Non-interactive Dynamic Identity-Based Broadcast Encryption without Random Oracles

Yanli Ren, Shuozhong Wang, and Xinpeng Zhang

School of Communication and Information Engineering,
Shanghai University,
Shanghai 200072, China
{ryl1982,shuowang,xzhang}@shu.edu.cn

Abstract. A dynamic broadcast encryption (DBE) is a broadcast encryption (BE) scheme where a new user can join the system anytime without modifying preexisting user decryption keys. In this paper, we propose a non-interactive dynamic identity-based broadcast encryption (DIBBE) scheme that is fully secure without random oracles. The PKG does not need to execute any interactive operation with the user during the lifetime of the system. The ciphertext is of constant size, and the public key size is linear in the maximal number of receivers for one encryption. This is the first non-interactive DIBBE scheme which is fully secure without random oracles, and it is collusion resistant for arbitrarily large collusion of users.

1 Introduction

Broadcast encryption (BE) scheme [1] allows a broadcaster to encrypt a message to an arbitrarily designated subset S of users who are listening to a broadcast channel. A BE scheme is said to be fully collusion resistant when, even if all users that are not in S collude, they can by no means infer information about the broadcast message [6]. A dynamic broadcast encryption (DBE) is a BE scheme in which the total number of users is not fixed in the setup phase and a new user can join the system anytime without modifying preexisting user decryption keys.

Identity-based (ID-based) encryption [2] is a cryptosystem where the public key can be represented as an arbitrary string. A private key generator (PKG) uses a master secret key to issue private keys for users based on their identities. Many ID-based schemes have been proposed, but practical schemes were not found until the work of Boneh and Franklin [9] in 2001. Their identity-based encryption (IBE) scheme was based on efficiently computable bilinear maps, but it is only provably secure in the random oracle model. Since 2001, several schemes have been introduced [3,7,10]. There are mainly two security definitions: full security and selective-ID security, and the selective-ID security is weaker than full security.

T.W. Chim and T.H. Yuen (Eds.): ICICS 2012, LNCS 7618, pp. 479–487, 2012.

In 2007, Sakai et al. proposed an identity-based broadcast encryption (IBBE) scheme with constant size ciphertext and private key [11]. The user can join the system anytime without generating new decryption keys for preexisting users. The scheme is only provably secure in the random oracle model. Delerablee proposed another dynamic IBBE scheme [5], where the ciphertext and private key are also of constant size, and the public key is of size linear to the maximal value of the set of receivers. The scheme only achieves selective-ID security in the random oracle model. Gentry et al. proposed several IBBE schemes [8], one of which is dynamic, but it only achieves sublinear size ciphertext in the standard model, or constant size ciphertext in the random oracle model. Boneh et al. described a dynamic IBBE scheme in 2008, which is only selective-ID secure without random oracles [4]. Zhao et al. presented another dynamic IBBE scheme, which is fully secure without random oracles [12]. However, the PKG needs to execute multiple interactive operations with each user in the extract phase, which is not efficient in practice if there are a lot of users in the system. Currently, there is no non-interactive DIBBE scheme available that is fully secure without random oracles.

Our Contributions. In this paper, we solve the open problem raised in [5] and propose a non-interactive DIBBE scheme that is fully secure without random oracles. The scheme has constant size ciphertexts and a tight reduction based on the q-wABDHE assumption. To the best of our knowledge, this is the first non-interactive DIBBE scheme that is fully secure without random oracles. Moreover, our DIBBE scheme is collusion resistant for arbitrarily large collusion of users.

2 Definitions

Below, we review the definition of a symmetric bilinear map and the security model for a DIBBE system. We also discuss the complexity assumption on which our system is based.

2.1 Symmetric Bilinear Map

Let p be a large prime number, G_1 and G_2 be two groups of order p, and g be a generator of G_1. $e : G_1 \times G_1 \to G_2$ is a symmetric bilinear map, which has the following properties [3,9,10]:

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

(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

Our scheme is based on decisional weaker augmented bilinear Diffie-Hellman exponent (wABDHE) assumption. The detailed definition is as follows: Given a vector of $2q+2$ elements

$$(g', (g')^{\alpha^{q+2}}, \ldots, (g')^{\alpha^{2q}}, g, g^{\alpha}, \ldots, g^{\alpha^{q}}, Z) \in G_1^{2q+1} \times G_2$$

to decide whether $Z = e(g', g)^{\alpha^{q+1}}$.

