Hierarchical Identity-Based Encryption with Constant-Size Private Keys

Leyou Zhang, Qing Wu, and Yupu Hu

The main challenge at present in constructing hierarchical identity-based encryption (HIBE) is to solve the trade-off between private-key size and ciphertext size. At least one private-key size or ciphertext size in the existing schemes must rely on the hierarchy depth. In this letter, a new hierarchical computing technique is introduced to HIBE. Unlike others, the proposed scheme, which consists of only two group elements, achieves constant-size private keys. In addition, the ciphertext consists of just three group elements, regardless of the hierarchy depth. To the best of our knowledge, it is the first efficient scheme where both ciphertexts and private keys achieve O(1)-size, which is the best trade-off between private-key size and ciphertext size at present. We also give the security proof in the selective-identity model.

Keywords: HIBE, large-scale network, identity-based encryption, standard model, selective-identity security.

I. Introduction

Identity-based encryption (IBE), introduced by Shamir [1], allows for a party to encrypt a message using the recipient's identity as a public key. The ability to use identities as public keys eliminates the need for certificates as used in a traditional public-key infrastructure. The first efficient IBE was provided in [2]. Although the advantages of IBE are compelling, having a single private-key generator (PKG) would completely eliminate online lookup of public keys or public parameters. However, it is undesirable for a large network because the single PKG becomes a bottleneck: (i) private-key generation is computationally expensive, (ii) the single PKG must verify proofs of identities, and (iii) the single PKG must establish secure channels to transmit private keys. Hence, a hierarchical structure for IBE is needed. Hierarchical IBE (HIBE) is a generalization of IBE. It allows a root PKG to distribute the workload by delegating private-key generation and identity authentication to lower-level PKGs. In a HIBE scheme, a root PKG needs only to generate private keys for domain-level PKGs, which in turn generates private keys for users in their domains in the next level. Authentication and private-key transmission can be done locally. Another advantage of HIBE schemes is damage control as disclosure of domain PKG secrets do not compromise the secrets of higher-level PKGs.

In this letter, we focus on HIBE. Interest in HIBE is spurred by its applications. It is especially useful in large companies or e-government systems where there are hierarchical administrative issues. HIBE provides one of the most direct and practical solutions to the key exposure problem for public-key infrastructure applications that occur in daily life. Recently, Sun and Fang [3] applied it to the Electronic Health Record system. In [4], the authors also used it to strengthen the cloud computing security. More recently, Smart and Warinschi proposed a new construction of group signature from HIBE [5]. The first efficient construction for HIBE was due to Gentry and Silverberg [6], where security was based on the bilinear Diffie-Hellman (BDH) assumption in the random oracle model. The first construction without random oracles was given by Boneh and Boyen [7] based on decision BDH. Many schemes without random oracles were proposed [8]-[16] based on the bilinear pairing. The most recent constructions were introduced based on hard problems on lattices [17], [18]. In these schemes, the secret key is a "short" basis B of a certain integer lattice L. To

Manuscript received Apr. 7, 2011; revised June 13, 2011; accepted July 1, 2011.

This work was partially supported by the Nature Science Foundation of China under grant (61100231, 60970119, 61100165), and the Fundamental Research Funds for the Central Universities of China (K50511700003).

Leyou Zhang (phone: +86 29 8802860, leyouzhang77@yahoo.com.cn) is with the Department of Mathematics, Xidian University, Xi'an, China.

Qing Wu (xidianwq@yahoo.com.cn) is with the School of Automation, Xi'an University of Posts and Telecommunications, China.

Yupu Hu (yphu@mail.xidian.edu.cn) is with the Key Lab of CNIS, Xidian University, China.

http://dx.doi.org/10.4218/etrij.12.0211.0140

 © 2012 ETRI

delegate the key to a child, the parent creates a new lattice L_0 derived from L and uses B to generate a random short basis for this lattice L_0. In all previous constructions, the dimension of the child lattice L_0 is larger than the dimension of the parent lattice L. As a result, private keys or ciphertexts become longer as one descends into the hierarchy.

