Efficient Hierarchical Identity Based Encryption Scheme in the Standard Model

Yanli Ren and Dawu Gu
Dept. of Computer Science and Engineering
Shanghai Jiao Tong University
Shanghai 200240, China
E-mail: {renyanli1982,dwgu}@situ.edu.cn

Keywords: hierarchical, identity based, standard model

Received: September 12, 2007

Constructing identity based schemes is one of the hot topics of current cryptography. Hierarchical identity based cryptography is a generalization of identity based encryption that mirrors an organizational hierarchy. It allows a root public key generator to distribute the workload by delegating public key generation and identity authentication to lower-level public key generators. Currently, there is no hierarchical identity based encryption scheme that is fully secure in the standard model, with short public parameters and a tight reduction. In this paper, we propose an anonymous hierarchical identity based encryption scheme based on the q-ABDHE problem that is fully secure in the standard model. The ciphertext size is independent of the level of the hierarchy. Moreover, our scheme has short parameters, high efficiency and a tight reduction.

Povzetek: Opisana je kriptografska metoda za hierarhično identifikacijo.

1 Introduction

Identity based (ID-based) cryptosystem [1] is a public key cryptosystem where the public key can be represented as an arbitrary string such as an email address. A private key generator(PKG) uses a master secret key to issue private keys to identities that request them. For an Identity Based Encryption (IBE) scheme, Alice can securely encrypt a message to Bob using an unambiguous name of him, such as email address, as the public key. For an Identity Based Signature (IBS) scheme, Alice can sign a message using her private key that corresponds to Aliceąŕs identity. Then anybody can verify the authenticity of the signature from the identity.

The concept was proposed by Shamir in 1984. However, practical IBE schemes were not found until the work of Boneh and Franklin in 2001 [8]. Their scheme is provably secure in the random oracle model. Almost all of the IBE systems since Boneh-Franklin follow the "common strategy" for proving security; consequently, they suffer from long parameters (when security is proven in the standard model) and lossy reductions (in the standard model or the random oracle model). The IBE systems described in [5] have short parameters and achieve a tight reduction, but this is because they are proven secure only against selective-ID attacks. In 2006, Genty proposed an anonymous IBE scheme [4] that is fully secure in the standard model with a tight reduction. Anonymity means that there is no adversary can distinguish two ciphertexts of same message with two identities in polynomial time.

Hierarchical ID-based cryptography was first proposed in [3] and [9] in 2002. It is a generalization of IBE that mirrors an organizational hierarchy. And it allows a root PKG to distribute the workload by delegating private key generation and identity authentication to lower-level PKGs. In a hierarchical ID-based encryption (HIBE) scheme, a root PKG only needs to generate private keys for domain-level PKGs, who in turn generate private keys for their users in the domains of the lower level. To encrypt a message to Bob, Alice only needs to obtain the public parameters of Bob's root PKG and his identity. It is especially useful in large companies or e-government structure where there are hierarchical administrative issues needed to be taken care.

The first construction for HIBE is due to Gentry and Silverberg [3] where security is based on the Bilinear Diffie-Hellman (BDH) assumption in the random oracle model. A subsequent construction due to Boneh and Boyen gives an efficient (selective-ID secure) HIBE based on BDH without random oracles [5]. But the ciphertext length is linear in the depth of the hierarchy. In 2005, they proposed a hierarchical identity based encryption with constant size ciphertext and proved it is selective-ID secure in the standard model [7]. Moreover, the size of public parameters is independent of the number of bit representing an identity, while the size of public parameters of the scheme in [11] grows with a factor of h, where h is the number of block to represent an identity of n bits, with each block using n/h bits. In 2006, Man Ho Au constructed a HIBE scheme that is fully secure in the standard model [10]. However, the scheme can not convert to an IBE scheme, that is to say, it is only valid for a user with identity $ID = (ID_1, ID_2, \ldots, ID_i), i \geq 2$. Moreover, the adversary can compute the private key of ID_1 after requesting private key of its children and the

$q - SDH$ problem can not be solved exactly during the reduction. At the same year, an anonymous HIBE [12] is proposed. But the ciphertext size is dependent to the level of the hierarchy. In addition, the scheme has long parameters, large computation and the reduction is not tight. Currently, there is no HIBE scheme that is fully secure in the standard model, with short public parameters and a tight reduction.

Our Contributions. In this paper, we propose a constant size anonymous HIBE scheme that is fully secure in the standard model. The ciphertext size is independent of the level of the hierarchy. Compared to the previous HIBE schemes, our scheme has shorter parameters, higher efficiency and a tighter reduction.

