Direct CCA Secure Identity-Based Broadcast Encryption

Leyou Zhang[1], Qing Wu[2], and Yupu Hu[3]

[1] Department of Mathematics, School of Science, Xidian University, Xi'an, 710071, China
[2] School of Automation, Xi'an University of Posts and Telecommunications, Xi'an, 710121, China
[3] Key Laboratory of Computer Networks and Information Security, Xidian University, Xi'an, 710071, China
leyouzhang77@yahoo.com.cn

Abstract. In the previous works, the general transformation methods from a CPA(chosen-plaintext attacks) secure scheme to a CCA(chosen-ciphertext attacks) secure scheme are the hierarchical identity-based encryption, one-time signature and MAC. These folklore construction methods lead to the CCA secure schemes that are somewhat inefficient in the real life. In this paper, a new direct chosen-ciphertext technique is introduced and a practical identity-based broadcast encryption(IBBE) scheme that is CCA secure is proposed. The new scheme has many advantages over the available, such as constant size private keys and constant size ciphertexts, which solve the trade-off between the private keys size and ciphertexts size. In addition, under the standard model, the security of the new scheme is reduced to the hardness assumption-decision bilinear Diffie-Hellman exponent problem(DBDHE). This assumption is more natural than many of the hardness assumptions recently introduced to IBBE in the standard model.

Keywords: IBBE, direct CCA technique, provable security, standard model.

1 Introduction

Identity-based encryption (IBE) was introduced by Shamir[1]. 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 concept of Broadcast Encryption (BE) was introduced by Fiat and Naor. In a broadcast encryption scheme a broadcaster encrypts 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.

L. Xu, E. Bertino, and Y. Mu (Eds.): NSS 2012, LNCS 7645, pp. 348–360, 2012.

Since the first scheme appeared in 1994, many BE schemes have been proposed [2-6]. In this paper, we mainly consider the construction of the identity-based broadcast encryption(IBBE). IBBE [7-11] 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. In [7, 11], the proposed scheme was based on random oracles. In addition, the size of the ciphertexts grows linearly with the number of the users. The well known construction of IBBE was proposed by Delerablée [8]. This construction achieved constant size private keys and constant size ciphertexts. However the security of her main scheme achieved only selective-identity security(a weak security) and relied on the random oracles. In [10], a new scheme with full security was proposed. But it was impractical in real-life practice since their security relied on the complex assumptions. In addition, the work in [10] had the sublinear-size ciphertexts. Moreover, the authors in [10] used a sub-algorithm at the Encrypt phase to achieve full security which increased the computations cost. In [11,12], the authors also proposed two schemes with full security. But these schemes have a same feature that achieves only CPA security. CPA-security does not guarantee any security against chosen-ciphertext attacks(CCA), where the adversary may request decryptions even after seeing the challenge ciphertext, under the natural limitation that the adversary may not request decryption of the challenge ciphertext itself. See [15-17, 19,21] for further discussion of these definitions.

In [13], the authors declared their scheme achieved fully CCA security. Unfortunately in [14], the authors proved their scheme was even not chosen plaintext secure(CPA). Hence how to construct a CCA secure IBBE is still an interesting problem. The authors in the previous scheme claimed their scheme could be transformed to the CCA scheme. However, the transformation methods in their paper were the general methods, such as hierarchical identity-based encryption, one-time signature and MAC. These folklore construction methods lead to schemes that are somewhat inefficient in the real life. The direct chosen-ciphertext technique is needed. It has been used in [15,16,17]. In this paper, we extend this technique to IBBE. The resulting scheme is more efficient than the available.Our scheme achieves constant size ciphertexts and private keys as well as scheme in [8]. However, our proposed scheme has fully CCA security. In addition, the security of our scheme is reduced to the DBDHE assumption instead of other strong assumptions. To the best of our knowledge, it is the first efficient scheme that is direct CCA secure in the standard model.

2 Preliminaries

2.1 Bilinear Maps

Let G and G_1 be two (multiplicative) cyclic groups of prime order p and g be a generator of G. A bilinear map e is a map $e : G \times G \longrightarrow G_1$ with the following properties:

(i) bilinearity: for all $u, v \in G, a, b \in Z_p$, we have $e(u^a, v^b) = e(u, v)^{ab}$;
(ii) non-degeneracy: $e(g, g) \neq 1$;
(iii) computability: there is an efficient algorithm to compute $e(u, v)$ for all $u, v \in G$.