However, the drawbacks of the previous works are obvious. In [7]-[11], [13]-[18], the private keys all depend on the hierarchy and maximum hierarchy. In [7], [13], [17], [18], the ciphertexts also depend on hierarchy or maximum hierarchy. These drawbacks directly increase the computation cost of the senders and storage cost of the users.

As a natural extension of the efforts to improve schemes, we present a new efficient HIBE. As a new technique, we change the master private keys to two parts: main master private keys and shared private keys created by the PKGs. It results a new construction which is different from the previous schemes. The ciphertext size as well as the private-key size is independent of the hierarchy depth. Ciphertexts in our system are always just three group elements, and decryption requires two bilinear pairing. Private keys in our scheme only contain two group elements. It is a desirable feature since it is the first scheme whose private keys and ciphertexts achieve $O(1)$-size. However, our scheme only achieves selective-identity security, which is a weak security for identity-based cryptography.

II. Preliminaries

1. Selective-Identity Security Model

The selective-identity security model for HIBE (chosen plaintext secure (*IND-sID-CPA*)) is defined as the following game between an adversary and a simulator.

Init. The adversary outputs an identity challenge ID^*.

Setup. The simulator sets up the HIBE protocol and provides the public parameters to the adversary and keeps the master key to itself.

Phase 1. The adversary issues queries $q_1,\ldots, q_m$ where each query q_i is one of the following:

-Private-key query. The adversary issues a private-key query for ID_i where $ID_i \neq ID^*$, and ID_i is not a prefix of ID^*. The simulator responds by running algorithm *Key Generation* to generate the private key d_i corresponding to the public key ID_i. It sends d_i to the adversary.

Challenge. Once the adversary decides that phase 1 is over, it outputs two equal length plaintexts, M_0 and M_1, on which it wishes to be challenged. The simulator picks a random bit $b \in \{0, 1\}$ and sets the challenge ciphertext to C=*Encryption*($param$, ID^*, M_b). It sends C as the challenge to adversary.

Phase 2. The adversary issues additional queries as phase 1 with constraint $ID_i \neq ID^*$, and ID_i is not a prefix of ID^*.

Guess. Finally, the adversary outputs a guess $b' \in \{0, 1\}$ and wins if $b = b'$.

2. Decisional BDH Exponent Problem (n+1-BDHE).

Given a tuple $(g, y_0, y_1,\ldots, y_n, y_{n+2},\ldots, y_{2n+2}, T)$, where $y_i = g^{\alpha^i}$ and $y_0 = g^c$, decide $T = e(g,g)^{\alpha^{n+1}c}$ or random in G_1. The (t, ε)-decisional n+1-BDHE assumption holds if no t-time algorithm has a non-negligible advantage ε in solving the above game.

III. New Construction

1. Our Scheme

Let G be a group of prime order p, g be a random generator of G, and l denote the maximum depth of HIBE.

Setup. Pick $\alpha, \alpha_{i1},\ldots,\alpha_{in}, \beta_{i1},\ldots,\beta_{in}$ in Z_p at random for $1 \le i \le l$. Set $g_1 = g^\alpha$, then choose g_2 randomly in G. The public key is PK=$\{g, g_1, g_2\}$. The master key is g_2^α. At hierarchy depth i, PKG_i is given the shared master key Msk_i=$\{\alpha_{i1},\ldots,\alpha_{in}, \beta_{i1},\ldots,\beta_{in}\}$.

Key Generation.