An algorithm A that outputs $w \in \{0, 1\}$ has advantage of ε in solving the decision q-wABDHE problem if

$$\begin{aligned} &|Pr[A(g', (g')^{\alpha^{q+2}}, \ldots, (g')^{\alpha^{2q}}, g, \ldots, g^{\alpha^{q}}, e(g', g)^{\alpha^{q+1}}) = 0] \\ &-Pr[A(g', (g')^{\alpha^{q+2}}, \ldots, (g')^{\alpha^{2q}}, g, \ldots, g^{\alpha^{q}}, Z) = 0]| \geq \varepsilon, \end{aligned}$$

where the probability depends on the random choice of $g, g' \in G_1, \alpha \in Z_p^*, Z \in G_2$, and the random bits consumed by A. We refer to the distribution on the left or right as P_{wABDHE} or R_{wABDHE}.

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

2.3 Security Model

In this section, we define full security against an chosen plaintext attack (IND-ID-CPA) for a non-interactive DIBBE scheme. It is executed by the following game between an adversary A and a challenger B.

Setup. The challenger runs $Setup(\lambda, m)$ algorithm to obtain a public key PK and sends it to A.

Phase 1. The adversary A adaptively issues queries.

Joinging query (ID_i): A sends ID_i to B. The challenger runs $Join$ algorithm on ID_i and returns A a decryption key d_{ID_i}.

Challenge. A sends (S^*, K_0, K_1) to B, where the identities in S^* have not been executed the joining query in Phase 1.

The challenger randomly chooses $w \in \{0, 1\}$ and runs algorithm *Encrypt* to obtain (Hdr^*, K_w). It then gives Hdr^* to adversary A.

Phase 2. A adaptively issues joining query (ID_i), where $\mathsf{ID}_i \notin S^*$.

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

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

Definition. A non-interactive DIBBE system is (t, ε, q) IND-ID-CPA secure if all t-time IND-ID-CPA adversaries making at most q joining queries have advantage of at most ε in winning the above game.

3 The Proposed DIBBE Scheme

We present a non-interactive DIBBE scheme with constant size ciphertext which is fully secure without random oracles. The system makes use of the hybrid encryption paradigm (KEM-DEM) where the broadcast ciphertext only encrypts a symmetric key used to encrypt the broadcast contents.

3.1 Setup

Given security parameter λ and an integer m, the maximal size of the set of receivers for one encryption, two groups G_1, G_2 of order p are constructed. $e : G_1 \times G_1 \to G_2$ is a symmetric bilinear map and g is a generator of G_1. The PKG randomly chooses $l_0 \in G_1, \alpha, \beta, c \in Z_p^*$, and computes $k_0 = g^{\alpha\beta}, \mathrm{f}(x) = cx$. Finally, the public parameters are $(\mathrm{f}(x), g, g^{\alpha}, \ldots, g^{\alpha^m}, l_0, l_0^{\alpha}, \ldots, l_0^{\alpha^m}, k_0, k_0^{\alpha}, \ldots, k_0^{\alpha^m})$ and α, β are the master secret keys of PKG.

3.2 Join

To an $\mathsf{ID}_i \in Z_p^*$, the PKG randomly chooses $r_i \in Z_p^*, h_i \in G_1$, and sets

$$d_{1,i} = (h_i g^{r_i})^{\frac{1}{\alpha\beta(\alpha - ID_i)}}, d_{2,i} = r_i,\ d_{3,i} = (l_0^{f(r_i)} h_i)^{1/\alpha\beta}, lab_i = \{h_i, h_i^{\alpha}, \ldots, h_i^{\alpha^m}\},$$

so the corresponding private key is $d_{ID_i} = (d_{1,i}, d_{2,i}, d_{3,i}, lab_i)$.

3.3 Encrypt

For a set S, randomly choose $s \in Z_p^*, K \in G_2$, and compute

$$c_1 = k_0^{s \cdot \prod_{i \in S}(\alpha - ID_i)}, c_2 = (g^{\alpha})^{-s},\ c_3 = e(g,g)^{-s}, c_4 = K \cdot e(g, l_0)^s.$$

The ciphertext is (Hdr, S), where $Hdr = (c_1, c_2, c_3, c_4)$. Then K is used to encrypt the message.

3.4 Decrypt

The receiver of S with identity ID_i decrypts

$$[e(c_1, d_{1,i}) e(c_2, h_i g^{d_{2,i}})^{A_{i,S}(\alpha)}]^{\frac{1}{\prod_{j \in S}^{j \neq i}(-ID_j)}} c_3^{d_{2,i}} = e(g, h_i)^s,$$
$$[e(c_1, d_{3,i}) e(c_2, l_0^{f(d_{2,i})} h_i)^{B_{i,S}(\alpha)}]^{\frac{1}{\prod_{i \in S}(-ID_i)}} = e(g, l_0^{f(r_i)} h_i)^s,$$

$$[e(g, l_0^{f(r_i)} h_i)^s / e(g, h_i)^s]^{\frac{1}{f(d_{2,i})}} = e(g, l_0)^s, c_4 / e(g, l_0)^s = K,$$

where $A_{i,S}(\alpha) = \frac{1}{\alpha}[\prod_{j \in S}^{j \neq i}(\alpha - \mathsf{ID}_j) - \prod_{j \in S}^{j \neq i}(-\mathsf{ID}_j)]$,
$B_{i,S}(\alpha) = \frac{1}{\alpha}[\prod_{i \in S}(\alpha - \mathsf{ID}_i) - \prod_{i \in S}(-\mathsf{ID}_i)]$.

