=1}^{j} r_k (I_k \hat{g}_1 + \hat{h}_k), r_1 \hat{g}, \ldots, r_j \hat{g} \right) = \left(d_0, RD_1, \ldots, RD_j \right) \in \hat{\mathrm{G}}^{j+1}.$$

The length of private key and ciphertext grows linearly in hierarchy depth of the identity. For entities at lower levels, they are challenged by more tasks of dealing with more components in private keys and ciphertexts compared to entities at upper levels, thus putting them at a disadvantage. Furthermore, the ciphertext C_{ID_j} is decrypted with private key for Entity j as:

$$M' = C_0 \cdot \frac{\prod_{k=1}^{j} e(RE_k, RD_k)}{e(C_1, d_0)} = C_0 \cdot \frac{\prod_{k=1}^{j} e\left(s(I_k g_1 + h_k), r_k \hat{g}\right)}{e\left(sg, \hat{g}_0 + \sum_{k=1}^{j} r_k \left(I_k \hat{g}_1 + \hat{h}_k\right)\right)} = M,$$

which indicates that time needed for decryption (the number of needed bilinear map computations) grows linearly in hierarchy depth correspondingly. It is undesirable that lower-level entities should be equipped with more storage space and more computing power in order to cope with linear correspondence between computation & communication complexity and identity hierarchy depth.

Different from the linear relationship existing in BB[1] system [3], the selective identity secure HIBE system in [4] and the fully secure HIBE system in [9] have the merit of being of constant size ciphertext. As of system in [4], the Entity j's private key d_{ID_j}, denoted $(d_0,\ d_1,\ RH_{j+1},\ \ldots,\ RH_\ell)$, is expressed as:

$$d_{ID_j} = \left(\alpha g_2 + r\left(g_3 + \sum_{k=1}^{j} I_k h_k \right),\quad rg,\quad rh_{j+1},\quad \ldots,\quad rh_\ell \right).$$

where the $\ell - j$ components $RH_{j+1}, \cdots, RH_\ell$ are historical content for hierarchically deriving private keys for Entity j's descendants. Actually, if private key derivation is disabled, the private key for an entity, *i.e.*, (d_0, d_1), is of constant size. That is, if the root PKG does not provide these $\ell - j$ components when distributing a private key for Entity j, where (d_0, d_1) is still a valid private key for Entity j from cryptographic operation perspective, then the private key for Entity j consists of only two group elements.

A ciphertext corresponding to given message $M \in \mathrm{G}_T$ is generated on identity on identity $ID_j = (I_1, \ldots, I_j) \in (\mathrm{Z}_q^*)^j$ with a random number $s \in \mathrm{Z}_q$ as:

$$C = \left(M \cdot e(g_1, g_2)^s,\quad sg,\quad s\left(g_3 + \sum_{k=1}^{j} I_k h_k \right) \right),$$

where there are only three group elements, or ciphertext size is independent of the hierarchy depth of the intended recipient. All identifiers along identity hierarchy of the intended recipient are integrated into one component of a ciphertext, which is the key idea of constructing HIBE system with short ciphertext. With both private key and ciphertext

being of constant number of group elements, the decryption time is independent of the hierarchy depth of the recipient, and the decryption only requires two bilinear map computations.

Enforcing Authorized Delegation. It is necessary that HIBE systems provide flexible means for permitting only some ancestors of an entity instead of all of its ancestors to be able to complete tasks for the entity, such as decrypting ciphertexts, signing messages and so on. However, direct and unrestricted private key derivation (that we call unlimited delegation, as in HIBE systems [7][1][3]) should be prohibited.

As of BB[1] system [3], a private key $d_{ID_{j+1}}$ for Entity $^{j+1}$ as parent of Entity ^{j} can be derived by randomizing the Entity ^{j}'s private key $d_{ID_j} = (d_0, RD_1, \ldots, RD_j)$, with $j+1$ random numbers $r_1, \cdots, r_{j+1}$ from Z_q as:

$$d_{ID_{j+1}} = \left(d_0 + \sum_{k=1}^{j+1} r_k (I_k \hat{g}_1 + \hat{h}_k), RD_1 + r_1 \hat{g}, \ldots, RD_j + r_j \hat{g}, r_{j+1} \hat{g} \right).$$

Consequently, any ancestor of an entity being capable of generating valid private key for the descendant can act on behalf of the entity.

