Journal of Software Engineering

ISSN 1819-4311

Academic Journals Inc.

www.academicjournals.com

OPEN ACCESS Journal of Software Engineering

ISSN 1819-4311
DOI: 10.3923/jse.2016.279.284

Research Article
On Delegating Private Key Derivation in Hierarchical Identity Based Encryption and Related Encryption Privacy

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

[1]Institute of Electrical Engineering, Yanshan University, 066004 Qinhuangdao, China
[2]School of Transportation, Shijiazhuang Tiedao University, 050043 Shijiazhuang, China
[3]Collaborative Innovation Center, Shijiazhuang Tiedao University, 050043 Shijiazhuang, China
[4]Department of Automation, Shanghai Jiao Tong University, 200240, China

Abstract

As of Hierarchical Identity Based Encryption (HIBE) systems, there are two important tasks should be accomplished properly, the first one is to establish logically hierarchical relationship between entities in the hierarchy tree, which is essentially accomplished through private key derivation by delegating responsibilities to lower-level PKGs and the other task is to achieve encryption privacy of ciphertext targeting an intended recipient. In this study, mechanisms of private key derivation in HIBE systems are classified, which explicitly define how and to what extent an entity in the hierarchy takes its level PKGs role of generating valid private keys for its descendants in the hierarchy. Moreover, a new delegation mechanism, authorized delegation is introduced, which can prevent any entity from deriving private keys for its descendants with use of its private key and delegate the responsibility of generating private keys for a specified entity through authorization by distributing a specific secret to an entity as an ancestor of the specified entity by the root PKG (primitive authorization) or some other authorized entities (chained authorization). As for encryption privacy of ciphertext in a HIBE system, which measures the possibility that ciphertexts targeting an entity are successfully decrypted by its ancestors or descendants, the encryption privacy is studied from two distinct perspectives, i.e., private key derivation perspective and private key legitimacy perspective. Furthermore, dominated encryption privacy and dedicated encryption privacy are defined and discussed from private key legitimacy perspective.

Key words: Identity-based encryption, HIBE, private key derivation, authorized delegation, encryption privacy

Received: March 14, 2016 Accepted: April 30, 2016 Published: June 15, 2016

Citation: Jian-Wu Zheng, Jing Zhao and Xin-Ping Guan, 2016. On delegating private key derivation in hierarchical identity based encryption and related encryption privacy. J. Software Eng., 10: 279-284.

Corresponding Author: Jian-Wu Zheng, Institute of Electrical Engineering, Yanshan University, 066004 Qinhuangdao, China Tel: +86 15613158336

Competing Interest: The authors have declared that no competing interest exists.

Data Availability: All relevant data are within the paper and its supporting information files.

INTRODUCTION

An Identity Based Encryption (IBE) system is a public key system that an entity's public key can be any identifier of the entity (arbitrary string that is public and can identify the entity) and private key for the entity can be calculated from its identifier 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 (1985), there are no usable IBE constructions until the studies by Boneh and Franklin (2001), Cocks (2001) and Sakai and Kasahara (2000). The concept of Hierarchical Identity Based Encryption (HIBE) was first introduced by Horwitz and Lynn (2002). Gentry and Silverberg (2002), Canetti *et al*. (2003), Boneh and Boyen (2004a), Gentry (2006) and Waters (2005, 2009) constructed their schemes under the Decisional Bilinear Diffie-Hellman assumption (or variants of BDH assumption) and proved the security of their systems in standard model. Studies by Gentry (2006), Waters (2005, 2009) and Boneh *et al*. (2005) provided some fully secure schemes without random oracles.

Conventionally, it is taken for granted that in a HIBE system entities in the hierarchy have the power of generating valid private keys for their descendants; specifically, an entity can not only directly use its own private key and some public parameters to derive valid private keys along the hierarchy tree (usually derivation is accomplished by randomizing an ancestor's private key), but also unrestrictedly generate valid private keys for all descendants of the entity if the entity wants to. Boneh *et al*. (2005) presented a HIBE scheme that is selective identity secure in standard model and fully secure in the random oracle model; notably, the scheme can achieve limited delegation and short ciphertexts regardless of the hierarchy depth.

