New Constructions of Identity-based Broadcast Encryption without Random Oracles

Leyou Zhang[1], Qing Wu[2] and Yupu Hu[3]
[1] Department of mathematical science, Xidian University,
Xi'an, 710071, China
[e-mail: leyouzhang77@yahoo.com.cn]
[2] School of Automation, Xi'an Institute of Posts and Telecommunications,
Xi'an, 710121, China
[e-mail: xidianzly@163.com]
[3] Key Laboratory of Computer Networks and Information Security, Ministry of Education,
Xidian University, Xi'an, 710071, China
*Corresponding author: Leyou Zhang

Received August 20, 2010; revised October 18, 2010; revised November 23, 2010;
accepted January 18, 2011; published February 28, 2011

Abstract

The main challenge in building efficient broadcast systems is to encrypt messages with short ciphertexts. In this paper, we present a new construction based on the identity. Our construction contains the desirable features, such as constant size ciphertexts and private keys, short public keys and not fixing the total number of possible users in the setup. In addition, the proposed scheme achieves the full security which is stronger than the selective-identity security. Furthermore we show that the proof of security does not rely on the random oracles. To the best our knowledge, it is the first efficient scheme that is full security and achieves constant size ciphertexts and private keys which solve the trade-off between the ciphertext size and the private key size.

Keywords: Identity-based encryption, broadcast encryption, full security, the standard model, provable security

This paper was partially supported by the Nature Science Foundation of China under grant (60970119, 60803149), the National Basic Research Program of China(973) under grant 2007CB311201 and the Fundamental Research Funds for the Central Universities.

DOI: 10.3837/tiis.2011.02.011

1. Introduction

Broadcast Encryption (BE) [1] allows a broadcaster to encrypt a message for some subset *S* of users who are listening on a broadcast channel. Any user in *S* can use his private key to decrypt the broadcast. Any user outside the privileged set *S* should not be able to recover the message. Recently it has been widely used in digital rights management applications such as pay-TV, multicast communication, and DVD content protection. Since the first scheme appeared in 1994, many BE schemes have been proposed [2][3][4][5].

Identity-based encryption (IBE) was introduced by Shamir [6]. It 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 avoids the need to distribute public key certificates. So it can simplify many applications of public key encryption (PKE) and is currently an active research area. The first efficient IBE was proposed by Boneh and Franklin [7] in 2001. They proposed a solution using efficiently computable bilinear maps that was shown to be secure in the random oracle model. There have been many schemes shown to be secure without random oracles at present[8-13].

This paper is devoted to constructing the identity-based broadcast encryption(IBBE). IBBE is a generalization of IBE. One public key can be used to encrypt a message to any possible identity in IBE scheme. But in an IBBE scheme, one public key can be used to encrypt a message to any possible group of *S* identities. Recently, many IBBE schemes have been proposed [13][14][15][16][17]. But the well known construction of IBBE was attained by Delerablée [14]. This construction achieves constant size private keys and ciphertexts which solve the trade-off problem between the ciphertext size and the private key size. However her main scheme achieves only selective-identity security and relies on the random oracles. So an open problem is left in her paper to find direct construction which achieves a stronger security. In [16][17], two schemes with full security are proposed. But they are impractical comparing with [14] since they cannot solve the trade-off between the ciphertext size and the private key size. In [16], the private key size grows linear with the number of privileged receivers. Recent work in [17] has the sublinear-size ciphertexts. Hence the work in [17] also does not solve the trade-off problem between the ciphertext size and the private key size. Moreover, the authors in [17] use a sub-algorithm at the *Encrypt* phase to achieve full security. In [18], authers also proposed a scheme which had constant size of private keys and ciphertexts. However this scheme only achives selective-identity security which is a weak security model for identity-based cryptosystems. In addtion, Zhao *ea al*[19] proved that this scheme was not secure.

We focus on IBBE scheme with constant size ciphertexts. In BGW1 [4], the public key is linear in the total number of decryption keys that can be distributed. Moreover, this number is fixed in the setup. Thus one of our motivations is to introduce a system in which the number of possible decryption keys is not fixed in the setup, and thus does not have any impact on the size of the public key. In [16] and [17], the trade-off between the ciphertext size and the private key size implies that if we want to have short ciphertexts, the private keys cannot be constant size. Thus we would like to have both ciphertexts and private keys of constant size. Note that in some systems like the HIBE scheme in [10], the size of the public key can be reduced by using a hash function, viewed as a random oracle in the security proof, but this is not the case in BGW1, because all the elements of the public depend on a single value.