Different from mechanism of direct and unrestricted private key derivation [7][1][3], limited delegation is achieved in HIBE constructions presented in [4] and [9]. As of the HIBE construction in [4], to derive a private key for Entity $^{j+1}$ with use of Entity ^{j}'s private key d_{ID_j}, denoted $(d_0, d_1, RH_{j+1}, \ldots, RH_\ell)$, pick a random number r from Z_q, and output

$$d_{ID_{j+1}} = \Big(d_0 + r\left(g_3 + \sum_{k=1}^{j+1} I_k h_k \right) + I_{j+1} RH_{j+1}, d_1 + rg,$$

$$RH_{j+2} + rh_{j+2}, \ldots, RH_\ell + rh_\ell \Big).$$

By repeating the process above, private keys for all descendants of Entity ^{j} can be derived with use of the Entity ^{j}'s private key and needed historical content. Different from private key derivation in BB[1] system, where private keys for a child can be derived by only randomizing its parent's private keys, this HIBE system however does need some extra historical information in deriving a private key for a child, in addition to randomizing the parent's private key. For example, in deriving a private key for Entity $^{j+1}$ from Entity ^{j}'s private key, RH_{j+1} ($= rh_{j+1}$) as an important historical argument, which is product of a public parameter h_{j+1} and a random number r selected by the root PKG when Entity ^{j}'s private key is extracted by the root PKG, or is deduced from the last private key derivation when Entity ^{j}'s private key is derived from its parent's private key, is needed for calculating $I_{j+1} RH_{j+1}$ as one important share of the resulted private key for Entity $^{j+1}$, as well as randomizing Entity ^{j}'s private key to get the other share of the private key for Entity $^{j+1}$.

If the root PKG does not provide $\ell - j$ components $RH_{j+1}, \cdots, RH_{\ell}$ in d_{ID_j}, which are historical information for hierarchically deriving private keys for Entity j 's descendants, where (d_0, d_1) is still a valid private key for Entity j from cryptographic operation perspective, there is no means of generating a valid private key for any descendant of Entity j with using Entity j 's private key (d_0, d_1). By providing a restricted private key with only t components rh_{j+k} for $k = 1, \ldots, t$ to Entity j, Entity j is only capable of generating private keys for its descendants of bounded depth t, *i.e.*, from descendant at level $j+1$ to descendant at level $j+t$ along hierarchy tree. That is called limited delegation.

Limited delegation does prevent private keys for those descendants at depth beyond the limited depth from being derived. Nevertheless, there is no means to only derive a private key for Entity $j+t$ with use of Entity j 's private key without revealing private keys for those Entity j 's descendants which are Entity $j+t$'s ancestors, or entities at level $j+1, \cdots, j+t-1$. This undesirable breach in privacy is resulted from the need of a parent's private key when deriving a private key for its child.

Therefore, it is desirable to construct a HIBE system, where a flexible means for delegating the responsibility of generating private keys for some specified entity to some of its ancestors is provided, while disabling direct and unrestricted private key derivation. That we call authorized delegation.

1.3. Our Approach

HIBE construction with constant size ciphertext and free from key escrow problem. We construct a selective identity secure HIBE system in standard model with constant size private key, constant size ciphertext and authorized delegation, where any entity being not authorized does not have the capability of deriving private keys for any of its descendants with use of its private key, any entity however can be authorized to be capable of generating valid private keys for any of its descendants. Because an entity is incapable of generating valid private keys for its descendants without being authorized by the root PKG, and its private key is not legitimate to ciphertexts encrypted on identity of any of its descendants, then Encryption Privacy of Ciphertext Dedicated Only to Intended Recipient (that we call Dedicated Encryption Privacy) is achieved from both private key derivation and private key legitimacy perspectives.

Identifier Discrimination. Private key for an entity is constructed in our construction by differentiating between the local identifier I_j of identity $ID_j = (I_1, \ldots, I_j)$ and non-local identifiers $I_1, \cdots, I_{j-1}$, *i.e.*, by introducing two independent components defined on non-local identifiers with respect to hierarchy $I_1 \rightarrow \cdots \rightarrow I_{j-1}$ and on local identifier I_j with j^{th} level-dependent parameter respectively to randomize the master key of HIBE system in order to extract a private key for ID_j. That we call Identifier Discrimination.

Because the private key extracted for ID_j is neither an extension (further randomization) of its parent's private key nor secret eligible for deriving its child's private keys, the private key is anchored to the identity ID_j.