2.2 Decision Bilinear Diffie-Helllman Expoent Problem (DBDHE)

The decisional bilinear Diffie-Hellman Exponent problem has been used widely to construct encryption schemes. It is given as follows. Algorithm B is given as input a random tuple $(g, y_0, y_1, \cdots, y_n, y_{n+2}, \cdots, y_{2n+2}, T)$ where $y_i = g^{\alpha^i}, y_0 = g^c$ and $\alpha, c \in Z_p^*$. Algorithm B's goal is to output 1 when $T = e(g, y_0)^{\alpha^{n+1}} = e(g, g)^{\alpha^{n+1}c}$ and 0 otherwise. Let $TU = (g, y_0, y_1, \cdots, y_n, y_{n+2}, \cdots, y_{2n+2})$. Algorithm B that outputs $b \in \{0, 1\}$ has advantage ε in solving decision *n+1*-BDHE in G if

$$|Pr(B(TU, e(g, y_0)^{\alpha^{n+1}}) = 0) - Pr(B(TU, T) = 0)| \geq \varepsilon.$$

A weak version is used in this paper[18]. It works as follows: Algorithm B is given as input a random tuple $(g, y_0, y_1, \cdots, y_n, T)$ where $y_i = g^{\alpha^i}, y_0 = g^c$ and $\alpha, c \in Z_p^*$. Algorithm B's goal is to output 1 when $T = e(g, y_0)^{\alpha^{n+1}} = e(g, g)^{\alpha^{n+1}c}$ and 0 otherwise. We also call it decision *n+1*-BDHE problem.

Definition 1. *The (t, ε)-decisional BDHE assumption holds if no* t*-time algorithm has a non-negligible advantage ε in solving the above game.*

2.3 IBBE

An identity-based broadcast encryption scheme(IBBE) with the security parameter and the maximal size m of the target set is specified as follows.

Setup. Take as input the security parameter and output a master secret key and a public key.

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 $S = \{ID_1, \cdots, ID_s\}$ with $s \leq m$, and output a pair (Hdr, K), where Hdr is called the header and K is a key for the symmetric encryption scheme. Compute the encryption C_M of M under the symmetric key K and broadcasts (Hdr, S, C_M).

Decrypt. Take as input a subset S, an identity ID_i and the corresponding private key, if $ID_i \in S$, the algorithm outputs K which is then used to decrypt the broadcast body C_M and recover M.

2.4 Security Model

Following [11-13], we define the security model for IBBE as follows: Both the adversary and the challenger are given as input m, the maximal size of a set of receivers.

Setup: The challenger runs Setup to obtain a public key PK and sends it to A.

Query phase 1: The adversary A adaptively issues queries $q_1, \cdots, q_{s0}$, 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(ID_i, S, Hdr): The challenger responds with $Decrypt$ $(S, ID_i, d_{ID_i}, Hdr, PK)$.

Challenge: When A decides that phase 1 is over, A outputs two same-length messages M_0, M_1 and a challenge identity S^*. The challenger picks a random $b \in \{0, 1\}$ and sets the challenge ciphertext $C^* = Encrypt(params, M_b, S^*)$. The challenger returns C^* to A.

Note that in this paper, we consider the hybrid encryption. In the encryption phase, the encrypted message is a symmetrical key. Hence the challenge can be modified as follows. When A decides that phase 1 is over, the challenger runs Encrypt algorithm 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 $q_{s0+1}, \cdots, q_t$, 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 $Hdr \neq Hdr*$ for any identity of S^*.

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

Let t denote the total number of extraction queries during the game. The advantage of A in winning the game is defined as follows [8]:

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

We call an adversary A in the above game a IND-ID-CCA adversary.