Our Contributions. These motivate us to construct a new scheme which can achieve a strong security-full security with constant size cipertexts and private keys. In this paper, we present a new construction. Our construction achieves $O(1)$-size private keys and $O(1)$-size ciphertexts. It has full security which is stronger than selective-identity security. In addition, we show that its security does not rely on the random oracles.

In Section 2, we give the preliminaries for our scheme. Section 3 addresses our new scheme and efficiency comparison. Section 4 presents security analysis of our scheme. A conclusion of this paper is given in Section 5.

2. Preliminaries

2.1 Bilinear Groups

We briefly review bilinear maps and use the following notations:

1. G and G_1 are two (multiplicative) cyclic groups of prime order p;
2. g is a generator of G .
3. e is a bilinear map $e: G \times G \to G_1$.

Let G and G_1 be two groups as above. A bilinear map is a map $e: G \times G \to G_1$ with the properties:

1. Bilinearity: for all $u, v \in G$, $a, b \in Z_p$, we have $e(u^a, v^b) = e(u, v)^{ab}$.
2. Non-degeneracy: $e(g, g) \neq 1$.
3. Computability: There is an efficient algorithm to compute $e(u, v)$ for all $u, v \in G$

2.2 The General Diffie-Hellman Assumption

As in [10], we also make use of the generalization of the Diffie-Hellman exponent assumption, which is given by Boneh, Boyen and Goh [10]. They introduced a class of assumptions which includes a lot of assumptions that appeared with new pairing-based schemes. It includes for example DDH, BDH, q−BDHI, and q−BDHE assumptions. We give an overview of it as follows [10][11][12][13][14].

Let p be an integer prime and let s, n be positive integers. Let $P, Q \in F_p[x_1, \cdots, x_n]^s$ be two s-tuple of n-variate polynomials over F_p and let $f \in F_p[x_1, \cdots, x_n]$. Thus, P and Q are just two ordered sets containing s multi-variate polynomials each. We write $P = (p_1, p_2, \cdots, p_s)$ and $Q = (q_1, q_2, \cdots, q_s)$. We require that the first components of P, Q satisfy $p_1 = q_1 = 1$; that is, the constant polynomials 1. For a set Ω, a function $h: F_p \to \Omega$, and a vector $(x_1, \cdots, x_n) \in F_p$, we write

$$h(P(x_1,\cdots,x_n))=(h(p_1(x_1,\cdots,x_n)),\cdots,h(p_s(x_1,\cdots,x_n)))\in\Omega^s.$$

We use similar notation for the s-tuple Q. Let G, G_1 be groups of order p and let e:$G\times G\rightarrow G_1$ be a non-degenerate bilinear map. Let $g_0\in G$ be a generator of G and set $g=e(g_0, g_0)\in G_1$.

The (P,Q, f)-General Diffie-Hellman Exponent problems are defined as follows.

Definition 1 ((*P*,*Q*, *f*)-GDHE). Given the tuple

$$H(x_1, . . . , x_n) = (g_0^{P(x_1,\cdots,x_n)}, g^{Q(x_1,\cdots,x_n)}),$$

compute $g^{f(x_1,\cdots,x_n)}$.

Definition 2 ((*P*,*Q*, *f*)-GDDHE). Given the tuple $H(x_1, . . . , x_n) = (g_0^{P(x_1,\cdots,x_n)}, g^{Q(x_1,\cdots,x_n)})$ and T, decide whether $T=g^{f(x_1,\cdots,x_n)}$.

In this paper, we will use the the following intermediate decisional problem.

Definition 3. ((f,g,F)-GDDHE). Let (p,G_1,G_2,G_T, e) be a bilinear map group system and let f and g be two coprime polynomials with pairwise distinct roots, of respective orders t and n. Let g_0 be a generator of G_1 and h_0 a generator of G_2. Solving the (f, g,F) -GDDHE problem consists, given

$$(g_0, g_0^{\alpha}, g_0^{\alpha^2},\cdots, g_0^{\alpha^{t-1}}, g_0^{\alpha f(\alpha)}, g_0^{\frac{1}{k}}, g_0^{\frac{\alpha}{k}}, g_0^{k\alpha f(\alpha)}, h_0, h_0^{\alpha}, h_0^{\alpha^2}, \cdots, h_0^{\alpha^{2n}},\cdots, h_0^{kg(\alpha)},)$$

and $T\in G_{\mathrm{T}}$, in deciding whether T is equal to $e(g_0, h_0)^{kf(\alpha)}$ or to some random element of G_T.

The intractability of distinguishing the two distributions involved in the (f, g,F)-GDDHE problem is given as follows.