Although, key escrow problem is inherent in IBE public cryptography, resulting from the mechanism of generating private keys for entities in the system, but it should not be exaggerated in HIBE systems, where lower level PKGs are unrestrictedly delegated to be capable of generating private keys for their descendants. Particularly, it is irrational and undesirable that a lower level PKG (as an ancestor) can generate valid private keys for a descendant with direct use of its private key and a lower level PKG can generate private keys for all of its descendants.

In order to preventing entities from deriving private keys for their descendants with direct use of their private keys, while providing a means for entities to be capable of deriving private keys for some of their descendants. A new technique for composing private keys for entities in HIBE hierarchy is proposed, that it was called differenting technique. When generating a private key for an identity, $ID_j = (I_1,\ldots,I_j) \in (Z_q^*)^j$ the local identifier I_j is used to differentiate all those non-local identifiers I_i, ... I_{j-1}, which maps the true identity I_j to a newly constructed identity (not necessary a true identity in the hierarchy). Most importantly, those ancestor entities of ID_j are not prefixes of the newly constructed identity, thus preventing the direct private key derivation and guaranteeing the related encryption privacy. Moreover, privilege of generating private keys for an entity can be delegated by the root PKG to any ancestor of the entity through authorization by distributing an authorized credential to the ancestor with respect to the differentiating technique. That it was called authorized delegation.

MATERIALS AND METHODS

Different from the one-PKG characterized IBE, Hierarchical Identity Based Encryption (HIBE) accommodates level-oriented PKG configuration. Namely, the top level PKG is the root PKG (at level zero), who maintains a hierarchy tree of which non-leaf nodes are viewed as level PKGs. The HIBE allows the root PKG to balance the workload by delegating identity authentication, private key generation and private key distribution to lower level PKGs. Usually, delegation of private key generation for entities in the hierarchy is main job of responsibility delegation (from root PKG to lower level PKGs). The mechanisms of delegating private key generation can be classified into three classes, i.e., unlimited delegation, limited delegation and a new delegation firstly propsed in this study, authorized delegation with reference to criteria listed below. For ease of presentation, it is assumed that $Entity_i$ with identity $ID_i = (I_1,..., I_i)$ is an ancestor of $Entity_j$ with identity $ID_i = (I_1,..., I_j)$ that is ID_i is a prefix of ID_j such that $ID_i [k] = ID_j [k]$ for all $k\epsilon\{1,...,i\}$.

- Only an entity's private key or some specially crafted content other than private key should be utilize to generate private keys for the entity's descendants, besides some public parameters, such as system parameters, identities (public keys) of the descendants whose private keys are derived and so on
- Whether the private key generation can be hierarchically derived along the identity hierarchy tree; specifically, whether private key for $Entity_{j+1}$ can be derived given a private key for $Entity_j$ is generated
- Whether $Entity_j$ should first generate private keys for all entities, which are descendants of $Entity_i$ and ancestors of $Entity_j$ prior to deriving a private key for $Entity_j$

Unlimited delegation: Unlimited delegation indicates that an entity dominates all of its descendants. Unlimited delegation means that an entity in the hierarchy can directly and unrestrictedly derive private keys for its descendants. Directly here means an entity can derive private keys for its descendant's with only use of its private key, or the private key for the entity is the only needed secret for generating the descendant's private keys. Unrestrictedly means that the private key derivation can be accomplished hierarchically by an entity for all of its descendants.

As of private key derivation in Boneh and Boyen (2004b, 2011) an $Entity_j$'s private key denoted d_{ID_j} can be hierarchically randomized to generate private keys for all of its descendants level by level. How $Entity_j$ can derive a private key for its child entity $Entity_{j+1}$ with use of its private key d_{ID_j}, public system parameters, identity of the child and some random values is exemplified below.