Authorized Delegation. In our HIBE system, although it is impossible for entities to derive valid private keys for their descendants with only using their private keys, the system does provide means for an entity to derive private keys for a specified descendant, that we call Authorized Delegation. Authorized Delegation is achieved by distributing a secret specific to an entity pair – the entity whose private keys can be derived and an ancestor of the entity who will generate private keys for the entity. Assume that Entity ^{i} with identity $ID_i = (I_1, \ldots, I_i)$ is authorized to be capable of deriving private keys for Entity ^{j} (as a descendant of Entity ^{i}) with identity $ID_j = (ID_i, \ldots, I_j)$, the root PKG first generates a copy of dedicated privacy for Entity ^{j}, denoted S_0, and another copy of privacy by randomizing the master key of the system along identity hierarchy $I_1 \rightarrow \ldots \rightarrow I_i$, denoted $S_1^{(i,ID_j)}$; secondly adds S_0 and $S_1^{(i,ID_j)}$ together to get a secret for Entity ^{i} as seed of deriving private keys for Entity ^{j}. Entity ^{i} being equipped with a proper secret can then further randomize the secret hierarchically (level by level) along identity hierarchy $I_{i+1} \rightarrow \ldots \rightarrow I_{j-1}$. The secret after being randomized at level $j-1$ is a secret for Entity ^{j}, which is actually a valid private key for Entity ^{j}.

If a secret for k^{th} level (where $1 \le k \le j-1$) is distributed to the entity at k^{th} level along identity hierarchy $I_i \rightarrow \ldots \rightarrow I_k \rightarrow \ldots \rightarrow I_j$ (defined from Entity ^{j}'s identity), *i.e.,* Entity ^{k}, then the ancestor Entity ^{k} (with identity ID_k) is authorized to derive secrets for its descendant Entity ^{j}.

2. Preliminaries

In this section, we briefly review bilinear pairings, HIBE systems and related complexity assumptions.

2.1. Bilinear Pairings

Definition 1. 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 prime order q, $\mathbb{G}_T$ a multiplicatively-written group of order q with identity denoted by 1, and let $e: \mathbb{G} \times \hat{\mathbb{G}} \rightarrow \mathbb{G}_T$ be a function that maps pairs of elements in $\mathbb{G} \times \hat{\mathbb{G}}$ to elements of a group of $\mathbb{G}_T$. $\Lambda = (\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T, q, e)$ is a bilinear 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 e are all efficiently computable (probabilistic polynomial-time bounded time complexity).

Let $\Lambda = (\mathrm{G}, \hat{\mathrm{G}}, \mathrm{G}_T, q, e)$ be a bilinear pairing, then $(\mathrm{G}, \hat{\mathrm{G}})$ is called a bilinear group pair, and $(\mathrm{G}, \hat{\mathrm{G}}, \mathrm{G}_T)$ is called bilinear map group tuple. The bilinear pairing is called symmetric if $\hat{\mathrm{G}}$ is G, denoted Λ_{sym}.

2.2. HIBE Systems

Hierarchical Identity Based Encryption (HIBE). A HIBE system is made up of five algorithms [8,7,1,3]: $Setup$, $Extract$, $Derive$, $Encrypt$, and $Decrypt$. The $Setup$ algorithm takes responsible of outputting parameters for HIBE setting, including public parameters and master key only known to the root PKG (at level 0). The $Extract$ algorithm takes master key and an identity $ID_j = (I_1, \ldots, I_j)$ (as public key of Entity ^{j}) as input, and outputs a private key for ID_j. Algorithm $Derive$ functions alike to $Extract$, it takes some private values of an entity and outputs private keys for its descendants, where the private values of the entity are not necessarily private key for the entity, and can either be used to generate private keys for one, some, or all of its descendants. The $Encrypt$ algorithm encrypts a message on identity of the intended recipient. Algorithm $Decrypt$ recovers a message from a ciphertext with use of a private key for the recipient.