Our scheme is based on Gentry's IBE scheme, and we convert it to a HIBE scheme. However, the conversion is not straightforward. Several techniques have to suitably combined to obtain the required proof. Moreover, our scheme decreases the redundancy of Gentry's scheme.

2 Definitions

Before presenting the hierarchical identity based encryption scheme, we introduce some difficult problems and security models of the scheme first.

2.1 Bilinear Map

Let p be a large prime number, G_1, G_2 are two groups of order p, g is a generator of G_1. $e : G_1 \times G_1 \rightarrow G_2$ is a bilinear map, which satisfies the following properties [2]:

(1)Bilinearity: For all $u, v \in G_1$ and $a, b \in Z$, $e(u^a, v^b) = e(u, v)^{ab}$.

(2)non-degeneracy: $e(g, g) \neq 1$.

(3)Computability: There exists an efficient algorithm to compute $e(u, v)$,

$\forall u, v \in G_1$.

2.2 Complexity Assumption

The security of our scheme is based on a complexity assumption that we call the q-augmented bilinear Diffie-Hellman exponent (ABDHE) problem [4].

q-ABDHE problem

Let g, g' be generators of G_1. Given $(g, g^\alpha, \ldots, g^{\alpha^q}, g', g'^{\alpha^{q+2}}, T) \in G_1^{q+3} \times G_2$, where $\alpha \in Z_p^*$, decide whether $T = e(g, g')^{\alpha^{q+1}}$.

Since the tuple has not the term $g^{\alpha^{q+1}}, g'^{\alpha^{q+1}}$, the bilinear map does not seem to help decide whether $T = e(g, g')^{\alpha^{q+1}}$. Introducing the additional term $g'^{\alpha^{q+2}}$ still does appear to ease the decision of $e(g, g')^{\alpha^{q+1}}$, since the tuple is missing the term $g^{\alpha^{-1}}$. we say the q-ABDHE problem is (t, ε)-difficult in G_1, G_2, if no t-time algorithm has advantage at least ε in solving the q-ABDHE problem.

An algorithm A that outputs $b \in \{0, 1\}$ has advantage ε in solving the decision q-ABDHE if

$$|Pr[A(g', g'^{\alpha^{q+2}}, g, g^\alpha, \ldots, g^{\alpha^q}, e(g', g)^{\alpha^{q+1}}) = 0] \\ -Pr[A(g', g'^{\alpha^{q+2}}, g, g^\alpha, \ldots, g^{\alpha^q}, T) = 0]| \geq \varepsilon,$$

where the probability is over the random choice of generators $g, g' \in G_1, \alpha \in Z_p^*, T \in G_2$, and the random bits consumed by A. We refer to the distribution on the left as P_{ABDHE} and the distribution on the right as R_{ABDHE}.

We say that the decision (t, ε, q)-ABDHE assumption holds in G_1, G_2 if no t-time algorithm has advantage at least ε in solving the decision q-ABDHE problem in G_1, G_2.

2.3 Secure Model

IND-ID-CCA2: Boneh and Franklin defined chosen ciphertext security for IBE systems under a chosen ciphertext attack via the following game [6,8].

Setup: The challenger runs Setup, and forwards parameters to the adversary.

Phase 1: Proceeding adaptively, the adversary issues queries $q_1, \ldots, q_m$ where q_i is one of the following:

Key generation query $< ID_i >$: the challenger runs *KeyGen* on ID_i and forwards the resulting private key to the adversary.

Decryption query $< ID_i, c_i >$. The challenger runs *KeyGen* on ID_i, decrypts c_i with the resulting private key, and sends the result to the adversary.

Challenge: The adversary submits two plaintexts m_0, m_1 and an identity ID^*. ID^* or its prefix must not have appeared in any key generation query in Phase 1. The challenger selects a random bit $b \in \{0, 1\}$, sets $c^* = Encrypt(params, ID^*, m_b)$, and sends c^* to the adversary as its challenge ciphertext.

Phase 2: This is identical to Phase 1, except that the adversary may not request a private key for ID^* or the decryption of (ID^*, c^*).

Guess: The adversary submits a guess $b' \in \{0, 1\}$. The adversary wins if $b' = b$.

We call an adversary A in the above game an IND-ID-CCA adversary. The advantage of an adversary A in this game is defined as $Pr[b' = b] - \frac{1}{2}$.