Theorem 1 ([10][11][12][13][14]). Let $P,Q\in F_p[x_1,\cdots,x_m]$ be two s-tuple of m-variate polynomials over F_p and let $F\in F_p[x_1,\cdots,x_m]$. Let d_P (*resp*. d_Q, d_F) denote the maximal degree of elements of P (*resp*. of Q, F) and pose $d = \max(2d_P , d_Q, d_F)$.If $F \not\in$<P,Q>, then for any generic-model adversary A totalizing at most q queries to the oracles (group operations in G,G_T and evaluations of e) which is given $H(x_1, . . . , x_m)$ as input and tries to distinguish $g^{F(x_1,\cdots,x_m)}$ from a random value in G_T, one has

$$Adv(A)=\frac{(q+2s+2)d}{2p}.$$

Proof: It is similar to [10(full version: Cryptology ePrint Archive Report 2005/015),14]. Note in this paper, $m=4, s=t+2n+6$.

Definition 4. ((f,g,F)-GDDHE Assumption). The (P, ε)-(f,g,F)-GDDHE assumption holds if no adversary has at least ε advantage in solving the above problem with polynomial time P.

For a detail description of this assumption, the readers are referred to [5][10][14].

Definition 5. (Weak Decisional Bilinear Diffie-Hellman Inversion (wDBDHI) Problem) [12]: An instance of the h-wDBDHI problem over (G_1, G_2, e) consists of a tuple (g, h, g^{α}, g^{α^2},$\cdots$, g^{α^h} , T) for some $\alpha\in Z_p$ and the task is to decide whether $T=e(g,h)^{\alpha^{h+1}}$ or T is a random element of G_T.

2.3 Identity-Based Broadcast Encryption

Identity-based broadcast encryption(IBBE) [13][14] is a generalization of IBE. One public key can be used to encrypt a message to any possible identity in IBE schemes. But in an IBBE scheme, one public key can be used to encrypt a message to any possible group of S identities. An identity-based broadcast encryption scheme(IBBE) with the security parameter and the maximal size m of the target set, consists of four algorithms *Setup, Extract, Encrypt, Decrypt* and is specified as follows.

Setup Take as input the security parameter and the maximal size m of the set of receivers for one encryption, *Setup* outputs a master secret key and a public key. The Private Key Generator(*PKG*) is given the master secret key, and the public key is made publicized.

Extract Take as input the master secret key and a user identity *ID*, *Extract* generates a user private key d_{ID}.

Encrypt Take as input the public key and a set of included identities $S=\{ID_1,\ldots, ID_s\}$ with $s \le m$, *Encrypt* outputs a pair (*Hdr*, *K*), where *Hdr* is called the header and *K* is a key for the symmetric encryption scheme.

When a message M is to be broadcast to users in S, the broadcaster generates (*Hdr*,*K*), computes the encryption C_M of M under the symmetric key K and broadcasts (*Hdr*, *S*, C_M).

Decrypt Take as input a subset $S=\{ID_1, \ldots, ID_s\}$ with $s \le m$, an identity ID_i and the corresponding private key, a header *Hdr* and the public key, if $ID \in S$, the algorithm outputs the message encryption key K which is then used to decrypt the broadcast body C_M and recover M.

2.4 Security Model for IBBE

Concerning the security in IBE systems, there are mainly two definitions:

1. Full security, which means that the attacker can choose adaptively the identity he wants to attack (after having seen the parameters);

2. Selective-Identity(ID) security, which means that the attacker must choose the identity he wants to attack at the beginning, before seeing the parameters. The Selective-ID security is thus weaker than full security.

A strong security notion is the full security in IBE scheme. Following [5][14][16][17], we define the security model for IBBE which is equivalent to the full security in IBE schemes. It is specified as follows: Both the adversary and the challenger are given as input m, the maximal size of a set of receivers $\tilde{S}$.

Setup: The challenger runs *Setup* to obtain a public key *PK*. He gives *A* the public key *PK*.

Query phase 1*:* The adversary *A* adaptively issues queries $q_1, \ldots, q_{s0}$, where q_i is one of the following:

• Extraction query (ID_i) : The challenger runs *Extract* on ID_i and sends the resulting private key to the adversary.

• Decryption query for a triple (ID_i, *S*, *Hdr*) with $S \subseteq \tilde{S}$ and $ID_i \in S$. The challenger responds with *Decrypt*(*S*, ID_i, *Hdr*, *PK*).