Both private keys for $Entity_j$ and $Entity_{j+1}$ with identities $ID_j = (I_1,\ldots,I_j) \in (Z_q^*)^j$ of depth $j \leq l-1$ and $ID_{j+1} = (ID_j, I_{j+1}) \in (Z_q^*)^{j+1}$, denoted $d_{ID_j} \in \hat{G}^{j+1}$ and $d_{ID_{j+1}} \in \hat{G}^{j+2}$, respectively can be extracted as:

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

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

Let Δd_0 be the result of $d_{ID_{j+1}}[0]$, Δd_0 is calculated as:

$$\Delta d_0 = \sum_{k=1}^{j}(r_k^{(ID_{j+1})} - r_k^{(ID_j)})(I_k\hat{g}_1 + \hat{h}_k) + r_{j+1}^{ID_{j+1}}(I_{j+1}\hat{g}_1 + h_{j+1}).$$

Correspondingly, other components can as well be calculated as $(r_1^{(ID_{j+1})} - r_1^{(ID_j)})\hat{g},\ldots,(r_j^{(ID_{j+1})} - r_j^{(ID_j)})\hat{g}$ and $(r_{j+1}^{(ID_{j+1})} - 0)\hat{g}$. Let $(d_0^{(ID_j)}, RD_1^{(ID_j)},\ldots, RD_j^{(ID_j)})$ denote the private key for $Entity_j$ (i.e., d_{ID_j}) and $r_1,\ldots, r_{j+1}$ be j+1 random numbers from z_q, the private key for$Entityt_j$ can be derived as (other than extracting by extract (mk, ID_{j+1})):

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

By repeating the derivation process above, the private key of $Entity_{j+1}$ can be derived by any of its ancestors along the hierarchy. Consequently not only ciphertexts intended for an entity can be decrypted by any of its ancestors, but also the ancestor, being with knowledge of a private key of the descendant can do anything that the entity can do.

Limited delegation: Unlike unlimited delegation, limited delegation restricts the depth within which the descendant's private keys can be derived. Limited delegation means that an entity at depth k with public identity ID_k, denoted $Entity_k$ is given a restricted private key witht t instead of l-k (t<l-k, where l is the maximum hierarchy depth) extra secrets that only authorizes the ancestor (i.e., $Entity_k$) to be able to derive private keys for its descendants of limited depth, beginning from $Entity_k$'s child to its descendant at depth k+t (the deepest depth). If all l-k extra secrets are provided, then the entity at depth k can generate private keys for all of its descendant. Particularly, the HIBE system fails to only generate valid private keys for a descendant at a specified depth ξ for $k+2 \leq \xi \leq l$ without deriving private keys for descendants at depth k+1,..., ξ.

The HIBE system presented by Boneh *et al.* (2005) considers "Limited delegation" and related encryption privacy of preventing an ancestor from successfully decrypting ciphertexts targeting its descendants. Private keys for $Entity_j$ and $Entity_{j+1}$ with identities $ID_j = (I_1,\ldots,I_j) \in (Z_q^*)^j$ and $ID_{j+1} = (ID_j, I_{j+1})$, respectively are extracted by the root PKG as:

$$d_{ID_j} = (\alpha g_2 + r^{(ID_j)}(g_3 + \sum_{k=1}^{j} I_k h_k),\ r^{(ID_j)}g,\quad r^{(ID_j)}h_{j+1},\ldots,\quad r^{(ID_j)}h_\ell)$$

$$d_{ID_{j+1}} = (\alpha g_2 + r^{(ID_{j+1})}(g_3 + \sum_{k=1}^{j+1} I_k h_k),\ r^{(ID_{j+1})}g,\quad r^{(ID_{j+1})}h_{j+2},\ldots,\quad r^{(ID_{j+1})}h_\ell)$$

where, $r^{(ID_j)}$ and $r^{(ID_{j+1})}$ are two random numbers picked from Z_q by the root PKG. For clarity of representation, d_{ID_j} is denoted as $(d_0^{(ID_j)}, d_1^{(ID_j)}, RH_{j+1}^{(ID_j)},\ldots, RH_\ell^{(ID_j)})$. By picking a random number r from Z_q, a private key for $Entity_{j+1}$ is derived with use of d_{ID_j} as:

$$\begin{aligned} d_{ID_{j+1}} &= (d_0^{(ID_j)} + r(g_3 + \sum_{k=1}^{j+1} I_k h_k) + I_{j+1}RH_{j+1}^{(ID_j)}, \\ &= d_1^{(ID_j)} + rg,\ RH_{j+2}^{(ID_j)} + rh_{j+2},\ldots,RH_\ell^{(ID_j)} + rh_\ell) \end{aligned}$$