2.3. Complexity Assumptions

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

$$Adv^{DBDH}_{e:\mathrm{G}\times\hat{\mathrm{G}}\to\mathrm{G}_T,\mathrm{B}} = |\Pr[\mathrm{B}(g, ag, cg, \hat{g}, a\hat{g}, b\hat{g}, e(g,\hat{g})^{abc}) = 1] -$$

$$\Pr[\mathrm{B}(g, ag, cg, \hat{g}, a\hat{g}, b\hat{g}, T) = 1]|,$$

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

We refer to the distribution of the 7-tuple $(g, ag, cg, \hat{g}, a\hat{g}, b\hat{g}, e(g,\hat{g})^{abc})$ as P_{BDH} and that of $(g, ag, cg, \hat{g}, a\hat{g}, b\hat{g}, T)$ as R_{BDH}.

In terms of the computational time and the advantage in solving BDH problem, Decisional BDH assumption in pairing $\Lambda = (\mathrm{G}, \hat{\mathrm{G}}, \mathrm{G}_T, q, e)$ is defined as follows.

Definition 2. Decisional BDH Assumption. If there is no t-time algorithm B that has advantage at least ε in solving decisional BDH problem in pairing $\Lambda = (\mathrm{G}, \hat{\mathrm{G}}, \mathrm{G}_T, q, e)$,

then the (t,ε) -Decisional BDH assumption holds. For simplicity, Decisicional BDH assumption holds if for every PPT algorithm B, $Adv^{DBDH}_{e:\mathrm{G}\times\hat{\mathrm{G}}\to\mathrm{G}_T,\mathrm{B}}$ is negligible.

3. Our HIBE Construction with Constant Size Private Key and Constant Size Ciphertext

We now present our HIBE system, which is of constant size ciphertext, private key, and free from key escrow problem. The security of the HIBE system can be reduced to the intractability of Decisional Bilinear Diffie-Hellman problem. We opt to construct our HIBE system in asymmetric pairing $\Lambda=(\mathrm{G},\hat{\mathrm{G}},\mathrm{G}_T,q,e)$, which is also applicable to symmetric bilinear pairing.

3.1. Construction

- $\mathbf{Setup(1^k,\ell)\to\Lambda,params,mk}$. The root PKG runs algorithm *Setup* with security parameters 1^k and maximum hierarchy depth ℓ as input, to output a pairing Λ, system parameters *params* and master key of the system mk. Let $\Lambda=(\mathrm{G},\hat{\mathrm{G}},\mathrm{G}_T,q,e)$, where q is of k binary bits, G, $\hat{\mathrm{G}}$, G_T are all of prime order q and with generators g, $\hat{g}$ and $e(g,\hat{g})$ respectively, the algorithm picks two random numbers α and β from Z_q, sets $g_1=\alpha g$, $\hat{g}_1=\alpha\hat{g}$, $\hat{g}_0=\alpha\beta\hat{g}$, and calculates $v=e(g,\hat{g}_0)=e(g,\hat{g})^{\alpha\beta}$. It then selects $2\ell+1$ random numbers δ_0, δ_1, …, δ_ℓ, γ_1, …, γ_ℓ from Z_q, and sets $h_i=\delta_i g$, $\hat{h}_i=\delta_i\hat{g}$ for each i in $\{0,1,\ldots,\ell\}$, and sets $l_k=\gamma_k g$, $\hat{l}_k=\gamma_k\hat{g}$ for each $k\in\{1,\ldots,\ell\}$. The public system parameters $params\in\mathrm{G}^{2\ell+3}\times\hat{\mathrm{G}}^{2\ell+3}\times\mathrm{G}_T$ and the master secret $mk\in\hat{\mathrm{G}}$ are expressed as:

$$\begin{aligned} &params=\left(g,g_1,h_0,h_1,\ldots,h_\ell,l_1,\ldots,l_\ell,\hat{g},\hat{g}_1,\hat{h}_0,\hat{h}_1,\ldots,\hat{h}_\ell,\hat{l}_1,\ldots,\hat{l}_\ell,v\right),\\ &mk=(\hat{g}_0). \end{aligned} \tag{1}$$

- $\mathbf{Extract\left(mk,params,ID_j\right)\to d_{ID_j}}$. The *Extract* algorithm takes identity $ID_j=(I_1,\ldots,I_j)\in(\mathrm{Z}_q^*)^j$ ($j\le\ell$), master secret mk and public system parameters *params* as input, picks two random numbers r_0, r_1 from Z_q, and generates a private key $d_{ID_j}=(d_0,d_1,d_2)\in\hat{\mathrm{G}}^3$ for identity ID_j as:

$$d_{ID_j}=\left(\hat{g}_0+r_0\left(\sum_{k=1}^{j-1}I_k\hat{l}_k+\hat{h}_0\right)+r_1\left(I_j\hat{g}_1+\hat{h}_j\right),r_0\hat{g},r_1\hat{g}\right). \tag{2}$$