Definition 2. *An IBBE scheme is said to be (t, m)-IND-ID-CCA secure if $Adv_{IBBE}(t, m, A)$ is neglectable.*

2.5 Target Collision Resistant Hashing

A target collision resistant hash function (TCRHF)[19], also known as a universal one-way hash function (UOWHF), is a keyed hash function $H : K \times M_{in} \rightarrow M_{out}$ keyed by $k \in K$, where M_{in} is an input space, M_{out} is an output space and K is a hash-key space. Target collision resistance of a keyed hash function is defined using the following TCR game between the adversary and the TCR challenger:

Step 1. The adversary outputs $m_1 \in M_{in}$.

Step 2. The challenger selects random $k \in K$, and sends this to the adversary.

Step 3. The adversary outputs $m_2 \in M_{in}$. The adversary wins if $H_k(m_1) = H_k(m_2)$ and $m_2 \neq m_1$.

In this game, we call m_2 a target collision against m_1 under the key k.

Definition 3. *We say that a keyed hash function is the* (t, ϵ)*-TCRHF if no adversary running in time less than* t *can win the TCR game with probability greater than* ϵ*.*

3 New Constructions

3.1 Our Works

Setup. To generate the system parameters, PKG picks randomly $g, g_2, h_1, h_2, u_{j0}, u_{j1}, \cdots, u_{jl} \in G$ and $\alpha \in Z_p$, where $1 \leq j \leq m$. Then it sets $g_1 = g^\alpha$. The public parameters are defined as

$$PK = \{g, g_1, g_2, h_1, h_2, u_{j0}, u_{j1}, \cdots, u_{jl}, v = e(g_2, g_1)\}_{1 \leq j \leq m}$$

and the master key is g_2^α .

Extract. Given the identity $ID_i \in S$, where $S = \{ID_1, \cdots, ID_s\}$, $ID_i = (I_{i1}, \cdots, I_{il})$ and I_{ij} denotes the $\frac{n}{l} - bit$ integer in Z_p^*, PKG first computes $F_i = F(ID_i) = u_{i0} \prod_{j=1}^{l} u_{ij}^{I_{ij}}$ for $1 \leq i \leq s$. Then it selects randomly $r_i \in Z_p$ and computes the private keys as follows:

$$d_{ID_i} = (d_{i0}, d_{i1}, d_{i2} = (g_2^\alpha (F_i)^{r_i}, g^{r_i}, \prod_{j=1, j \neq i}^{s} (F_j)^{r_i}).$$

Encrypt. A broadcaster selects a random $k \in Z_p$, computes $Hdr = (C_1, C_2, C_3)$ and K as follows:

$$C_1 = g^k, C_2 = (h_1^t h_2)^k, C_3 = (\prod_{i=1}^{s} F_i)^k, K = v^k.$$

where $t = TCR(C_1)$ and TCR denotes the target collision resistant hash function.

Decrypt. In order to retrieve the message encryption key K encapsulated in the header $Hdr = (C_1, C_2, C_3)$, user with the identity ID_i and the corresponding private key $d_{ID_i} = (d_{i0}, d_{i1}, d_{i2})$ computes

$$K = \frac{e(d_{i0} d_{i2}, C_1)}{e(d_{i1}, C_3)}.$$

Correctness: If $Hdr = (C_1, C_2, C_3)$ is valid, then one can obtain

$$\frac{e(d_{i0} d_{i2}, C_1)}{e(d_{i1}, C_3)} = \frac{e(g_2^\alpha (F_i)^{r_i} \prod_{j=1, j \neq i}^{s} (F_j)^{r_i}, g^k)}{e(g^{r_i}, (\prod_{i=1}^{s} F_i)^k)} = e(g_2^\alpha, g^k) = v^k = K.$$

3.2 Efficiency

Our constructions achieve O(1)-size ciphertexts and O(1)-size private keys, which solve the trade-off of private keys and ciphertexts. In addition, v can be precomputed, so there is no pair computations at the phase of Encryption. Furthermore,

the security of the proposed scheme is reduced to the DBDHE. It is more natural than those in the existing schemes. In addition, the cost of decryption of our scheme is dominated by two pairing, which is much more efficient than that in the available. Table 1 gives the comparisons of efficiency with other schemes. From Table 1, one can find only the scheme in [13] and ours scheme have fully IND-ID-CCA security. But in [14], authors had shown the scheme in [13] was even not chosen plaintext secure(CPA).