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 content 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 $Entity_{j+1}$ with use of $Entity_j$'s private key, $RH_{j+1}^{(ID_j)}$ $(= r^{(ID_j)} h_{j+1})$ as an important historical argument is needed for calculating $I_{j+1}RH_{j+1}^{(ID_j)}$ 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 $Entity_{j+1}$.

Then, if the root PKG does not provide l-j components $RH_{j+1}^{(ID_j)},..., RH_{\ell}^{(ID_j)}$ when distributing a private key for $Entity_j$, where $(d_0^{(ID_j)}, d_1^{(ID_j)})$ is still a valid private key for $Entity_j$ from perspective of cryptographic operation without considering private key derivation, there is no means of generating valid private keys for any descendant of $Entuty_j$ with using $Entuty_j$'s private key $(d_0^{(ID_j)}, d_1^{(ID_j)})$, because of lack of the needed historical argument $RH_{j+1}^{(ID_j)}$.

Actually, only the component $RH_{j+1}^{(ID_j)}$ instead of all those l-j components is not provided, it is impossible to derive a private key for $Entity_{j+1}$ with use of $Entity_j$ private key and thus disabling the hierarchical private key derivation along the hierarchy tree. That is, by providing a restricted private key with onlyt components $r^{(ID_j)}h_{j+k}$ for k = 1,...,t to $Entity_j$ can be capable of only generating private keys for its descendants of bounded depth t, i.e. from descendant at depth j+1 to descendant at depth j+1 along hierarchy tree.

Authorized 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 entities, which are at level between j+1 and j+t-1. This undesirable breach in privacy is resulted from the need of use of a parent's private key when deriving a child's private key.

Authorized delegation means that private keys for an entity cannot be derived directly from its ancestor's private keys. However, by distributing a secret specifically crafted for an entity to its ancestor by the root PKG, the ancestor is thus authorized to generate private keys for the specific descendant, while failing to generate private keys for any entity other than the specified descendant.

In the sequel a new technique: Differentiating technique is proposed, which can be applied to construct a HIBE system with authorized delegation of generating private keys for entities (always descendants of the generator). Particularly, what should be accomplished for achieving authorized delegation is as follows:

- Planning private key composition, such as including share of randomizing the master secret and some components that make direct and unrestricted delegation of generating private keys for descendants impossible. Contrasted to private key derivation in (Gentry and Silverberg, 2002; Boneh and Boyen, 2004a, 2011), where both S_j and d_{ID_j} can be hierarchically randomized to generate private keys for $ID_{j+1} = (_{Idj}, I_{j+1}) ID_{j+2}$,... and so on
- Providing means for an entity, such as through authorization to be capable of generating private keys for a specified descendant entity. Authorization here can be achieved through secret distribution by equipping the generator with specially crafted content for deriving private keys for the specified entity, somewhat analogous to HIBE system presented by Boneh *et al.* (2005), where by equipping $Entity_j$ with needed secrets $r^{(ID_j)}h_{j+1},..., r^{(ID_j)}h_{j+1}$ for deriving a private key for $Entity_j$'s descendant at depth j+1

The main idea of this solution differentiating technique is to differentiate between identifiers $I_1,..., I_j$ of the identity ID_j when extracting a private key for $Entity_j$. Specifically, in addition to randomizing the master secret of the root PKG with each identifier of $\{I_1,...,I_j\}$ independently and uniformly for extracting a private key for $Entity_j$, which is the only mechanism of private key extraction presented in Boneh and Boyen (2011) an extra share ξ resulted from the combination of $Entity_j$'s local identifier I_j and those random values picked correspondingly for identifiers $I_1,...,I_{j-1}$ is introduced into the $Entity_j$'s private key. The extra share ξ anchors the generated private key only to the identity $ID_j = (I_1,..., I_j)$. Anchor here means that the private key generated for $Entity_j$ can neither be used to derive private keys for its descendants, nor to decrypt ciphertexts intended for its ancestors or descendants. Namely, it is infeasible for an entity to derive private keys for its descendants with its private key, because there is no means for the $Entity_j$ to wipe off the share defined on its local identifier I_j from its private key and to introduce needed share related to the local identifier of each of its descendants for private key derivation in order to generate the corresponding descendant's private key.