Definition 1. An HIBE system is $(t, \varepsilon, q_e, q_d)$ IND-ID-CCA secure if all t-time IND-ID-CCA adversaries making at most q_e key generation queries and at most q_d decryption queries have advantage at most ε in winning the above game.

ANON-ID-CCA2: Informally, we say that an HIBE system is anonymous if an adversary cannot distinguish the public key ID under which a ciphertext was generated. More formally, we define anonymity for HIBE systems under a chosen ciphertext attack via the following game [4].

Setup: As described above.

Phase 1: As described above.

Challenge: The adversary submits two identities ID_0, ID_1 and a message m^*. ID_0, ID_1 or their prefix must not have appeared in any key generation query in Phase 1. The challenger selects a random bit $b \in \{0, 1\}$, sets $c^* = Encrypt(params, ID_b, m^*)$, and sends c^* to the adversary as its challenge ciphertext.

Phase 2: This is identical to Phase 1, except that the adversary may not request a private key for ID_0, ID_1 or the decryption of $(ID_0, c^*), (ID_1, c^*)$.

Guess: The adversary submits a guess $b' \in \{0, 1\}$. The adversary wins if $b' = b$.

We call an adversary A in the above game an ANON-ID-CCA adversary. The advantage of an adversary A in this game is defined as $Pr[b' = b] - \frac{1}{2}$.

Definition 2. An HIBE system is $(t, \varepsilon, q_e, q_d)$ ANON-ID-CCA secure if all t-time ANON-ID-CCA adversaries making at most q_e key generation queries and at most q_d decryption queries have advantage at most ε in winning the above game.

3 Hierarchical identity based encryption scheme

3.1 Set up

Let p be a large prime number, G_1, G_2 are groups of order p. $e : G_1 \times G_1 \rightarrow G_2$ is a bilinear map, g is a generator of $G_1, g_1 = g^\alpha$, where $\alpha \in Z_p^*$. l is the maximum number of levels in the HIBE. H is a hash function from $G_1^2 \times G_2^2$ to Z_p^*. The PKG randomly chooses $r_0 \in Z_p^*, h_i \in G_1, i = 0, 1, \ldots, l$. The public parameters are $(g, g_1, r_0, H, h_i(i = 0, 1, \ldots, l))$, α is the private key of PKG.

3.2 Key generation

To a user U with identity $ID = (ID_1, ID_2, \ldots, ID_i) \in Z_p^i$, the PKG randomly chooses $r_i \in Z_p^*$, and computes

$d_{0,i} = (h_0 g^{-r_0})^{\frac{1}{\alpha}} \cdot (\prod_{k=1}^i h_k^{ID_k})^{r_i}, d_{1,i} = g_1^{r_i}$,
$d_{i+1,i} = h_{i+1}^{r_i}, \ldots, d_{l,i} = h_l^{r_i}$,

so the private key of U is $d = (d_{0,i}, d_{1,i}, d_{i+1,i}, \ldots, d_{l,i})$.

The private key can also be generated by its parent $(ID_1, ID_2, \ldots, ID_{i-1})$ having the secret key $(d_{0,i-1}, d_{1,i-1}, d_{i,i-1}, \ldots, d_{l,i-1})$. It computes:

$d_{0,i} = d_{0,i-1} \cdot d_i^{ID_i} \cdot (\prod_{k=1}^i h_k^{ID_k})^t$,
$d_{1,i} = d_{1,i-1} \cdot g_1^t, d_{k,i} = d_{k,i-1} \cdot h_k^t (k = i + 1, \ldots, l)$,
where $r_i = r_{i-1} + t$.

3.3 Encryption

To encrypt a message $m \in G_2$ for the user with identity $ID = (ID_1, \ldots, ID_i)$, randomly choose $s \in Z_p^*$ and compute

$c_1 = (\prod_{k=1}^i h_k^{ID_k})^s, c_2 = e(g, g)^s, c_3 = g_1^s$,
$c_4 = m \cdot e(g, h_0)^s, c_5 = h_1^s \cdot h_2^{s\beta}$,
where $\beta = H(c_1, c_2, c_3, c_4)$.

The ciphertext is $c = (c_1, c_2, c_3, c_4, c_5)$.

Notice that encryption does not require any pairing computations once $e(g, g), e(g, h_0)$ have been pre-computed.

3.4 Decryption

The receiver computes $\beta = H(c_1, c_2, c_3, c_4)$, and verifies whether $e(g_1, c_5) = e(c_3, h_1 h_2^\beta)$. Then he decrypts $c_4 \cdot \frac{e(d_{1,i}, c_1) c_2^{-r_0}}{e(c_3, d_{0,i})} = m$.