Table 1. Comparison of Security

Schemes	Hardness assumption	security model	pk size	Ciphertext size
[8]	GBDHE	IND-sID-CPA	O(1)	O(1)
[10] 1^{st}	BDHE	IND-sID-CPA	O($\|S\|$)	O(1)
[10] 2^{nd}	BDHE	IND-sID-CPA	O(1)	O(1)
[10] 3^{rd}	BDHE	IND-ID-CPA	O(1)	Sublinear of $\|S\|$
[11]	GBDHE	IND-ID-CPA	O(1)	O(1)
[12]	Static	IND-ID-CPA	O($\|S\|$)	O(1)
[13]	TBDHE	IND-ID-**CCA**	O($\|S\|$)	O(1)
Ours	BDHE	IND-ID-**CCA**	O(1)	O(1)

3.3 Security Analysis

We give a game-based security analysis of the proposed scheme. Our proof is mainly based on the one given by Waters [20], where we make some important modifications to be able to deal with chosen-ciphertext attacks.

Theorem 1. *Under the Decisional Bilinear Diffie-Hellman exponent assumption, the IBBE is secure against chosen-ciphertext attacks.*

Proof. We will use a sequence of games to show the security of the new scheme. The first game defined will be the real identity-based encryption game. In this game, the simulator is a real oracle. Then we will change this game until the last one appears. The last one will be one in which the adversary has no advantage unconditionally. These games are run between an adversary A and a simulating algorithm B.

Game0. This is a real CCA game. In this game, we will make many conventions on how the algorithm B chooses the values appearing in the game. These conventions will be purely conceptual and, compared to the original algorithm in the previous works, do not change the distribution of any value appearing during the game. It works as follows.

Setup. B begins by choosing some values $\alpha, a, b \in Z_p$ at random. It selects randomly the elements $g, h_2, u_{j0}, u_{j1}, \cdots, u_{jl}$ and sets $g_1 = g^{\alpha}, h_1 = g^{\alpha+b}$, $g_2 = g^{\alpha^l+a}$, $v = e(g^{\alpha}, g_2)$, which implies the master key $g_2^{\alpha} = g^{a\alpha+\alpha^{l+1}}$. The public keys are

$$PK = \{g, g_1, g_2, h_1, h_2, u_{j0}, u_{j1}, \cdots, u_{jl}, v = e(g_2, g_1)\}.$$

Query Phase 1: The adversary A adaptively issues queries $q_1, \cdots, q_{s0}$, 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(ID_i, S, Hdr): The challenger responds with $Decrypt$ $(S, ID_i, d_{ID_i}, Hdr, PK)$.

Challenge: When A decides that phase 1 is over, A outputs two same-length messages M_0, M_1 and a set of identity S^* on which it wishes to be challenged. The constraint is that the adversary does not make Extraction query for $ID_i^* \in S^*$ in Phase 1. The ciphertext is constructed as follows:

$$C_1^* = g^c, t^* = TCR(C_1^*), C_2^* = (h_1^{t^*} h_2)^c, C_3 = (\prod\nolimits_{i=1}^{s} F_i^*)^c, K^* = v^c.$$

B picks a random $b \in \{0, 1\}$, sets $K_b = K^* = v^c$ and K_{1-b} to a random value. Then B returns $(Hdr^*, K0, K1)$ to A.

Phase 2: The adversary continues to issue queries $q_{s0+1}, \cdots, q$, where qi 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 with the constraint that $S \neq S^*, Hdr \neq Hdr^*$.

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

For $0 \leq i \leq 8$, Let X_i denote the following event:

$$X_i : B \; wins \; the \; game_i.$$

Following the **Game0**, one can obtain $|P(X_0) - 1/2| = Adv_{IBBE}(t, q, A)$.

Game1. This game will be similar to **Game0** but hash collisions will be eliminated. It is worth noting that $C_1^* = g^c$ and $t^* = TCR(C_1^*)$ are independent of the view of A until the Guess phase runs. Hence we can assume the C_1^* and t^* have already generated at the beginning of the game.

In this game, when A issues the Decryption queries at the Query phase, B changes the responds as follows. Let $Hdr = (C_1, C_2, C_3), t = TCR(C_1)$.