The master key $\hat{g}_0$ is randomized by two components independently defined by differentiating between non-local identifiers and local identifier, *i.e.,* $r_0(\sum_{k=1}^{j-1}I_k\hat{l}_k+\hat{h}_0)$ being defined on I_1, …, I_{j-1} along hierarchy $I_1\to\ \ldots\to\ I_{j-1}$, and $r_1(I_j\hat{g}_1+\hat{h}_j)$

being defined on local identifier I_j with level-dependent parameter $\hat{h}_j$. The level-dedicated component $r_1(I_j\hat{g}_1+\hat{h}_j)$ makes private key for ID_j being not an eligible secret for private key derivation. The private key d_{ID_j} for Entity j is transferred securely from the root PKG to the Entity j.

- $\mathbf{Derive(i,ID_j,S_{(i,ID_j)})\rightarrow d_{ID_j}}$. Algorithm *Derive* takes as input an identity $ID_j=(I_1,\ldots,I_j)$ of depth $j\in\{2,\ldots,\ell\}$, an index $i\in\{1,\ldots,j-1\}$ specifying an identity of depth i as prefix of ID_j (denoted $ID_i=(I_1,\ldots,I_i)$), and a secret $S_{(i,ID_j)}\in\hat{\mathbb{G}}$ for identity pair (ID_i,ID_j), and outputs a private key $d_{ID_j}\in\hat{\mathbb{G}}^3$ for ID_j ($=(ID_i,I_{i+1},\ldots,I_j)$). $S_{(i,ID_j)}$ is a secret specific to (ID_i,ID_j), which is eligible as delegation credentials to be used to derive private keys for ID_j along the identity hierarchy $I_{i+1}\rightarrow\ldots\rightarrow I_j$. The secret $S_{(i,ID_j)}$ for (ID_i,ID_j) is originally generated by the root PKG. How secret $S_{(i,ID_j)}$ is generated is detailed in Section 4.

To derive a private key d_{ID_j} for ID_j with $S_{(i,ID_j)}=(S_0,S_1,S_2,R_{i+1},\ldots,R_{j-1})\in\hat{\mathbb{G}}^{j-i+2}$ for (ID_i,ID_j), pick two random values $r_0,r_1\in\mathbb{Z}_q$, and output

$$d_{ID_j}=\Big(S_0+\sum_{k=i+1}^{j-1}R_kI_k+r_0\Big(\sum_{k=1}^{j-1}I_k\hat{l}_k+\hat{h}_0\Big)+r_1\big(I_j\hat{g}_1+\hat{h}_j\big),$$
$$S_1+r_0\hat{g},S_2+r_1\hat{g}\Big). \tag{3}$$

- $\mathbf{Encrypt(pa\ rams,ID_j,M)\rightarrow C_{ID_j}}$. To encrypt a given message $M\in\mathbb{G}_T$ on identity $ID_j=(I_1,\ldots,I_j)$, algorithm *Encrypt* picks a random value $s\in\mathbb{Z}_q^*$ and outputs a ciphertext $C_{ID_j}=(C_0,C_1,C_2,C_3)\in\mathbb{G}_T\times\mathbb{G}^3$ as:

$$C_{ID_j}=\left(Mv^s,sg,s\Big(\sum_{k=1}^{j-1}I_kl_k+h_0\Big),s\big(I_jg_1+h_j\big)\right). \tag{4}$$

- $\mathbf{Decrypt\big(params,d_{ID_j},C_{ID_j}\big)\rightarrow M}$. Algorithm *Decrypt* takes a private key $d_{ID_j}=(d_0,\ d_1,\ d_2)$ for $ID_j=(I_1,\ldots,I_j)$ and the ciphertext $C_{ID_j}=(C_0,C_1,C_2,C_3)$ encrypted on ID_j as input, and outputs a message as:

$$M=C_0\cdot e\big(C_2,d_1\big)\cdot e\big(C_3,d_2\big)/e\big(C_1,d_0\big). \tag{5}$$