Challenge*:* When *A* decides that phase 1 is over, the challenger runs *Encrypt* algrithm to obtain $(Hdr^*, K) = Encrypt(S^*, PK)$. The challenger then randomly selects $b \in \{0, 1\}$, sets $K_b =$

K, and sets K_{1-b} to a random value . The challenger returns (Hdr^*, K_0, K_1) to *A*.

Query phase 2*:* The adversary continues to issue queries $q_{s0+1}, \ldots, q_t$, where q_i is one of the following:

- Extraction query (ID_i), as in phase 1 with the constraint that $ID_i \notin S^*$.
- Decryption query, as in phase 1, but with the constraint that $Hdr \neq Hdr^*$. The challenger responds as in phase 1.

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

Let q_D denote the total number of Decryption queries and *t* denote the total number of extraction queries during the game. The advantage of *A* in winning the game is defined as follows [14]:

$$Adv_{IBBE}(t, q_D, m, A) = |\, 2P(b = b') - 1 \,| .$$

We call an adversary *A* in the above game a *IND-ID-CCA*(chosen ciphertext security for IBBE systems under chosen identity attacks) adversary.

Definition 6. An identity-based broadcast encryption scheme(IBBE) is said to be (t, m, q_D)-*IND-ID-CCA* secure if $Adv_{IBBE}(t, q_D, m, \mathrm{A})$ is neglectable.

Let (t, m) denote the adversary's attacking parameters, we can obtain the definition of *(t,m)-Collusion Resistance* [5]. Our construction only achieves (t, m)-Collusion Resistance.

We say that if the above indistinguishability game allow no decryption oracle query, then the IBBE scheme is only chosen plaintext (*IND-ID-CPA*) secure. There have been many methods to convert an *IND-ID-CPA* scheme to an *IND-sID-CCA* scheme(*e.g.* [20]). Therefore, we only focus on constructing the *IND-ID-CPA* scheme in this paper.

3. New Identity-Based Broadcast Encryption

3.1 New Construction

Setup To generate the system parameters, the PKG picks randomly generators g, $h_1 \in G_1$, $h \in G_2$ and a random $\alpha \in Z_p$. It sets $g_1 = g^{\alpha}$, $h_2 = h_1^{\alpha} \in G_1$. The public keys are $PK = (g_1, h_1, h_2, h, h^{\alpha}, h^{\alpha^2}, \cdots, h^{\alpha^m}, v)$ where $v = e(g, h)$ and master key is (α, g).

Extract To generate a private key for identity $ID_i \in S$, the PKG selects random $r \in Z_p$, and outputs the private key

$$d_{ID_i} = (d_{i1}, d_{i2}) = ((gh_1^{-r_i})^{\frac{1}{\alpha - ID_i}}, r_i),$$

If $ID = \alpha$, the PKG aborts.

Encrypt Without loss of generality, let $S = (ID_1, ID_2, \cdots, ID_s)$ denote the set of users with $s \le m$. A broadcaster selects a random $k \in Z_p^*$, computes $Hdr = (C_1, C_2, C_3, C_4)$ and K as follows:

$$C_1 = g_1^{-k},\ C_2 = h_2^k,\ C_3 = h_1^k,\ C_4 = h^{k\sum_{i=1}^{s}(\alpha - ID_i)},\ K = v^k,$$

Note that C_4 can be computed from ($h^{\alpha}, h^{\alpha^2}, \cdots, h^{\alpha^m}$).

Decrypt In order to retrieve the message encryption key K encapsulated in the header *Hdr* = (C_1, C_2, C_3, C_4), user with the identity $ID_i \in S$ and the corresponding private key d_{ID_i} =(d_{i1}, d_{i2})=($(gh_1^{-r_i})^{\frac{1}{\alpha - ID_i}}$, r_i), computes

$$K = (e(C_1 C_2^{d_{i2}}, h^{\frac{1}{\alpha} p(\alpha)}) e(d_{i1}, C_4))^{\frac{1}{p_i}} e(C_3, h)^{d_{i2}} .$$

Where $p(\alpha) = \prod_{j=1, j \neq i}^{s} (\alpha - ID_j) + (-1)^{s-1} \prod_{j=1, j \neq i}^{s} ID_j$ and $p_i = (-1)^s \prod_{j=1, j \neq i}^{s} ID_j$.