If $t = t^*$ and $C_1 \neq C_1^*$, B aborts. Otherwise, it will complete this game. Let $Abort_H$ denote the aborting event. Then following [20], one can obtain

$$|\Pr(X_1) - \Pr(X_0)| \leq \Pr(Abort_H) \leq Adv_A^{TCR}(k),$$

Where $Adv_A^{TCR}(k)$ denotes the advantage of A finding the collision of TCR hash function.

Game2. We will change the game as follows. The generating method comes from the Waters's scheme[20].

Setup. Set $m = 4q$ and choose integers k_i uniformly at random between 0 and l. B then chooses random vectors $X_j = (x_{j0}, x_{j1}, \cdots, x_{jl})$ from Z_m and random vectors $Y_j = (y_{j0}, y_{j1}, \cdots, y_{jl})$ from Z_p, $1 \leq j \leq m$. Let $y_i = y^{\alpha^i}$ for $1 \leq i \leq l$. B assigns the parameters as follows.

$$u_{i0} = g^{y_{i0}} y_{l-i+1}^{p-k_i m + x_{i0}}, u_{ij} = g^{y_{ij}} y_{l-i+1}^{x_{ij}}, 1 \leq i \leq m, 1 \leq j \leq l.$$

Let

$$f_i(ID_i) = y_{i0} + \sum\nolimits_{j=1}^{l} I_{ij} y_{ij},$$

$$J_i(ID_i) = p - k_i m + x_{i0} + \sum\nolimits_{j=1}^{l} I_{ij} x_{ij}.$$

Then

$$F_i = u_{i0} \prod\nolimits_{j=1}^{l} u_{ij}^{I_{ij}} = g^{f_i(ID_i)} y_{l-i+1}^{J_i(ID_i)}.$$

The public keys are

$$PK = \{g, g_1, g_2, h_1, h_2, u_{j0}, u_{j1}, \cdots, u_{jl}, v = e(g_2, g_1)\}.$$

From the A's view, it is not different from the Game1. So one can obtain

$$\Pr(X_2) = \Pr(X_1).$$

Game3. In this game, according to the proof of [20], we will add the Forced abort. Let

$$K_i(ID_i) = \begin{cases} 0 \; if x_{i0} + \sum_{j=1}^{l} I_{ij} x_{ij} = 0 \bmod m \\ 1 \qquad\qquad otherwise \end{cases}$$

In the Query phase and Challenge phase, B will abort if $K_i(ID_i) = 0$ and $K_i(ID_i^*) \neq 0$. Following [20], we have

$$\Pr(X_3) = \Pr(X_2 \cap \overline{Abort}) + \frac{1}{2} \Pr(Abort).$$

Of course, we can add the other forced abort: Artificial Abort[13].

One can obtain $\Pr(X_2 \cap \overline{Abort}) \geq \Pr(X_2) \cdot \Pr(\overline{Abort})$. Following [17,20], we can obtain the upper bound of abortion is $\frac{1}{2(4lq2^{\frac{n}{l}})^s}$. By using the techniques in [20],

We can obtain

$$|\Pr(X_2) - (2(4lq2^{\frac{n}{l}})^s) \Pr(X_3)| \leq \frac{\rho}{2}.$$

where ρ will be given in the end of the proof.

Game4. In this game, We will changes the private key generations. Suppose A issues a private key query for an identity $ID_i \in S$. If $K_i(ID_i) = 0$, then B aborts. Otherwise, B selects a random $r'_i \in Z_p$ and sets the private keys as follows.