4 Analysis of security

4.1 Correctness

$(1) e(g_1, c_5) = e(g_1, h_1^s h_2^{s\beta}) = e(c_3, h_1 h_2^\beta)$

$(2) c_4 \cdot \frac{e(d_{1,i}, c_1) c_2^{-r_0}}{e(c_3, d_{0,i})}$
$= m \cdot e(g, h_0)^s \cdot \frac{e(g_1^{r_i}, \prod_{k=1}^i h_k^{ID_k})^s e(g,g)^{-sr_0}}{e(g_1^s, (h_0 g^{-r_0})^{\frac{1}{\alpha}} \cdot (\prod_{k=1}^i h_k^{ID_k})^{r_i})}$
$= m \cdot e(g, h_0)^s \cdot \frac{1}{e(g^s, h_0)}$
$= m$

4.2 Indistinguishability of ciphertext

Theorem 1 Assume that the q-ABDHE problem is (t', ε')-difficult in group G_1, then the encryption scheme is $(t, \varepsilon, q_e, q_d)$-IND-ID-CCA2, where $t = t' - (q_e + q_d) t_{ave}, \varepsilon = \varepsilon' + \frac{1}{2}$, t_{ave} is the average time of querying oracles.

Proof. Assume A is an IND-ID-CCA adversary, B is a challenger. At the beginning of the game, B is given a tuple $(g, g^\alpha, \ldots, g^{\alpha^q}, g', g'^{\alpha^{q+2}}, T)$ to decide whether $T = e(g, g')^{\alpha^{q+1}}$.

Set Up. B randomly chooses $f(x) \in Z_p[x]$ of degree q with $f(0) \neq 0$, and computes $g(x) = \frac{f(x) - f(0)}{x}$. Let $g_1 = g^\alpha, h_0 = g^{f(\alpha)}, r_0 = f(0), h_i = g_1^{a_i} (i = 1, 2, \ldots, l)$, $a_i \in Z_p^*$ is a random number. H is a hash function from $G_1^2 \times G_2^2$ to Z_p^*. The public parameters are $(g, g_1, r_0, H, h_0, h_1, \ldots, h_l)$.

Phase 1.

Key generation query. A sends identity $ID = (ID_1, ID_2, \ldots, ID_i)$ to B.

B randomly chooses $r_i \in Z_p^*$, and computes

$d_{0,i} = g^{g(\alpha)} \cdot (\prod_{k=1}^i h_k^{ID_k})^{r_i}, d_{1,i} = g_1^{r_i}$,
$d_{i+1} = h_{i+1}^{r_i}, \ldots, d_l = h_l^{r_i}$.

It is a valid private key, where

$d_{0,i} = g^{g(\alpha)} \cdot (\prod_{k=1}^i h_k^{ID_k})^{r_i}$
$= g^{\frac{f(\alpha) - f(0)}{\alpha}} \cdot (\prod_{k=1}^i h_k^{ID_k})^{r_i}$
$= (h_0 g^{-r_0})^{\frac{1}{\alpha}} \cdot (\prod_{k=1}^i h_k^{ID_k})^{r_i}$.

Decryption query. A sends (ID, c) to B.

B first executes the key generation query to identity ID, then decrypts c with the private key of identity ID.

Challenge. A chooses (ID^*, m_0, m_1) to B, where $ID^* = (ID_1^*, ID_2^*, \ldots, ID_i^*)$ and ID^* or its prefix must not have appeared in any key generation query in Phase 1.

B chooses $m_b, b \in \{0, 1\}$, let $s = \log_g g' \cdot \alpha^{q+1}$, and computes

$c_1^* = \prod_{k=1}^i (g'^{\alpha^{q+2}})^{a_k ID_k}, c_2^* = T$,
$c_3^* = g'^{\alpha^{q+2}}, c_4^* = m_b \cdot \frac{e(c_3^*, d_{0,i^*})}{e(d_{1,i^*}, c_1^*) c_2^{*-r_0}}$,

$c_5^* = g'^{\alpha^{q+2}(a_1+a_2\beta^*)}$, where

$\beta^* = H(c_1^*, c_2^*, c_3^*, c_4^*), d_{0,i^*}, d_{1,i^*}$ is the private key of ID^*.