Moreover, this HIBE system does provide a mechanism for authorized private key derivation, i.e., deriving a valid private key for and only for a specified descendant. Assume that $Entity_i$ as an ancestor of $Entity_j$ is authorized to derive private keys for $Entity_j$ (the specified entity). $Entity_j$ can be authorized by distributing to it two copies of information, the first information is the result of randomizing the master secret along the identity hierarchy $I_1 \rightarrow ... \rightarrow I_i$ and the other copy is the

result of combination of local identifier I_j of $Entity_j$ (not $Entity_i$) with those random numbers picked for identifiers $I_1,..., I_i$ in randomizing the master secret. Then with these two copies of information $Entity_j$ can further hierarchically randomized these two copies with identical random number series along the identity hierarchies $I_{i+1}\rightarrow...\rightarrow I_j$ and $I_j\rightarrow...\rightarrow I_j$, respectively and at last add these two copies of information. The summation is a private key for $Entity_j$. It is worth noting that two copies of information during the derivation process, i.e., along the identity hierarchy $I_{j+1}\rightarrow...\rightarrow I_{j-1}$, neither can be used to derive private keys for entities other than $Entity_j$, nor can be added to get a private key for any ancestor of $Entity_j$.

RESULTS AND DISCUSSION

Unlike public key cryptography implemented in Public Key Infrastructure (PKI), where an entity's public and private key pair can be selected by either the trusted authority or the entity itself, private keys for an entity in HIBE system can only be generated by the root PKG or some domain (lower-level) PKGs. That is key escrow problem is inherent in (H) IBE public cryptography and ciphertexts for an entity can be decrypted by those entities that are capable of generating valid private keys for the entity. As a result, there is no encryption privacy of ciphertexts targeting entities for which private keys can be derived by their ancestor entities from the ancestor's point of view.

With the technique detailed in section above, unlimited delegation is disabled with the differentiating technique and any entity needs to be authorized by the root PKG for being able to generate private keys for any of its descendants. Moreover, other than from private key derivation perspective, it is necessary to consider encryption privacy from private key legitimacy perspective, i.e., whether an entity's private key is legitimate for ciphertexts encrypted on identity of the entity's descendants.

Dominated encryption privacy: Means that ciphertexts targeting an entity can be decrypted by all or some of its ancestors without burden of generating a private key for the entity but with direct use of these ancestor's private keys. As for HIBE scheme in Gentry and Silverberg (2002) and BB1 scheme in Boneh and Boyen (2004b, 2011) it is not necessary that any ancestor of $Entity_j$ should derive a private key for $Entity_j$ in order to decrypt ciphertexts intended for $Entity_j$. When encrypting a given message $M\in G_t$ intended for $Entity_j$ with identity $ID_j = (I_1,...,I_j) \in (Z_q^*)^j$, the encryptor picks a random value $s \in Z_q^*$ and outputs the ciphertext as:

$$C=\left(Mv^s, sg, s(I_1g + h_1),\ldots,s(I_jg + h_j)\right)\in G_t \times G^{j+1}$$

Let $Entity_j$ with identity $ID_k = (I_1,..., I_k)$ be an ancestor of $Entity_j$, the private key for $Entity_k$ denoted $\left(d_0^{(ID_k)}, RD_1^{(ID_k)},\ldots,RD_K^{(ID_k)}\right)$ is extracted as:

$$d_{ID_K} = \left(\hat{g}_0+\sum_{i=1}^{k} r_i\left(I_i\hat{g}_1+\hat{h}_i\right), r_1\hat{g},\ldots,r_k\hat{g}\right)$$