$$d_{ID_i} = (d_{i0}, d_{i1}, d_{i2})(g_2^{\alpha}(F_i)^{r_i}, g^{r_i}, \prod_{j=1,j\neq i}^{s}(F_j)^{r_i})$$

where $r_i = r'_i - \frac{\alpha^i}{J_i(ID_i)}$. In fact, according the Game2,

$$\begin{aligned} d_{i0} = g_2^{\alpha}(F_i)^{r_i} &= g^{a\alpha+\alpha^{l+1}}(g^{f_i(ID_i)}y_{l-i+1}^{J_i(ID_i)})^{r'_i-\frac{\alpha^i}{J_i(ID_i)}} \\ &= g^{a\alpha}y_{l+1}(g^{f_i(ID_i)}y_{l-i+1}^{J_i(ID_i)})^{r'_i}(g^{f_i(ID_i)}y_{l-i+1}^{J_i(ID_i)})^{-\frac{\alpha^i}{J_i(ID_i)}} \\ &= y_1^a y_{l+1}(g^{f_i(ID_i)}y_{l-i+1}^{J_i(ID_i)})^{r'_i}y_i^{-\frac{f_i(ID_i)}{J_i(ID_i)}}y_{l+1}^{-1} \\ &= y_1^a(g^{f_i(ID_i)}y_{l-i+1}^{J_i(ID_i)})^{r'_i}y_i^{-\frac{f_i(ID_i)}{J_i(ID_i)}} \end{aligned}$$

Hence B can compute it. For the similar technique, B can compute

$$(d_{i1}, d_{i2}) = (g^{r_i}, \prod_{j=1,j\neq i}^{s}(F_j)^{r_i})$$

since they do not depend on y_{l+1}.

From the adversary A's view, there are no changes from game3 to game4. So

$$\Pr(X_4) = \Pr(X_3).$$

Game5. In this game, we will continue to modify the game. The public key h_2 will be reconstructed. B selects a $\gamma \in Z_p$ and sets $h_2 = g^{\gamma}(h_1)^{-t^*}$, where $t^* = TCR(C_1^*)$. The public keys are given as follows,

$$PK = \{g, g_1, g_2, h_1, h_2, u_{j0}, u_{j1}, \cdots, u_{jl}, v = e(g_2, g_1)\}.$$

where

$$h_1 = g^{\alpha+b}, v = e(g_2, g_1), h_2 = g^{\gamma}(h_1)^{-t^*}, u_{i0} = g^{y_{i0}}y_{l-i+1}^{p-k_i m+x_{i0}}, u_{ij} = g^{y_{ij}}y_{l-i+1}^{x_{ij}},$$

B still knows the master key α. One can obtain easily $\Pr(X_5) = \Pr(X_4)$.

Game6. In this game, we will continue to add the forced aborts. When the adversary A issues Decryption for $(S, Hdr\ )$, B will abort if $K(ID_i) = 0$ and $t = t^*$.

If it happens in the guess phase, this game is indistinguishable from game5. Hence

$$\Pr(X_6) = \Pr(X_5).$$

If it happens in the Query phase, one can obtain easily

$$|\Pr(X_6) - \Pr(X_5)| \leq \frac{q}{p}.$$

Game7. In this game, we will change the response to the decryption queries.

- The adversary A will issue the private key query for $ID_i \in S$. If $K(ID_i) \neq 0$, B responds using the method in game4.
- Then A issues the decryption query for (S, Hdr) . If $K(ID_i) = 0, ID_i \in S$, B gives the responds as follows.

If $t = t^*$, B aborts. Otherwise, B verifies whether $e(C_1, \prod_{i=1}^{s} F_i) = e(g, C_3)$ holds or not. If the verification fails, B returns a random value as the session key. Otherwise, B gives the respond as the follows,

$$K = e(C_2/C_1^{\gamma}, g_2)^{\frac{1}{t-t^*}} / e(C_1^b, g_2).$$

From the A's view, this assigning is a real game as described in game6. In fact,

$$\begin{aligned}
\frac{e(d_{i0}d_{i2}, C_1)}{e(d_{i1}, C_3)} &= e(g_2^{\alpha}(F_i)^{r_i} \prod_{j=1, j\neq i}^{s} (F_j)^{r_i} \\
&= \frac{e(g_2^{\alpha}, C_1) e(\prod_{j=1}^{s} (F_j)^{r_i}, C_1)}{e(g^{r_i}, C_3)} \\
&= \frac{e(g_2, C_1^{\alpha}) e(\prod_{j=1}^{s} (F_j)^{r_i}, C_1)}{e(g^{r_i}, C_3)} \\
&= \frac{(e(C_2/C_1^{\gamma}, g_2)^{\frac{1}{t-t^*}} / e(C_1^b, g_2)) e(\prod_{j=1}^{s} (F_j)^{r_i}, C_1)}{e(g^{r_i}, C_3)}.
\end{aligned}$$

Note that $(C_2/C_1^{\gamma})^{\frac{1}{t-t^*}} = ((h_1^t g^{\gamma} (h_1)^{-t^*})^k)/C_1^{\gamma})^{\frac{1}{t-t^*}} = C_1^b C_1^{\alpha}$.