Correctness: Let *Hdr* be well-known for *S*. One can obtain

$$e(C_1 C_2^{d_{i2}}, h^{\frac{1}{\alpha} p(\alpha)}) e(d_{i1}, C_4) = e(g_1^{-k} h_2^{kd_{i2}}, h^{\frac{1}{\alpha} p(\alpha)}) e(d_{i1}, h^{k \sum_{i=1}^{s} (\alpha - ID_i)})$$

$$= e((gh_1^{-r_i})^{-k\alpha}, h^{\frac{1}{\alpha} p(\alpha)}) e((gh_1^{-r_i})^{\frac{1}{\alpha - ID_j}}, h^{k \sum_{i=1}^{s} (\alpha - ID_i)})$$

$$= e(gh_1^{-r_i}, h)^{-k(\prod_{j=1, j \neq i}^{s} (\alpha - ID_j) + (-1)^{s-1} \prod_{j=1, j \neq i}^{s} ID_j)} e((gh_1^{-r_i})^{\frac{1}{\alpha - ID_j}}, h^{k \sum_{i=1}^{s} (\alpha - ID_i)})$$

$$= e(gh_1^{-r_i}, h)^{-k(\prod_{j=1, j \neq i}^{s} (\alpha - ID_j) + (-1)^{s-1} \prod_{j=1, j \neq i}^{s} ID_j)} e(gh_1^{-r_i}, h)^{k \prod_{j=1, j \neq i}^{s} (\alpha - ID_j)}$$

$$= e(gh_1^{-r_i}, h)^{k(-1)^s \prod_{j=1, j \neq i}^{s} ID_j}$$

and

$$(e(C_1 C_2^{d_{i2}}, h^{\frac{1}{\alpha} p(\alpha)}) e(d_{i1}, C_4))^{\frac{1}{p_i}} e(C_3, h)^{d_{i2}} = e(gh_1^{-r_i}, h)^k \; e(h_1^k, h)^{r_i} = e(g, h)^k = K.$$

3.2 Efficiency

Our construction achieves constant size ciphertext, private keys and *O(m)*-size public keys. In addition, our construction, as the next section will show, can achieve full security in the standard model. **Table 1** and **Table 2** give the comparisons of efficiency with other schemes. The computing efficiency is denoted mainly by the bilinear pair computation. It is specified in **Table 2**. We only give the comparison of the third scheme in [17] since scheme 3 has full security.

Table 1. Comparisons of Efficiency.

schemes	**Public key size**	**Private key size**	**Ciphertext size**	**Security Model**
[16]	$O(\lambda)$	$O(n)$	$O(1)$	Full security
[17] 1st	$O(m)$	$O(n)$	$O(1)$	*semi-static* security
[17] 2nd	$O(m)$	$O(1)$	$O(1)$	*semi-static* security
[17] 3rd	$O(m)$	$O(1)$	Sublinear of n	Full Security
[18]	$O(1)$	$O(1)$	$O(1)$	Selective-ID security
Ours	$O(m)$	$O(1)$	$O(1)$	Full security

Table 2. Comparisons of Computing Efficiency.

schemes	Pair Computing		Hash computing	
	Encrypt	***Decrypt***	***Encrypt***	***Decrypt***
[16]	5	3	Yes	Yes
scheme 3 in [17]	2	2	NO	NO
Ours	0	3	NO	NO

Note: λ is a security parameter. *m* and *n* denote the maximal size of the set of receivers and the size of receivers for one encryption($2n \le m$). *Semi-static security* can be obtained in [17].

From **Table 2**, one can conclude that the scheme in [16] impractical in real-life practice. In addition, in order to achieve the full security, the authors of [17] use a *Tag-encrypt* algorithm at the *Encrypt* phase in the scheme 3. This folklore construction method leads to the scheme that is somewhat inefficient. To the best of our knowledge, our IBBE is the first efficient scheme that is full security with constant size private key and ciphertext.

Table 3. Comparison III of the Approximate Computation Efficiency with the others.

Schemes	[16]		[17]		Our scheme	
	Encrypt	***Decrypt***	***Encrypt***	***Decrypt***	***Encrypt***	***Decrypt***
Computation cost	120.586 *s*	67.506 *s*	41.323*s* +time(symencrypt)	41.323*s* +time(symdecrypt)	20.125*s*	67.125*s*

In **Table 3**, we select *m*=300, *n*=150. It is worth noting that the computation cost of pairing operations, point multiplications operations and modular inverse is about 11110 , a few hundreds and 70 multiplications respectively. (We assume that all schemes are all using the GDH group derived from the curve $E/F_{3^{163}}$ defined by the equation $y^2 = x^3 - x + 1$). Hence our schemes are more efficient in terms of computation cost than others. In **Table 3**, *s* denots cputime (Second). In addition, we only consider the computation cost of the En. and De. phases. All experiments are run on a personal computer with Pentium Dual core E6500 (2.94 GHz) and a maximum of 2.0 GB of the memory available. The program of the algorithms is written in Matlab 7.1 language.