$Entity_k$ can decrypt ciphertext C denoted $\left(C_0, C_1, RE_1^{(ID_j)},\ldots,RE_j^{(ID_j)}\right)$, intended for $Entity_j$, as:

$$\begin{aligned} M &= C_0\cdot\frac{\prod_{i=1}^{k} e(RE_i^{(ID_j)}, RD_i^{(ID_k)})}{e\left(C_1, d_0^{(ID_k)}\right)} \\ &= M\cdot v^s\cdot\frac{\prod_{i=1}^{k} e\left(s(I_ig_1+h_i), r_i\hat{g}\right)}{e\left(sg, \hat{g}_0+\sum_{i=1}^{k} r_i\left(I_i\hat{g}_1+\hat{h}_i\right)\right)} \\ &= M \end{aligned}$$

That is any ancestor of an entity can decrypt ciphertexts encrypted on the public key (i.e. identity) of the entity with only use of its own private key without need of deriving a valid private key for the entity.

Dedicated encryption privacy: Means that all entities other than the intended recipient of a ciphertext cannot decrypt the ciphertext, thus achieving encryption privacy of ciphertext dedicated only to the intended recipient. As for encryption privacy of HIBE system presented by Boneh *et al.* (2005), assume that $Entity_j$ is an ancestor of $Entity_j$ (without respect to whether $Entity_j$ is capable of deriving private keys for $Entity_j$ or not) and an encryptor encrypts a given message$M\epsilon G_1$ on $Entity_j$'s identity $ID_j = (I_1,..., I_j)$ as:

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

then $Entity_j$ can decrypt the ciphertext with its private key as:

$$\begin{aligned} M' &= M\cdot e(g_1, g_2)^s\times\frac{e\left(rg, s\left(g_3+\sum_{k=1}^{j} I_k h_k\right)\right)}{e\left(sg, g_2^{\alpha}+r\left(g_3+\sum_{k=1}^{j} I_k h_k\right)\right)} \\ &= M\cdot\left(e(g, g)^{\sum_{k=i+1}^{j} I_k\alpha_k}\right)^{rs} \end{aligned}$$

For a successful decryption, it is required that $\sum_{k=i+1}^{j} I_k \alpha_k$ is congruent to zero with modulus prime q, where α_k for k = 1,...,l are logarithms of $\log_g^{h_k}$. α_j is calculated as:

$$\alpha_j \equiv - I_j^{-1} \sum_{k=i+1}^{j-1} I_k \alpha_k \pmod q$$

where, I_j^{-1} is multiplicative inverse of I_j in Zq. Because α_1,... and α_l are all uniformly and independently selected from Z_q, then the probability of event that α_j is of value $-I_j^{-1} \sum_{k=i+1}^{j-1} I_k \alpha_k \bmod q \in Z_q$ is 1/q, which means the probability of success of decrypting a ciphertext intended for $Entity_j$ by $Entity_i$ as an ancestor equals the probability that a specific value $-I_j^{-1} \sum_{k=i+1}^{j-1} I_k \alpha_k \bmod q \in Z_q$ is selected as $q \epsilon Z_q$. Similarly, if α_j is a descendant of $Entity_j$, it is required that $\sum_{k=j+1}^{i} I_k \alpha_k$ is congruent to zero with modulus prime q for a successful description.

CONCLUSION

The mechanism of delegating private key generation is crucial in establishing logically hierarchical relationship between entities along hierarchy tree in HIBE systems, which should reflect the true institutional structures in real world. The delegation mechanisms are classified into three classes, with reference to how an entity's private key can be generated by lower-level PKGs other than the root PKG. Moreover, differentiating technique for achieving authorized delegation is proposed, which hierarchically derive secrets along identity hierarchies $I_1 \rightarrow ... \rightarrow I_j$ and $I_j \rightarrow ... \rightarrow I_j$, i.e. by randomizing the master secret of the root PKG along the former and privacy specifically pertained to local identifier I_j (dedicated privacy) along the later and at last get a private key for $Entity_j$. Contrasted to direct and unrestricted private key derivation in unlimited delegation HIBE systems and restricted private key derivation of limited depth in limited delegation HIBE systems, authorized delegation can explicitly authorize some entity to generate valid private keys for some specified entity of which ancestor's private keys are not needed or generated at all.