If $T = e(g, g')^{\alpha^{q+1}}$, $c^* = (c_1^*, c_2^*, c_3^*, c_4^*, c_5^*)$ is a valid ciphertext. Otherwise, it is an invalid ciphertext.

Phase 2. A executes key generation oracle to ID and decryption oracle as phase 1, except that the adversary may not request a private key for ID^* and its prefix or the decryption of (ID^*, c^*).

Guess. A submits a guess $b' \in \{0, 1\}$.

Executing the game many times, where q_e, q_d are the number of queries to key generation oracle and decryption oracle respectively. If $Pr(b' = b) = \varepsilon > \frac{1}{2}$, then B has advantage at least ε' in solving the q-ABDHE problem, where $\varepsilon' = \varepsilon - \frac{1}{2}$.

Remark If $T = e(g, g')^{\alpha^{q+1}}$,

$c_1^* = \prod_{k=1}^{i}(g'^{\alpha^{q+2}})^{a_k ID_k} = (\prod_{k=1}^{i} h_k^{ID_k})^s$,

$c_2^* = T = e(g, g')^{\alpha^{q+1}} = e(g, g)^s$,

$c_3^* = g'^{\alpha^{q+2}} = g_1^s$,

$c_4^* = m_b \cdot \frac{e(c_3^*, d_{0,i^*})}{e(d_{1,i^*}, c_1^*)c_2^{*-r_0}} = m_b \cdot e(g, h_0)^s$,

$c_5^* = g'^{\alpha^{q+2}(a_1+a_2\beta^*)} = g_1^{s(a_1+a_2\beta^*)} = h_1^s h_2^{s\beta^*}$,

c^* is a valid ciphertext. Otherwise, it is an invalid ciphertext.

4.3 Anonymity of ciphertext

Theorem 2 Assume q-ABDHE problem is (t', ε')-difficult in group G_1, then the encryption scheme is $(t, \varepsilon, q_e, q_d)$-ANON-ID-CCA2, where $t = t' - (q_e + q_d)t_{ave}, \varepsilon = \varepsilon' + \frac{1}{2}$, t_{ave} is the average time of querying oracles.

Proof. Assume A is an ANON-ID-CCA adversary, B is a simulator. At the beginning of the game, given B a tuple $(g, g^{\alpha}, \ldots, g^{\alpha^q}, g', g'^{\alpha^{q+2}}, T)$ to decide whether $T = e(g, g')^{\alpha^{q+1}}$.

Set Up. As presented in theorem 1.

Phase 1. As presented in theorem 1.

Challenge. A sends (ID_0, ID_1, m^*) to B, where ID_0, ID_1 or their prefix must not have appeared in any key generation query in Phase 1.

B chooses $ID_b, b \in \{0, 1\}$, let $s = \log_g g' \cdot \alpha^{q+1}$,

$c_1^* = \prod_{k=1}^{i}(g'^{\alpha^{q+2}})^{a_k ID_{b,k}}, c_2^* = T, c_3^* = g'^{\alpha^{q+2}}$,

$c_4^* = \frac{m^* \cdot e(c_3^*, d_{0,|ID_b|})}{e(d_{1,|ID_b|}, c_1^*)c_2^{*-r_0}}, c_5^* = g'^{\alpha^{q+2}(a_1+a_2\beta^*)}$,

where $\beta^* = H(c_1^*, c_2^*, c_3^*, c_4^*), d_{0,|ID_b|}, d_{1,|ID_b|}$ is the private key of ID_b.

If $T = e(g, g')^{\alpha^{q+1}}$, $c^* = (c_1^*, c_2^*, c_3^*, c_4^*, c_5^*)$ is a valid ciphertext. Otherwise, it is an invalid ciphertext.

Phase 2. A executes key generation oracle to ID and decryption oracle as phase 1, except that the adversary may not request the private key of ID_0, ID_1 and the decryption of $(c^*, ID_0), (c^*, ID_1)$.

Guess. A submits a guess $b' \in \{0, 1\}$.

Executing the game many times, where q_e, q_d are the number of queries to key generation oracle and decryption oracle respectively. If $Pr(b' = b) = \varepsilon > \frac{1}{2}$, then B has advantage at least ε' in solving the q-ABDHE problem, where $\varepsilon' = \varepsilon - \frac{1}{2}$.

4.4 Efficiency

In the following table, we compare the efficiency of the known HIBE schemes in the standard model.