4. Security Analysis

Theorem 2. Our construction is ($P'(\lambda), t, n, \varepsilon'$)-*IND-ID-CPA* secure if the ($P(\lambda)$, ε) (*f*, *g*, *F*)-GDDHE problem holds with $\varepsilon' \le 2\varepsilon$ and $P'(\lambda) = P(\lambda) - O(\tau t^2)$, where *n* denotes the maximal size of a set of included users *S*, *t* denotes the total number of extraction queries that can be issued by the adversary and τ is the time required to compute the exponent in G_1.

Proof: Suppose there exists an adversary *A* breaking our scheme under a (*t*, *m*)-collusion, we will build an algorithm *B* that can solve the (*f*, *g*, *F*)-GDDHE problem. *B* takes as input a tuple $(g_0, g_0^{\alpha}, g_0^{\alpha^2}, \cdots, g_0^{\alpha^{t-1}}$, $g_0^{\alpha f(\alpha)}$, $g_0^{\frac{1}{k}}, g_0^{\frac{\alpha}{k}}$, $g_0^{k\alpha f(\alpha)}$, $h_0, h_0^{\alpha}, h_0^{\alpha^2}$, $\cdots, h_0^{\alpha^{2n}}$, $\cdots$, $h_0^{kg(\alpha)}$, *T*),where *T* is equal to $e(g_0, h_0)^{kf(\alpha)}$ or to some random element of G_T .We define the following game between *A* and *B*.

Setup Algorithm *B* is given as input a group system (p,G_1,G_2, G_T , e) and (*f*, *g*, *F*) -*GDDHE* instance: g_0, $g_0^{\alpha}, g_0^{\alpha^2},\cdots, g_0^{\alpha^{t-1}}$, $g_0^{\alpha f(\alpha)}$, $g_0^{\frac{1}{k}}, g_0^{\frac{\alpha}{k}}$, $g_0^{k\alpha f(\alpha)}$, h_0, $h_0^{\alpha}, h_0^{\alpha^2}$, $\cdots$, $h_0^{\alpha^{2n}},\cdots, h_0^{kg(\alpha)}$,Where *f*(*x*) and *g*(*x*) are two coprime polynomials with pairwise distinct roots and have respective orders *t* and *n*. For simplicity, *f*(*x*) and *g*(*x*) are defined as follows:

$$f(x)=\prod_{i=1}^{t}(x+x_i),\ g(x)=\prod_{i=t+1}^{t+n}(x+x_i).$$

The techniques have been used in [5][14]. Then it sets $g=g_0^{f(\alpha)}$ and

$$h_1=g_0^{\frac{1}{k}},\ h_2=g_0^{\frac{\alpha}{k}}=h_1^{\alpha},\ g_1=g_0^{\alpha f(\alpha)}=g^{\alpha},h=h_0^{g(\alpha)};$$

$$v=e(g_0,h_0)^{f(\alpha)g(\alpha)}=e(g,h).$$

Note that *B* can by no means compute the value *g*. It sends the public key *PK* =(g_1, h_1, h_2, *h*, $h^{\alpha},h^{\alpha^2},\cdots,h^{\alpha^m}$, *v*) to *A*.

Phase 1: *A* makes key generation queries q_1, q_2, ⋯, q_m. *B* responds to a query q_i on $ID_i \in Z_p$ as follows. Note that $ID_i \neq \alpha$, otherwise if $ID_i = \alpha$, *B* can solve *t*-wDBDHI problem. Then *B* sets the private key (d_1,d_2) to be ($g_0^{\frac{f(\alpha)-f(ID_i)}{\alpha-ID_i}}$, $f(ID_i)$). This is a valid private key for ID_i. In fact, let $r = f(ID_i)$, then

$$g_0^{\frac{f(\alpha)-f(ID_i)}{\alpha-ID_i}}=(g_0^{f(\alpha)}g_0^{-f(ID_i)})^{\frac{1}{\alpha-ID_i}}=(gh_1^{-r})^{\frac{1}{\alpha-ID_i}}.$$

Challenge: The adversary submits a set $S^*=(ID_1^*,ID_2^*,\cdots,ID_s^*)$ of identities. The constraint is that the adversary does not make *Extraction query* for ID_i^* in *Phase* 1 and $ID_i^* \neq \alpha$. Then *B* runs *Encrypt* algorithm and computes $Hdr^*=(C_1^*,C_2^*,C_3^*,C_4^*)$ and K^* as follows:

$$C_1^*=g_0^{-k\alpha f(\alpha)},C\ _2^*=g_0^{\alpha},C_3^*=g_0,C_4^*=h_0^{kg(\alpha)\prod_{i=1}^{s}(\alpha-ID_i^*)},K^*=T^{\prod_{i=t+1}^{t+n}x_i}e(g_0^{kaf(\alpha)},h_0^{q(\alpha)}),$$

where $q(\alpha)=\frac{1}{\alpha}(g(\alpha)-\prod_{i=t+1}^{t+n}x_i)$ and C_4^* can be computed from *PK* and (*f*, *g*, *F*)-*GDDHE* instance.