For the first level ID=(v_1) with $v_1 = (v_{11},\cdots, v_{1n})$, $v_{1j} \in \{0,1\}$, PKG first computes $h_{1i} = (h_{1(i-1)})^{\alpha_{1i}^{v_{1i}}\beta_{1i}^{1-v_{1i}}}$, $1 \le i \le n$, where h_{10}=g. Then, the private key for ID is generated by

$$d_{ID} = (d_0, d_1) = (g_2^\alpha h_{1n}^r, g^r), \text{ where } r \in Z_p.$$

For the k-th level ID=$(v_1,\cdots,v_k)$ $(k \le l)$ with $v_i = (v_{i1},\cdots, v_{in})$ and $v_{ij} \in \{0,1\}$, by using the parent $(k-1)$th level ID = $(v_1,\cdots, v_{k-1})$ and the corresponding private key

$$d'_{ID} = (d'_0, d'_1) = (g_2^\alpha (\prod_{i=1}^{k-1} h_{in})^r, g^r),$$

PKG_i first generates the auxiliary information parameters as follows. Let $h'_{k0} = d'_1$. For $1 \le j \le n$, PKG_i computes $h'_{kj} = (h'_{k(j-1)})^{\alpha_{kj}^{v_{kj}}\beta_{kj}^{1-v_{kj}}} = (g^r)^{\prod_{i=1}^{n}\alpha_{ki}^{v_{ki}}\beta_{ki}^{1-v_{ki}}}$. Set $h_{kn} = g^{\prod_{i=1}^{n}\alpha_{ki}^{v_{ki}}\beta_{ki}^{1-v_{ki}}}$. Then, one can obtain $h'_{kn} = (h_{kn})^r$. The private key for ID is

$$d_{ID} = (d_0, d_1) = (d'_0 h'_{kn}, d'_1) = (g_2^\alpha (\prod_{i=1}^{k} h_{in})^r, g^r).$$

Encryption. Let M be an encrypted message. Then, the ciphertexts can be computed by

$$C = (C_0, C_1, C_2) = (e(g_1, g_2)^s M, g^s, (\prod_{i=1}^{k} h_{in})^s),$$

where s is selected randomly in Z_p.

Decryption. Let C be valid ciphertexts. Then, the message M can be recovered by the private key d_{ID}=(d_0, d_1) as follows:

$$M = C_0 \frac{e(d_1, C_2)}{e(d_0, C_1)}.$$

Correctness. For a valid ciphertext, we have

$$\frac{e(d_1,C_2)}{e(d_0,C_1)}=\frac{e(g^r,(\prod_{i=1}^{k}h_{in})^s)}{e(g_2^{\alpha}(\prod_{i=1}^{k}h_{in})^r,g^s)}=\frac{1}{e(g_2^{\alpha},g^s)}=\frac{1}{e(g_2,g_1)^s}.$$

2. Efficiency

Based on the new technique, the private keys in our scheme achieve $O(1)$-size. However, in previous HIBE systems, private-key size depends on the identity depth. In addition, the ciphertext of the proposed scheme contains only 3 elements, and decryption takes only 2 pairings. It is worth noting that $e(g_1, g_2)$ used for encryption can be precomputed. Hence, encryption does not require any pairings. Table 1 gives the comparison between our scheme and the available. In Table 1, k denotes the hierarchy depth, $k \le l$, and pk is the private key.

3. Security Analysis

Theorem. Suppose the decisional n+1-BDHE assumption holds in G, then the proposed scheme is secure in the selective-identity model.

Proof. Assume that there is an adversary A that breaks the proposed scheme with advantage ε. We show how to build an adversary B that solves the decisional n+1-BDHE problem with advantage $\varepsilon/2^{kn}$. For a generator $g \in G$ and $\alpha, c \in Z_p$, we set $y_i = g^{\alpha^i}$ and $y_0 = g^c$. Algorithm B is given a random tuple $(g, y_0, y_1, \ldots, y_n, y_{n+2}, \ldots, y_{2n+2}, T)$. Algorithm B's goal is to output 1 when $T = e(g,g)^{\alpha^{n+1}c}$ and 0 otherwise. □

Init. The adversary A first outputs an identity $ID^*=(v_1^*,\ldots,v_k^*)$ of depth $k \le l$ that it wants to attack.