Scheme	Security model	Public key size	Private key size	Cipher-text size	Pairing operation
BB[5]	sID	l+3	i+1	i+2	i+1
BBG[7]	sID	l+3	l-i+2	3	2
CS[11]	full	h+l+3	i+1	i+1	i+1
ALYW[10]	wrong	2l+1	l-i+2	4	2
BW[12]	full	$2l^2 + 6l + 5$	$3l^2 + 14l - li$ $-3i + 15$	2l+6	2l+5
Our	full	l+5	l-i+2	5	4

Table 1: Comparison to other HIBE schemes.

In this table, i represents the number of levels of identity on which the operations are performed, l is the maximum number of levels in the HIBE. $\sigma = max(2q, 2^{i/h})$, where $1 \leq h \leq i, q$ is the number of queries to oracles. "sID, full" denote selective-ID and adaptive-ID model respectively and "wrong" denotes the security proof is wrong.

We conclude that our HIBE scheme has short parameters, small computation and a tight reduction simultaneously from the table.

5 Conclusion

In this paper, we propose a constant size anonymous HIBE scheme that is fully secure in the standard model. The ciphertext size is independent of the level of the hierarchy. Moreover, our scheme has short parameters, high efficiency and a tight reduction. Our scheme is based on the q-ABDHE problem, an interesting problem is to construct an anonymous HIBE scheme that is fully secure based on a more standard assumption.

Acknowledgement

The work described in this paper was supported by the National Science Foundation of China under Grant (No.6057303), and also funded by the Program for New

Century Excellent Talents in University by Ministry of Education (NCET-05-0398). We also thank anonymous referees of this paper for their constructive comments.

References

[1] A. Shamir.(1984) Identity-Based Cryptosystems and Signature Schemes. In Advances in Cryptology-CRYPTO 1984, volume 196 of LNCS, Springer-Verlag, California, USA, pp. 47-53.

[2] B. Waters.(2005) Efficient Identity-Based Encryption without Random Oracles. In Advances in Cryptology-Eurocrypt 2005, volume 3494 of LNCS, Springer-Verlag, Aarhus, Denmark, pp. 114-127.

[3] C. Gentry and A. Silverberg.(2002) Hierarchical ID-Based Cryptography. In Advances in Cryptology-ASIACRYPT 2002, volume 2501 of LNCS, Springer-Verlag, Queenstown, New Zealand, pp. 548-566.

[4] C. Gentry.(2006) Practical identity-based encryption without random oracles. In Advances in Cryptology-EUROCRYPT 2006, volume 4404 of LNCS, Springer-Verlag, Saint Petersburg, Russia, pp. 445-464.

[5] D. Boneh and X. Boyen.(2004) Efficient Selective-ID Identity Based Encryption without Random Oracles. In Advances in Cryptology- Eurocrypt 2004, volume 3027 of LNCS, Springer-Verlag, Interlaken, Switzerland, pp. 223-238.

[6] D. Boneh, C. Gentry, and B. Waters.(2005) Collusion-Resistant Broadcast Encryption with Short Ciphertexts and Private Keys. In Advances in Cryptology-Crypto 2005, volume 3621 of LNCS, Springer-Verlag, California, USA, pp. 258-275, .

[7] D. Boneh, X. Boyen, E. J. Goh.(2005) Hierarchical Identity Based Encryption with Constant Size Ciphertext. In Advances in Cryptology-EUROCRYPT 2005, volume 3493 of LNCS, Springer-Verlag, Aarhus, Denmark, pp. 440-456.

[8] D.Boneh and M.Franklin.(2001) Identity-Based Encryption from the Weil Pairing. In Advances in Cryptology-CRYPTO 2001, volume 2139 of LNCS, Springer-Verlag, California, USA, pp. 213-229, .

[9] J. Horwitz and B. Lynn.(2002) Toward Hierarchical Identity-Based Encryption. In Advances in Cryptology-EUROCRYPT 2002, volume 2332 of LNCS, Springer-Verlag, Amsterdam, The Netherlands, pp. 466-481.

[10] M. H. Au, J. K. Liu, T. H. Yuen, and D. S. Wong.(2006) Practical Hierarchical Identity Based Encryption and Signature schemes Without Random Oracles. http://eprint.iacr.org/2006/368

[11] S. Chatterjee, P. Sarker.(2006) On Hierarchical Identity Based Encryption Protocols with Short Public Parameters. http://eprint.iacr.org/2006/279

[12] X. Boyen and B. Waters.(2006) Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles). In Advances in Cryptology-CRYPTO 2006, volume 4117 of LNCS, Springer-Verlag, California, USA, pp. 290-307.