Suppose that *B* is given a valid (*f*, *g*, *F*)-*GDDHE* tuple, i.e., $T = e(g_0, h_0)^{kf(\alpha)}$ then Hdr^* and K^* are valid for S^*. In fact, one can verify

$$C_1^*=g_0^{-k\alpha f(\alpha)}=g_1^{-k},C_2^*=g_0^{\alpha}=g_0^{\frac{\alpha}{k}k}=h_2^k,\ C_3^*=g_0=g_0^{\frac{1}{k}k}=h_1^k,$$

$$C_4^* = h_0^{kg(\alpha)\prod_{i=1}^{s}(\alpha-ID_i^*)} = h^{k\prod_{i=1}^{s}(\alpha-ID_i^*)}, K^* = T^{\prod_{i=t+1}^{t+n} x_i} e(g_0^{kaf(\alpha)}, h_0^{q(\alpha)}) = v^k .$$

Otherwise K is a random element of G_T . B randomly selects $b \in \{0,1\}$, sets $K_b = K^* = v^k$, and sets $K_{1\text{-}b}$ to a random value . Then B returns (Hdr^*, K_0, K_1) to A.

***Phase** 2*: The adversary continues to issue queries $q_{m+1}, \cdots, q_t$, where q_i is an extraction query ID_i with the constraint that $ID_i \notin S^*$.

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

Probability analysis: Following the [14], we can obtain $\varepsilon' \le 2\varepsilon$.

Time complexity: In the previous game, B's overhead is dominated by computing $g_0^{\frac{f(\alpha)-f(ID_i)}{\alpha-ID_i}}$ in response to A's key generation query on ID_i, where $\frac{f(\alpha)-f(ID_i)}{\alpha-ID_i}$ is a polynomial of degree t-1. Each such computation requires $O(t)$ exponentiations in G_1. A makes at most t such queries, hence $P(\lambda) = P'(\lambda) + O(\tau t^2)$.

5. Conclusion

We solve partly the open problem which is not solved in [5][14] and give a new identity-based broadcast encryption scheme in the standard model. It achieves a strong security without relying on the random oracles. But it still leaves an open problem to construct an IBBE system with constant size ciphertexts and private keys that is secure under a more standard assumption.

References

[1] A. Fiat and M. Naor, “Broadcast encryption,” in *Proc. of Crypto*., Lecture Notes in Computer Science, vol. 773, pp. 480-491, Berlin: Springer-Verlag, August 1993. Article (CrossRef Link).

[2] Y. Dodis and N. Fazio, “Public key broadcast encryption for stateless receivers,” in *Proc. of ACM Workshop on Digital Rights Management*, Lecture Notes in Computer Science, vol. 2696, pp. 61-80, Berlin: Springer-Verlag, November 2002. Article (CrossRef Link).

[3] Y. Dodis and N. Fazio, “Public key broadcast encryption secure against adaptive chosen ciphertext attack,” in *Proc. of Public Key Cryptography*, Lecture Notes in Computer Science, vol. 2567, pp. 100-115, Berlin: Springer-Verlag, January 2003. Article (CrossRef Link).

[4] D. Boneh, C. Gentry and B. Waters, “Collusion resistant broadcast encryption with short ciphertexts and private keys,” in *Proc. of CRYPTO*, Lecture Notes in Computer Science, vol. 3621, pp. 258-275, Berlin: Springer-Verlag, August 2005. Article (CrossRef Link).

[5] C. Delerablèe, P.Paillier and D. Pointcheval, “Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys,” in *Proc. of Pairing-Based Cryptography*, Lecture Notes in Computer Science, vol. 4575, pp. 39-59, Berlin: Springer-Verlag,

July 2007. Article (CrossRef Link).

[6] A. Shamir, “Identity-based Cryptosystems and Signature Schemes,” in *Proc. of Crypto*, Lecture Notes in Computer Science, vol. 196, pp. 47-53, Berlin: Springer-Verlag, August 1984. Article (CrossRef Link).