At last, two types of encryption privacy, i.e., dominated encryption privacy and dedicated encryption privacy are discussed and compared from private key legitimacy perspective. It is unquestionably necessary to achieve dedicated encryption privacy when constructing a HIBE system.

REFERENCES

Boneh, D. and M.K. Franklin, 2001. Identity-based Encryption from the Weil Pairing. In: Advances in Cryptology, Kilian, J. (Ed.). Springer, Berlin, Heidelberg, ISBN: 978-3-540-42456-7, pp: 213-229.

Boneh, D. and X. Boyen, 2004a. Efficient Selective-ID Secure Identity-Based Encryption without Random Oracles. In: Advances in Cryptology, Cachin, C. and J.L. Camenisch (Eds.). Springer, Berlin, Heidelberg, ISBN: 978-3-540-21935-4, pp: 223-238.

Boneh, D. and X. Boyen, 2004b. Secure Identity based Encryption without Random Oracles. In: Advances in Cryptology, Franklin, M. (Ed.). Springer, Berlin, Heidelberg, ISBN: 978-3-540-22668-0, pp: 443-459.

Boneh, D., X. Boyen and E.J. Goh, 2005. Hierarchical Identity based Encryption with Constant Size Ciphertext. In: Advances in Cryptology, Cramer, R. (Ed.). Springer, Berlin, Heidelberg, ISBN: 978-3-540-25910-7, pp: 440-456.

Boneh, D. and X. Boyen, 2011. Efficient selective identity-based encryption without random oracles. J. Cryptol., 24: 659-693.

Canetti, R., S. Halevi and J. Katz, 2003. A Forward-Secure Public-Key Encryption Scheme. In: Advances in Cryptology, Biham, E. (Ed.). Springer, Berlin, Heidelberg, ISBN: 978-3-540-14039-9, pp: 255-271.

Cocks, C., 2001. An Identity based Encryption Scheme based on Quadratic Residues. In: Cryptography and Coding, Honary, B. (Ed.). Springer, Berlin, Heidelberg, ISBN: 978-3-540-43026-1, pp: 360-363.

Gentry, C. and A. Silverberg, 2002. Hierarchical ID-based Cryptography. In: Advances in Cryptology, Yuliang, Z. (Ed.). Springer, Berlin, Heidelberg, ISBN: 978-3-540-00171-3, pp: 548-566.

Gentry, C., 2006. Practical Identity-based Encryption without Random Oracles. In: Advances in Cryptology, Vaudenay, S. (Ed.). Springer, Berlin, Heidelberg, ISBN: 978-3-540-34546-6, pp: 445-464.

Horwitz, J. and B. Lynn, 2002. Toward Hierarchical Identity-based Encryption. In: Advances in Cryptology, Knudsen, L. (Ed.). Springer, Berlin, Heidelberg, ISBN: 978-3-540-43553-2, pp: 466-481.

Sakai, R. and M. Kasahara, 2000. Cryptosystems based on pairings. Proceedings of the Symposium on Cryptography and Information Security, January 26-28, 2000, Okinawa, Japan.

Shamir, A., 1985. Identity-Based Cryptosystems and Signature Schemes. In: Advances in Cryptology, Blakley, G. and D. Chaum (Eds.). Springer, Berlin, Heidelberg, ISBN: 978-3-540-15658-1, pp: 47-53.

Waters, B., 2005. Efficient Identity-based Encryption without Random Oracles. In: Advances in Cryptology, Cramer, R. (Ed.). Springer, Berlin, Heidelberg, ISBN: 978-3-540-25910-7, pp: 114-127.

Waters, B., 2009. Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions. In: Advances in Cryptology, Halevi, S. (Ed.). Springer, Berlin, Heidelberg, ISBN: 978-3-642-03355-1, pp: 619-636.