If $e(C_1, \prod_{i=1}^{s} F_i) = e(g, C_3)$, then

$$\frac{(e(C_2/C_1^{\gamma}, g_2)^{\frac{1}{t-t^*}} / e(C_1^b, g_2)) e(\prod_{j=1}^{s} (F_j)^{r_i}, C_1)}{e(g^{r_i}, C_3)} = K.$$

Otherwise,

$$\frac{(e(C_2/C_1^{\gamma}, g_2)^{\frac{1}{t-t^*}} / e(C_1^b, g_2)) e(\prod_{j=1}^{s} (F_j)^{r_i}, C_1)}{e(g^{r_i}, C_3)}$$

is a random value in G_1.

So

$$\Pr(X_7) = \Pr(X_6).$$

Game8. In this game, the challenge ciphertexs will be changed. Given the challenge identities set S^*. If $K_i(ID_i^*) = 0$, then Hdr^* are constructed as follows.

$$C_1^* = g^c, C_2^* = (g^c)^d, C_3^* = (g^c)^{\sum_{j=1}^{s} f_i(ID_j^*)}, K = Te(y_1, g^a)$$

If $T = e(g, g^c)^{\alpha^{l+1}}$, B selects $b \in \{0, 1\}$, sets $K_b = K = e(g, g^c)^{\alpha^{l+1}} e(y_1, g^a)$.

Otherwise B set K_{1-b} to a random value.

It is worth noting that in the game8 the simulator B can give all simulating value by using $(g, g^c, y_1, \cdots, y_l)$. It does not need to know α. This is a real simulation. So we have

$$\Pr(X_8) = \frac{1}{2},$$

$$|\Pr(X_8) - \Pr(X_7)| \leq Adv_B^{BDDH}.$$

The probabilities all different games are given as follows.

$$\begin{aligned}
Adv_{IBBE}(t, m, A) &= |P(X_0) - 1/2| \\
&\leq |\Pr(X_1) + Adv_A^{TCR} - \frac{1}{2}| \\
&= |\Pr(X_2) + Adv_A^{TCR} - \frac{1}{2}| \\
&\leq |(2(4lq2^{\frac{n}{l}})^s)(\Pr(X_3) - \frac{1}{2}) + \frac{\rho}{2} + Adv_A^{TCR}| \\
&\leq |(2(4lq2^{\frac{n}{l}})^s)(\Pr(X_5) - \frac{1}{2}) + \frac{\rho}{2} + Adv_A^{TCR}| \\
&\leq |(2(4lq2^{\frac{n}{l}})^s)(\Pr(X_6) + \frac{q}{p} - \frac{1}{2}) + \frac{\rho}{2} + Adv_A^{TCR}| \\
&= |(2(4lq2^{\frac{n}{l}})^s)(\Pr(X_7) + \frac{q}{p} - \frac{1}{2}) + \frac{\rho}{2} + Adv_A^{TCR}| \\
&= |(2(4lq2^{\frac{n}{l}})^s)(\Pr(X_7) + \frac{q}{p} - \Pr(X_8)) + \frac{\rho}{2} + Adv_A^{TCR}| \\
&\leq (2(4lq2^{\frac{n}{l}})^s)(Adv_B^{BDDH} + \frac{q}{p}) + \frac{\rho}{2} + Adv_A^{TCR}.
\end{aligned}$$

Let $\rho = Adv_{IBBE}(t, m, A)$. Then

$$Adv_{IBBE}(t, m, A) \leq 2(2(4lq2^{\frac{n}{l}})^s)(Adv_B^{BDDH} + \frac{q}{p}) + 2Adv_A^{TCR}.$$

4 Conclusions

In this paper, a direct chosen-ciphertext secure technique is introduced to construct a new IBBE scheme with the CCA security. It avoids the limitations in the previous works. The new scheme has constant size ciphtertext and private keys. It is more efficient than that in the previous works. In the standard model, we give the security proof by a sequence of games. However, our works also have some shortcomings. The public keys rely on the depth of the users set. In addition, the security of new scheme is reduced to a strong hardness assumption. It still leaves an open problem to construct an IBBE system with direct technique that is secure under a more standard assumption.