Setup. To generate the system parameters, B sets $g_1=y_1$. Then, it selects randomly $\gamma, \alpha_{ij}, \beta_{ij}$ and sets $g_2 = y_n g^{\gamma} = g^{\alpha^n+\gamma}$, where $1 \le i \le l$, $1 \le j \le n$. The master key is set as g_2^{α}. For any level i, the master keys Msk_i are set as

$$Msk_i=(\alpha_{ij}\alpha^{v_{ij}^*}, \beta_{ij}\alpha^{1-v_{ij}^*}),\ 1 \le i \le l, 1 \le j \le n.$$

Table 1. Comparison of efficiency.

Scheme	Ciphertext size	*pk* size	*PK* size
[7]	$O(k)$	$O(k)$	$O(l)$
[8]	$O(1)$	$O(l-k)$	$O(l)$
[13]	$O(k)$	$O(k)$	$O(l)$
[14]	$O(1)$	$O(l-k)$	$O(l)$
[15]	$O(1)$	$O(l-k)$	$O(l)$
[17]	$O(klnd^2)$	$O(k^2l^3n^2d^2)$	$O(kn^2d^3)$
[18]	$O(lnd^2)$	$O(l^3n^2d^2)$	$O(n^2d^3)$
Proposed	$O(1)$	$O(1)$	$O(k)$

The public key is $PK=\{g, g_1, g_2\}$.

Finally, B sends the PK to A. The corresponding master keys are unknown to B.

Phase 1. The adversary A issues up to q_s private-key queries. Each query q_i is described as follows. Let $ID=(v_1,\cdots,v_k)$ denote the corresponding identity. The restriction is that ID is not ID^* or a prefix of ID^*. This restriction shows that there exists a j such that $v_j \ne v_j^*$. To respond the query, B first derives the auxiliary information parameters as

$$h_{i1}=\begin{cases} g^{\alpha_{i1}^{v_{i1}}\beta_{i1}^{1-v_{i1}}} & \text{if } v_{i1} \ne v_{i1}^* \\ y_1^{\alpha_{i1}^{v_{i1}}\beta_{i1}^{1-v_{i1}}} & \text{if } v_{i1} = v_{i1}^* \end{cases},$$

$$h_{i2}=\begin{cases} h_{i1}^{\alpha_{i2}^{v_{i2}}\beta_{i2}^{1-v_{i2}}} & \text{if } v_{i2} \ne v_{i2}^* \\ y_1^{\alpha_{i2}^{v_{i2}}\beta_{i2}^{1-v_{i2}}} & \text{if } v_{i2} = v_{i2}^* \wedge v_{i1} \ne v_{i1}^* \cdots \\ y_2^{\alpha_{i2}^{v_{i2}}\beta_{i2}^{1-v_{i2}}} & \text{if } v_{i2} = v_{i2}^* \wedge v_{i1} = v_{i1}^* \end{cases}$$

where $1 \le i \le k$. Then, all auxiliary information parameters can be obtained.

Next, B first generates the private keys for $ID_j=(v_1,\ldots,v_j)$ where j denotes the first element such that $v_j \ne v_j^*$. To simplify, we suppose that t denotes the number of positions such that $v_{ji} = v_{ji}^*$. Then, one can obtain

$$h_{1n} = y_n^{T(v_1)}, \cdots, h_{(j-1)n} = y_n^{T(v_{j-1})},\ h_{jn} = y_t^{T(v_j)},$$

where $T(v_k)=\prod_{i=1}^{n}\alpha_{ki}^{v_{ki}}\beta_{ki}^{1-v_{ki}}$ for $1 \le k \le j$ and $t<n$.

B chooses randomly $r' \in Z_p$. Then, the private key is simulated as $d_{ID}=(d_0,d_1)=(g_2^{\alpha}(\prod_{i=1}^{j}h_{in})^{r'}, g^{r'})$, where $r=r'-\frac{\alpha^{n-t+1}}{T(v_j)}$. In fact, one can verify the following holds:

$$\begin{aligned}
&g_2^{\alpha}(\prod_{i=1}^{j}h_{in})^{r} \\
&= y_{n+1}y_1^{\gamma}(\prod_{i=1}^{j}h_{in})^{r'-\frac{\alpha^{n-t+1}}{T(v_j)}} \\
&= y_{n+1}y_1^{\gamma}(\prod_{i=1}^{j-1}h_{in})^{r}h_{jn}^{r'-\frac{\alpha^{n-t+1}}{T(v_j)}} = y_{n+1}y_1^{\gamma}(\prod_{i=1}^{j-1}h_{in})^{r}h_{jn}^{r'}h_{jn}^{-\frac{\alpha^{n-t+1}}{T(v_j)}} \\
&= y_{n+1}y_1^{\gamma}(\prod_{i=1}^{j-1}h_{in})^{r'-\frac{\alpha^{n-t+1}}{T(v_j)}}(y_t^{T(v_j)})^{r'}(y_t^{T(v_j)})^{-\frac{\alpha^{n-t+1}}{T(v_j)}} \\
&= y_{n+1}y_1^{\gamma}(\prod_{i=1}^{j-1}y_n^{T(v_i)})^{r'-\frac{\alpha^{n-t+1}}{T(v_j)}}(y_t^{T(v_j)})^{r'}y_{n+1}^{-1} \\
&= y_1^{\gamma}(\prod_{i=1}^{j-1}y_n^{T(v_i)})^{r'}(\prod_{i=1}^{j-1}y_{2n-t+1}^{-\frac{T(v_i)}{T(v_j)}})(y_t^{T(v_j)})^{r'},
\end{aligned}$$

Since y_{n+1} is cancelled out, all the terms in this expression are known to B. Thus, B can compute the first private-key component. The second component, $g^{r'}$, is $y_{n-t+1}^{-\frac{1}{T(v_j)}}g^{r'}$ (since $t<n$, y_{n-t+1} is known to B), which B can compute. So the simulation is perfect. Using the private keys of $ID_j=(v_1,\ldots,v_j)$, B can generate the private keys of $ID=(v_1,\ldots,v_k)$.

Challenge. When A decides that phase 1 is over, it outputs two messages $M_0, M_1 \in G_1$ on which it wishes to be challenged. First, B generates the auxiliary information parameters for challenge identity ID^* as $h_{in} = g^{T(v_i^*)}$ with $1 \le i \le k$. B picks a random bit $b \in \{0, 1\}$ and responds with the challenge ciphertext for ID^* in the following manner:

$$C^* = (C_0^*, C_1^*, C_2^*) = (M_b Te(y_1^\gamma, y_0), y_0, y_0^{\sum_{i=1}^k T(v_i^*)}).$$

If $T = e(g,g)^{\alpha^{n+1}c}$, then the challenge ciphertext is a valid encryption of M_b under the identity ID^*. In fact,

$$\begin{aligned} C_0^* &= M_b Te(y_1^\gamma, y_0) = M_b e(g,g)^{\alpha^{n+1}c} e(y_1^\gamma, y_0) \\ &= M_b e(g^{\alpha^n}, g^{\alpha c}) e(y_1^\gamma, y_0) = M_b e(y_n, y_1)^c e(g^\gamma, y_1)^c \\ &= M_b e(y_n g^\gamma, y_1)^c = M_b e(g_2, g_1)^c, \\ C_1^* &= y_0 = g^c, \\ C_2^* &= y_0^{\sum_{i=1}^k T(v_i^*)} = (g^{\sum_{i=1}^k T(v_i^*)})^c = (\prod_{j=1}^k g^{T(v_j^*)})^c = (\prod_{j=1}^k h_{jn})^c. \end{aligned}$$

On the other hand, when T is uniform, C^* is independent of b in the adversary's view.

Note that from the received inputs, A gets no information at all about the ID^* chosen by B, thus such a choice will be identical to the challenge identity with probability $1/2^{kn}$.

Phase 2. A continues to issue queries as phase 1. B responds as before.

Guess. Finally, A outputs a guess $b' \in \{0,1\}$. B concludes its own game by outputting a guess as follows. If $b=b'$, then B outputs 1 meaning $T = e(g,g)^{\alpha^{n+1}c}$. Otherwise, it outputs 0 meaning T is random in G_1.

