Advanced Science and Technology Letters
Vol.134 (CIA 2016), pp.125-132
http://dx.doi.org/10.14257/astl.2016.134.22

Efficient HIBE with Constant Size Ciphertext and Authorized Delegation

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

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

Abstract. In this paper, a new technique – Identifier Discrimination is proposed for composing private keys in hierarchical identity based systems, With the technique, we construct a selective identity secure HIBE system under Decisional Bilinear Diffie-Hellman (DBDH) assumption in standard security model, where the ciphertext and the private key consist of constant number of group elements, and decryption requires only three bilinear map computations, regardless of the identity hierarchy depth. Moreover, different from previous HIBE constructions, key escrow problem inherent in identity based cryptosystems is resolved in our HIBE construction. An entity in hierarchy can be authorized by the root PKG to be capable of deriving private keys for its descendants. That we call Authorized Delegation.

Keywords: Identity-Based Encryption, 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 HIBE scheme BB_1 under Decisional Bilinear Diffie-Hellman (DBDH) assumption in standard model. Later, works by Boneh et al. [2][4], Waters

ISSN: 2287-1233 ASTL

[10][11] and Lewko et al. [9] provided some fully secure schemes without random oracles.

1.1 Related Work

Depth Dependency. 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.

As for BB $_1$ system presented in [3], a private key $d_{ID_j} = (d_0, RD_1, \ldots, RD_j) \in \hat{\mathbb{G}}^{j+1}$ of Entity $_j$ with identity $ID_j = (I_1, \ldots, I_j)$ and a ciphertext $C_{ID_j} = (C_0, C_1, RE_1, \ldots, RE_j) \in \mathbb{G}_T \times \mathbb{G}^{j+1}$ encrypted on identity ID_j are expressed respectively as

$$d_{ID_j} = \left(\hat{g}_0 + \sum_{k=1}^{j} r_k (I_k \hat{g}_1 + \hat{h}_k), r_1 \hat{g}, \ldots, r_j \hat{g} \right),$$
$$C_{ID_j} = \left(Mv^s, sg, s(I_1 g + h_1), \ldots, s(I_j g + h_j) \right).$$

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

$$M' = C_0 \cdot \frac{\prod_{k=1}^{j} e(RE_k, RD_k)}{e(C_1, d_0)},$$

which indicates that time needed for decryption (the number of needed bilinear map computations) grows linearly in hierarchy depth correspondingly.

Key Escrow Problem. In traditional hierarchical identity based cryptosystems (HIBC), non-leaf entities 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 HIBC.

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 $r_1, \ldots, r_{j+1}$ from $\mathbb{Z}_q$ 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.

1.3 Our Approach

We construct a selective identity secure HIBE system in standard security model with constant size private key, constant size ciphertext and authorized delegation.

Authorized Delegation. In HIBE systems with unlimited delegation and limited delegation, private key derivation is accomplished by further randomizing one entity's private key level by level along the hierarchy to generate private keys for its descendants.

In order to resolve key escrow problem resulted from the capability of private keys in private key derivation, the function of private keys being as eligible credentials for private key derivation is disabled in our HIBE system, However, a means for authorizing an entity to be capable of deriving private keys for its descendants is provided. That we call Authorized Delegation.

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, $\ldots$, I_{j-1}, i.e., by introducing two independent components defined on non-local identifiers with respect to hierarchy $I_1 \rightarrow \ldots \rightarrow I_{j-1}$ 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.

2 Preliminaries

In this section, we briefly review bilinear pairing and HIBE systems.

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).

The bilinear pairing is called symmetric if $\hat{\mathbb{G}}$ is $\mathbb{G}$, denoted Λ_{sym}.

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.

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.

3.1 Construction

- $\mathbf{Setup}(1^k, \ell) \rightarrow \Lambda, params, mk$. 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 $\Lambda = (\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T, q, e)$, where q is of k binary bits, $\mathbb{G}$, $\hat{\mathbb{G}}$, $\mathbb{G}_T$ 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 $\mathbb{Z}_q$, 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 $\mathbb{Z}_q$, 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 $params \in \mathbb{G}^{2\ell+3} \times \hat{\mathbb{G}}^{2\ell+3} \times \mathbb{G}_T$ and the master secret $mk \in \hat{\mathbb{G}}$ are expressed as

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

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

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

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 $I_1 \rightarrow \ldots \rightarrow I_{j-1}$, 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.

- **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

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

- $\mathbf{Encrypt(pa\ rams, ID_j, M) \rightarrow C_{ID_j}}$. 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

$$C_{ID_j} = \Big(Mv^s, sg, s\Big(\sum_{k=1}^{j-1} I_k l_k + h_0\Big), s\big(I_j g_1 + h_j\big)\Big). \quad (4)$$

- $\mathbf{Decrypt\big(params, d_{ID_j}, C_{ID_j}\big) \rightarrow M}$. 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

$$M = C_0 \cdot e(C_2, d_1) \cdot e(C_3, d_2) / e(C_1, d_0). \quad (5)$$

3.2 Correctness of Our HIBE Construction

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 $ID_j = (I_1, \ldots, I_j) \in (\mathbb{Z}_q^*)^j$, 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

$$M' = C_0 \cdot e(C_2, d_1) \cdot e(C_3, d_2) / e(C_1, d_0)$$
$$= Mv^s \cdot e\Big(s\Big(\sum_{k=1}^{j-1} I_k l_k + h_0\Big), r_0\hat{g}\Big) \cdot e\big(s\big(I_j g_1 + h_j\big), r_1\hat{g}\big) /$$
$$e\Big(sg, \hat{g}_0 + r_0\Big(\sum_{k=1}^{j-1} I_k \hat{l}_k + \hat{h}_0\Big) + r_1\big(I_j \hat{g}_1 + \hat{h}_j\big)\Big)$$
$$= M.$$

That is, our HIBE system constructed above is consistent.