[7] D. Boneh and M. Franklin, “Identity Based Encryption from the Weil Pairing,” in *Proc. of CRYPTO*, Lecture Notes in Computer Science, vol. 2139, pp. 213-229, Berlin: Springer-Verlag, August 2001. Article (CrossRef Link).

[8] D. Boneh and X. Boyen, “Efficient Selective-ID Identity Based Encryption without Random Oracles,” in *Proc. of Eurocrypt*, Lecture Notes in Computer Science, vol. 3027, pp. 223-238, Berlin:Springer-Verlag, 2004. Article (CrossRef Link).

[9] D. Boneh and J. Katz, “Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity-Based Encryption,” in *Proc. of CT-RSA*, Lecture Notes in Computer Science, vol. 3376, pp. 87-103, Berlin: Springer-Verlag, February 2005. Article (CrossRef Link).

[10] D. Boneh, X. Boyen and E. J. Goh, “Hierarchical Identity Based Encryption with Constant Size Ciphertext,” in *Proc. Of Eurocrypt*, Lecture Notes in Computer Science, vol. 3494, pp. 440-456, Berlin: Springer-Verlag, May 2005. Article (CrossRef Link).

[11] D. Boneh and X. Boyen, “Secure Identity Based Encryption without Random Oracles,” in *Proc. of Crypto*, Lecture Notes in Computer Science, vol. 3152, pp. 443-459, Berlin: Springer-Verlag, August 2004. Article (CrossRef Link).

[12] C. Gentry, “Practical identity-based encryption without random oracles,” in *Proc. of EUROCRYPT*, Lecture Notes in Computer Science, vol. 4004, pp. 445-464, Berlin: Springer-Verlag, 2006. Article (CrossRef Link).

[13] Y. Mu *et al.*, “Identity-Based Authenticated Broadcast Encryption and Distributed Authenticated Encryption,” in *Proc. of ASIAN 2004*, Lecture Notes in Computer Science, vol. 3321, pp. 169- 181, Berlin: Springer-Verlag, December 2004. Article (CrossRef Link).

[14] C. Delerablée, “Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys,” in *Proc. of ASIACRYPT*, Lecture Notes in Computer Science, vol. 4833, pp. 200-215, Berlin: Springer-Verlag, December 2007. Article (CrossRef Link).

[15] X. Du *et al.*, “An ID-Based Broadcast Encryption Scheme for Key Distribution,” *IEEE Transactions on Broadcasting*, vol. 51, no. 2, pp. 264-266, 2005. Article (CrossRef Link)

[16] Y. L. Ren and D.W. Gu, “Fully CCA2 secure identity based broadcast encryption without random oracles,” *Information Processing Letters*, vol. 109, no. 11, pp. 527–533, 2009. Article (CrossRef Link)

[17] C. Gentry and B. Waters, “Adaptive Security in Broadcast Encryption Systems,” in *Proc. of EUROCRYPT 2009*, LNCS 5479, pp. 171–188, 2009. Article (CrossRef Link)

[18] L. Hu and Z. Liu, “Efficient Identity-based Broadcast Encryption without Random Oracles,” *Journal of Computers*, vol. 5, no. 3, pp. 331-336, 2010. Article (CrossRef Link)

[19] X · Zhao and F. Zhang, “Analysis on Hu et al's Identity-based Broadcast Encryption,” *International Journal of Network Security*, (Will appear in vol.12, no. 3, pp. 362-364, 2011) http://ijns.femto.com.tw/contents/ijns-v13-n3/ijns-2011-v13-n3-p178-180.pdf.

[20] R. Canetti, S. Halevi and J. Katz, “Chosen-Ciphertext Security from Identity- Based Encryption,”

in *Proc. of Eurocrypt*, Lecture Notes in Computer Science, vol. 3027, pp. 207-222, Berlin: Springer-Verlag, May 2004. Article (CrossRef Link)

Leyou Zhang: male. He received his Ph.D. from the Xidian University in 2009. Now he is an Associate Professor in the department of Mathematical science of Xidian University. His current research interests include network security, computer security, and cryptography. He has published more than thirty papers in international and domestic journals and conferences.

Qing Wu: female. She received her Ph.D. from the Xidian University in 2009. Now she is an Associate Professor in the school of automation of Xi'an institute of posts and telecommunication. Her current research interests include information security and applied mathematics. She has published more than twenty papers in international and domestic journals and conferences.

Yupu Hu: male. He received his Ph.D. from the Xidian University in 1999. Now he is a Professor in the School of Telecommunications Engineering of Xidian University. His current research interests include information security and cryptography. He has published more than a hundred papers in international and domestic journals and conferences. He is a Member of China Institute of Communications and a Director of Chinese Association for Cryptologic Research.