Therefore, if A breaks the proposed scheme with advantage ε, B solves the decisional n+1-BDHE problem with advantage $\varepsilon/2^{kn}$.

IV. Conclusion

In this letter, we introduced a new method to construct HIBE. Our new scheme achieves constant-size private keys and ciphertexts, which is the best trade-off at present. Unfortunately, our scheme only achieves selective-identity security. A natural question left open by this letter is to construct a HIBE system that is secure under a more standard assumption or achieves a stronger security notion.

References

[1] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," *Proc. CRYPTO*, *LNCS*, vol. 196, 1985, pp. 47-53.

[2] D. Boneh and M. Franklin. "Identity Based Encryption from the Weil Pairing," *Proc. CRYPTO*, *LNCS*, vol. 2139, 2001, pp. 213-229.

[3] J. Sun and Y. Fang, "Cross-Domain Delegation for Sensitive Data Sharing in Distributed Electronic Health Record Systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 6, 2010, pp. 754-764.

[4] L. Yan, C.M. Rong, and G.S. Zhao, "Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography," *CloudCom*, *LNCS*, vol. 5931, 2009, pp. 167-177.

[5] N.P. Smart and B. Warinschi, "Identity Based Group Signatures from Hierarchical Identity-Based Encryption," *Pairing*, *LNCS*, vol. 5671, 2009, pp. 150-170.

[6] C. Gentry and A. Silverberg, "Hierarchical ID-Based Cryptography," *Proc. ASIACRYPT*, *LNCS*, vol. 2501, 2002, pp. 548 -566.

[7] D. Boneh and X. Boyen, "Efficient Selective-ID Secure Identity-Based Encryption without Random Oracles," *Proc. EUROCRYPT*, *LNCS*, vol. 3027, 2004, pp. 223-238.

[8] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Ciphertext," *Proc. EUROCRYPT*, *LNCS*, vol. 3494, 2005, pp. 440-456.

[9] J.H. Seo and J.H. Cheon, "Fully Secure Anonymous Hierarchical Identity-Based Encryption with Constant Size Ciphertexts." http://eprint.iacr.org/2011/021

[10] J.H. Seo et al., "Anonymous Hierarchical Identity-Based Encryption with Short Ciphertexts," *IEICE Trans. Fundamentals*, vol. E94.A, no. 1, 2011, pp. 45-56.

[11] X.M. Hu, S.T. Huang, and X. Fan, "Practical Hierarchical Identity Based Encryption Scheme without Random Oracles," *IEICE Trans. Fundamentals Electron. Commun. Comput. Sci.*, E92.A, no. 6, June 2009, pp. 1494-1499.

[12] B. Waters, "Efficient Identity-Based Encryption without Random Oracles," *Proc. EUROCRYPT*, *LNCS*, vol. 3494, 2005, pp. 114-127.

[13] B. Waters, "Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions," *Proc. CRYPTO, LNCS*, vol. 5677, 2009, pp. 619-636.

[14] A. Lewko and B. Waters, "New Techniques for Dual System Encryption and Fully Secure HIBE with Short Ciphertexts," *Proc. TCC*, *LNCS*, vol. 5978, 2010, pp. 455-479.

[15] Y.L. Ren and D.W. Gu. "Efficient Hierarchical Identity Based Encryption Scheme in the Standard Model," *Informatica*, vol. 32, no. 2, 2008, pp. 207-211.

[16] X. Wang and X. Yang, "Cryptanalysis of Two Efficient HIBE Schemes in the Standard Model," Cryptology ePrint Archive, Report 2010/113, 2010.

[17] D. Cash, D. Hofheinz, and E. Kiltz, "How to Delegate a Lattice Basis," Cryptology ePrint Archive, Report 2009/351 (2009). http://eprint.iacr.org/

[18] S. Agrawal, D. Boneh, and X. Boyen, "Efficient Lattice (H)IBE in the Standard Model," *Proc. EUROCRYPT*, *LNCS*, vol. 6110, 2010, pp. 553-572.