4 Private Key Derivation with Authorized Secret

To calculate a secret $S_{(i,ID_j)} = (S_0, S_1, S_2, R_{i+1}, \ldots, R_{j-1}) \in \hat{\mathbb{G}}^{j-i+2}$ for (ID_i, ID_j) with ID_i being a prefix of ID_j, pick two random numbers r_0, r_1 from $\mathbb{Z}_q$, and output

$$S_{(i,ID_j)} = \Big(\hat{g}_0 + r_0\Big(\sum_{k=1}^{i} I_k \hat{l}_k + \hat{h}_0\Big) + r_1\big(I_j \hat{g}_1 + \hat{h}_j\big), r_0\hat{g}, r_1\hat{g}, r_0\hat{l}_{i+1}, r_0\hat{l}_{i+2}, \ldots, r_0\hat{l}_{j-1} \Big), \quad (6)$$

where $j-i-1$ components R_{i+1}, …, 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 $_j$.

5 Conclusion

Identifier Discrimination is proposed in this paper as technique of composing private keys for identities in HIBE systems, with which a HIBE system with constant size ciphertext and authorized delegation is constructed. Private key for identity $ID_j = (I_1, \ldots, I_{j-1}, I_j)$ is the result of randomizing the master key of the HIBE system with two logically independent components, i.e., $r_0(\sum_{k=1}^{j-1} I_k \hat{l}_k + \hat{h}_0)$ and $r_1(I_j \hat{g}_1 + \hat{h}_j)$. As a result, Private key in our HIBE system contains only three elements from $\hat{\mathbb{G}}$, and ciphertext includes three group elements with one element from $\mathbb{G}_T$ and two elements from $\mathbb{G}$, regardless of depth of identity hierarchy.

Because there is no means of canceling out the component defined on local identifier with level-dependent parameter from private key for the entity in order to generate an eligible secret for deriving private keys for its descendant identities, any entity in our HIBE system is prevented from deriving private keys for any of its descendants, thus resolving the key escrow problem. However, any entity can be authorized by the root PKG to be capable of deriving private keys for any of its descendants by distributing a copy of specially crafted credentials, with which an eligible secret for deriving private keys for the descendant can be deduced. That is, authorized delegation is achieved.

References

1. Boneh, D., Boyen, X.: Efficient selective-id secure identity-based encryption without random oracles. In: Cachin, C., Camenisch, J. (eds.) Advances in Cryptology - EUROCRYPT 2004, LNCS, vol. 3027, pp. 223–238. Springer Berlin Heidelberg (2004)
2. Boneh, D., Boyen, X.: Secure identity based encryption without random oracles. In: Franklin, M. (ed.) Advances in Cryptology - CRYPTO 2004, LNCS, vol. 3152, pp. 443–459. Springer Berlin Heidelberg (2004)
3. Boneh, D., Boyen, X.: Efficient selective identity-based encryption without random oracles. Journal of Cryptology 24(4), 659–693 (2011)
4. Boneh, D., Boyen, X., Goh, E.J.: Hierarchical identity based encryption with constant size ciphertext. In: Cramer, R. (ed.) Advances in Cryptology - EUROCRYPT 2005, LNCS, vol. 3494, pp. 440–456. Springer Berlin Heidelberg (2005)
5. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. SIAM J. Comput. 32(3), 586–615 (Mar 2003)
6. Cocks, C.: 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, vol. 2260, pp. 360–363. Springer Berlin Heidelberg (2001)
7. Gentry, C., Silverberg, A.: Hierarchical id-based cryptography. In: Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology. pp. 548–566. ASIACRYPT'02, Springer-Verlag, London, UK, UK (2002)
8. Horwitz, J., Lynn, B.: Toward hierarchical identity-based encryption. In: Knudsen, L. (ed.) Advances in Cryptology - EUROCRYPT 2002, LNCS, vol. 2332, pp. 466–481. Springer Berlin Heidelberg (2002)
9. Lewko, A., Waters, B.: New techniques for dual system encryption and fully secure hibe with short ciphertexts. In: Micciancio, D. (ed.) Theory of Cryptography, LNCS, vol. 5978, pp. 455–479. Springer Berlin Heidelberg (2010)
10. Waters, B.: Efficient identity-based encryption without random oracles. In: Cramer, R. (ed.) Advances in Cryptology - EUROCRYPT 2005, LNCS, vol. 3494, pp. 114–127. Springer Berlin Heidelberg (2005)
11. Waters, B.: Dual system encryption: Realizing fully secure ibe and hibe under simple assumptions. In: Halevi, S. (ed.) Advances in Cryptology - CRYPTO 2009, LNCS, vol. 5677, pp. 619–636. Springer Berlin Heidelberg (2009)