Acknowledgments. This paper was partially supported by the Nature Science Foundation of China under grant (61100231, 60970119, 61100165), the National Basic Research Program of China(973) under grant 2007CB311201, Natural Science Basic Research Plan in Shaanxi Province of China (Program No. 2012JQ8044) and the Fundamental Research Funds for the Central Universities of China.

References

1. Shamir, A.: Identity-Based Cryptosystems and Signature Schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)
2. Boneh, D., Franklin, M.: Identity-Based Encryption from the Weil Pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
3. Boneh, D., Boyen, X.: Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004)
4. Boneh, D., Katz, J.: Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity-Based Encryption. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 87–103. Springer, Heidelberg (2005)
5. Boneh, D., Boyen, X.: Secure Identity Based Encryption Without Random Oracles. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 443–459. Springer, Heidelberg (2004)
6. Gentry, C.: Practical Identity-Based Encryption Without Random Oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445–464. Springer, Heidelberg (2006)
7. Mu, Y., Susilo, W., Lin, Y.-X., Ruan, C.: Identity-Based Authenticated Broadcast Encryption and Distributed Authenticated Encryption. In: Maher, M.J. (ed.) ASIAN 2004. LNCS, vol. 3321, pp. 169–181. Springer, Heidelberg (2004)
8. Delerablée, C.: Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 200–215. Springer, Heidelberg (2007)
9. Du, X.J., Wang, Y., Ge, J.H., et al.: An ID-Based Broadcast Encryption Scheme for Key Distribution. IEEE Transactions on Broadcasting 51(2), 264–266 (2005)
10. Gentry, C., Waters, B.: Adaptive Security in Broadcast Encryption Systems (with Short Ciphertexts). In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 171–188. Springer, Heidelberg (2009)
11. Zhang, L.Y., Wu, Q., Hu, Y.P.: New constructions of identity-based broadcast encryption without random oracles. KSII Transactions on Internet and Information Systems 5(2), 428–439 (2011)
12. Zhang, L.Y., Hu, Y.P., Wu, Q.: Adaptively Secure Identity-based Broadcast Encryption with constant size private keys and ciphertexts from the Subgroups. Mathematical and Computer Modelling 55, 12–18 (2012)
13. Ren, Y.L., Gu, D.W.: Fully CCA2 secure identity based broadcast encryption without random oracles. Information Processing Letters 109, 527–533 (2009)
14. Wang, X.A., Weng, J., Yang, X.Y.: Cryptanalysis of an identity based broadcast encryption scheme without random oracles. Information Processing Letters 111, 461–464 (2011)

15. Kiltz, E.: Chosen-ciphertext secure identity-based encryption in the standard model with short ciphertexts. Cryptology ePrint Archive, Report 2006/122 (2006), http://eprint.iacr.org/
16. Kiltz, E.: Chosen-Ciphertext Security from Tag-Based Encryption. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 581–600. Springer, Heidelberg (2006)
17. Zhang, L.Y., Wu, Q., Hu, Y.P.: Direct Chosen-ciphertext technique for IBBE. Journal of Computational Information System 7(9), 3343–3350 (2011)
18. Chatterjee, S., Sarkar, P.: New Constructions of Constant Size Ciphertext HIBE Without Random Oracle. In: Rhee, M.S., Lee, B. (eds.) ICISC 2006. LNCS, vol. 4296, pp. 310–327. Springer, Heidelberg (2006)
19. Cramer, R., Shoup, V.: Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM Journal on Computing 33(1), 167–226 (2003)
20. Waters, B.: Efficient Identity-Based Encryption Without Random Oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005)
21. Canetti, R., Halevi, S., Katz, J.: Chosen-Ciphertext Security from Identity-Based Encryption. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 207–222. Springer, Heidelberg (2004)