3.2. Correctness and Dedicated Encryption Privacy

Let $C = (C_0, C_1, C_2, C_3) \in \mathbb{G}_T \times \mathbb{G}^3$ be a ciphertext of a message M encrypted on identity $ID_j = (I_1, \ldots, I_j) \in \left(\mathbb{Z}_q^*\right)^j$, with respect to *Encrypt* and *Decrypt* calculations defined in Eq. (4) and Eq. (5), and $d_{ID_j} = (d_0, d_1, d_2) \in \hat{\mathbb{G}}^3$ be a private key for identity ID_j, a plaintext M' can be recovered as:

$$M' = C_0 \cdot e(C_2, d_1) \cdot e(C_3, d_2) / e(C_1, d_0)$$

$$= Mv^s \cdot e\left(s\left(\sum_{k=1}^{j-1} I_k l_k + h_0\right), r_0 \hat{g}\right) \cdot e\left(s\left(I_j g_1 + h_j\right), r_1 \hat{g}\right) /$$

$$e\left(sg, \hat{g}_0 + r_0\left(\sum_{k=1}^{j-1} I_k \hat{l}_k + \hat{h}_0\right) + r_1\left(I_j \hat{g}_1 + \hat{h}_j\right)\right)$$

$$= Me(g, \hat{g}_0)^s \cdot e\left(s\left(\sum_{k=1}^{j-1} I_k l_k + h_0\right), r_0 \hat{g}\right) \cdot e\left(s\left(I_j g_1 + h_j\right), r_1 \hat{g}\right) /$$

$$\left(e(sg, \hat{g}_0) \cdot e\left(sg, r_0\left(\sum_{k=1}^{j-1} I_k \hat{l}_k + \hat{h}_0\right)\right) \cdot e\left(sg, r_1\left(I_j \hat{g}_1 + \hat{h}_j\right)\right)\right)$$

$$= M.$$

That is, our HIBE system constructed above is consistent.

Because direct private key derivation is disabled in our system, which will be detailed in Section 4, then there is no means for an entity's ancestors to generate a private key for the entity with only use of their private keys and publicly available values, such as system parameters, public key (identity) of the entity and so on. Moreover, it is required exact component-wise match between a private key and a ciphertext for a successful decryption, which is exhibited by the correspondence between components defined in (2) and (4). That is, ciphertexts targeting an entity cannot be decrypted by other entities with their private keys being incapable of deriving a valid private key for the intended recipient and illegitimate to ciphertexts encrypted on the identity of the intended recipient. Thus dedicated encryption privacy is achieved from both private key derivation and private key legitimacy perspectives.

4. Authorized Delegation: Private Key Derivation with Authorized Secret

4.1. Private Key – Ineligible Secret for Derivation

Different from previous constructions [7,1,3] where direct and unrestricted private key derivation is possible, and constructions [4,9] with limited delegation, where private keys for descendants of limited depth can be derived, any entity cannot derive valid private keys for its descendants with only the knowledge of its private key and public values (including public system parameters and public keys (identities) of descendants) in our HIBE system, such as by randomizing its private key along the hierarchy.

Let $d_{ID_j} = (d_0, r_0\hat{g}, r_1\hat{g})$ and $d_{ID_{j+1}} = (d_{0'}, r_{0'}\hat{g}, r_{1'}\hat{g})$ are private keys for identity $ID_j = (I_1, \ldots, I_j)$ and $ID_{j+1} = (ID_j, I_{j+1})$ respectively (ID_j be parent identity of ID_{j+1}), and Δd_0 be the result of $d_{0'} - d_0$, Δd_0 is calculated as:

$$\Delta d_0 = r_{0'}\left(\sum_{k=1}^{j} I_k\hat{l}_k + \hat{h}_0\right) + r_{1'}(I_{j+1}\hat{g}_1 + \hat{h}_{j+1}) - r_0\left(\sum_{k=1}^{j-1} I_k\hat{l}_k + \hat{h}_0\right) - r_1(I_j\hat{g}_1 + \hat{h}_j)$$

$$= (r_{0'} - r_0)\left(\sum_{k=1}^{j} I_k\hat{l}_k + \hat{h}_0\right) + r_0 I_j\hat{l}_j - r_1(I_j\hat{g}_1 + \hat{h}_j) + r_{1'}(I_{j+1}\hat{g}_1 + \hat{h}_{j+1}).$$

It is evident that private key $d_{ID_{j+1}}$ for ID_{j+1} can be derived from private key d_{ID_j} for ID_j, if value $r_0 I_j\hat{l}_j - r_1(I_j\hat{g}_1 + \hat{h}_j)$ can be calculated. However, there is no means for the entity with knowledge of private key d_{ID_j} to calculated the required value. In other word, it is infeasible to calculate $r_0\hat{l}_j$, $r_1\hat{g}_1$ and $r_1\hat{h}_j$ given the knowledge of $r_0\hat{g}$ and $r_1\hat{g}$. That is, any entity in our HIBE system is prevented from deriving private keys for any of its descendants with use of its private key and publicly available values.

4.2. Authorized Secret for Derivation

However, our construction does provide a means for authorizing an entity to derive private keys through randomization for any of its descendants along the hierarchy of the descendant. Specifically, some specially crafted values (delegation credentials or secrets) are generated by the root PKG in order to empower an entity to be capable of deriving private keys for its descendants, and the entity being authorized can derive private keys for its descendants through randomization with these secrets.

Suppose the root PKG wants to authorize Entity i with identity $ID_i = (I_1, \ldots, I_i)$ to be capable of deriving private keys for Entity j with identity $ID_j = (ID_i, \ldots, I_j)$ (as a descendant of Entity i), the root PKG needs to craft a secret $S_{(i,ID_j)}$ specific to identity pair (ID_i, ID_j) and distribute the secret to Entity i. To calculate a secret $S_{(i,ID_j)} = (S_0, S_1, S_2, R_{i+1}, \ldots, R_{j-1}) \in \hat{G}^{j-i+2}$ for (ID_i, ID_j) with ID_i being a prefix of ID_j, pick two random numbers r_0, r_1 from Z_q, and output

$$S_{(i,ID_j)} = \Big(\hat{g}_0 + r_0\left(\sum_{k=1}^{i} I_k\hat{l}_k + \hat{h}_0\right) + r_1\left(I_j\hat{g}_1 + \hat{h}_j\right),$$

$$r_0\hat{g}, r_1\hat{g}, r_0\hat{l}_{i+1}, r_0\hat{l}_{i+2}, \ldots, r_0\hat{l}_{j-1} \Big), \tag{6}$$

where $j-i-1$ components $R_{i+1}, \cdots, R_{j-1}$ are needed for hierarchically randomizing the secret $S_{(i,ID_j)}$ to generate a series of secrets along the identity hierarchy $I_{i+1} \rightarrow \ldots \rightarrow I_{j-1}$ and at last get a private key for Entity j.

The entity with knowledge of $S_{(i,ID_j)}$ specific to (ID_i, ID_j) is empowered to be capable of generating a series of secrets $S_{(i+1,ID_j)}$, $\cdots$ $S_{(j-1,ID_j)}$ specific to identity pairs (ID_{i+1}, ID_j), $\cdots$, (ID_{j-1}, ID_j) respectively through randomization, of which the secret $S_{(j-1,ID_j)}$ is exactly a private key for identity ID_j.

5. Conclusion

In order to improve effectiveness and efficiency of identity based cryptographic operations in HIBE system, a selective identity secure HIBE system with constant size private key, constant size ciphertext and authorized delegation is constructed in this paper under DBDH assumption without using random oracles.

Compared to previous constructions, a new technique – Identifier Discrimination is introduced for composing private keys for entities in HIBE system. By discriminating between local identifier and the other ancestor identifiers (non-local identifiers) of an entity, dedicated privacy is defined on the local identifier and the hierarchy depth as a special share being introduced into the total entropy of a private key, which characterizes the private key; the complementary privacy share for the private key is defined on non-local (ancestor) identifiers as usual, such as randomizing the master key along the identity hierarchy.

By applying the technique, unlimited delegation is disabled, authorized delegation is introduced, and correspondence between components of an entity's private key and ciphertexts encrypted on the entity's identity is established, thus preventing ciphertexts intended for a recipient from being decrypted by unauthorized entities from both private key derivation and private key legitimacy perspectives.

The identifier discrimination technique opens up a new way to design HIBE systems and prove security of HIBE systems. Currently, we do not know whether there is a form of identifier discrimination functioning equivalently as a cryptographic hash function, with which a fully secure HIBE system can be constructed under simple assumptions, such as DBDH assumption.

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, "Efficient selective identity-based encryption without random oracles", Journal of Cryptology, vol. 24, no. 4, **(2011)**, pp. 659–693.

[4] D. Boneh and X. Boyen, 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.

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.
[10] 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.
[11] 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, He 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, She 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, He 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.