4 Analysis of the DIBBE Scheme

In this section, we analyze security of the DIBBE scheme and compare the proposed scheme with the previous ones.

4.1 Security

We now prove that the DIBBE scheme achieves IND-ID-CPA security under the q-wABDHE assumption without random oracles.

Theorem 1. Assume that the (t', ε', q)-wABDHE assumption holds in G_1, G_2, then the DIBBE scheme is $(t, \varepsilon, q-1)$ IND-ID-CPA secure for $t = t' - O(t_{exp} \cdot mq), \varepsilon = \varepsilon' + 1/p, q \geq 2m$, where m is the maximal size of the set of receivers for one encryption and t_{exp} is the average time required to exponentiate in G_1 respectively.

Proof. Assume A is an IND-ID-CPA adversary as described in Section 2.3, then we can construct an algorithm B that solves the q-wABDHE problem as follows. At the beginning of the game, B is given

$$(g', (g')^{\alpha^{q+2}}, \ldots, (g')^{\alpha^{2q}}, g, g^{\alpha}, \ldots, g^{\alpha^q}, Z) \in G_1^{2q+1} \times G_2$$

to decide whether $Z = e(g', g)^{\alpha^{q+1}}$.

Setup. B randomly chooses $E(x) = \sum_{j=0}^{m-1} b_{0,j} x^j, \beta \in Z_p^*$ and sets

$$F(x) = xE(x) + b_0, \mathrm{f}(x) = \frac{1}{b_0} x, k_0 = g^{\alpha\beta}, k_0^{\alpha} = g^{\alpha^2\beta}, \ldots, k_0^{\alpha^m} = g^{\alpha^{m+1}\beta},$$
$$l_0 = g^{F(\alpha)}, l_0^{\alpha} = g^{\alpha F(\alpha)}, \ldots, l_0^{\alpha^m} = g^{\alpha^m F(\alpha)}, \text{ where } b_{0,j}, b_0 \in Z_p^*.$$

In fact, B can compute the parameters as follows:

$$l_0 = g^{b_0} \prod_{j=0}^{m-1} (g^{\alpha^{j+1}})^{b_{0,j}} = g^{\sum_{j=0}^{m-1} b_{0,j}\alpha^{j+1} + b_0} = g^{\alpha E(\alpha) + b_0} = g^{F(\alpha)},$$
$$l_0^{\alpha} = g^{b_0 \alpha} \prod_{j=0}^{m-1} (g^{\alpha^{j+2}})^{b_{0,j}} = g^{\sum_{j=0}^{m-1} b_{0,j}\alpha^{j+2}} g^{b_0\alpha} = g^{\alpha F(\alpha)}, \ldots,$$
$$l_0^{\alpha^m} = g^{b_0 \alpha^m} \prod_{j=0}^{m-1} (g^{\alpha^{j+m+1}})^{b_{0,j}} = g^{\sum_{j=0}^{m-1} b_{0,j}\alpha^{j+m+1}} g^{b_0\alpha^m} = g^{\alpha^m F(\alpha)}.$$

B sends $(\mathrm{f}(x), g, g^{\alpha}, \ldots, g^{\alpha^m}, l_0, l_0^{\alpha}, \ldots, l_0^{\alpha^m}, k_0, k_0^{\alpha}, \ldots, k_0^{\alpha^m})$ to A as the public parameters. Note that the public keys are randomly distributed and indistiguishable from the real scheme for the adversary since $E(x), b_0$ and β are randomly chosen.

Phase 1. The adversary A adaptively issues queries.

Joining query $\langle \mathsf{ID}_i \rangle$: A sends ID_i to B. B randomly chooses

$$C_i(x) = \sum_{j=0}^{m-2} b_{i,j} x^j, D_i(x) = x(x - \mathsf{ID}_i)C_i(x) + b_i,$$

where $b_{i,j}, b_i \in Z_p^*$, and computes $d_{ID_i} = (d_{1,i}, d_{2,i}, d_{3,i}, lab_i)$ as below:

$$d_{1,i} = (g^{C_i(\alpha)})^{\frac{1}{\beta}}, d_{2,i} = -D_i(\mathsf{ID}_i) = -b_i,$$
$$d_{3,i} = (g^{-\frac{b_i}{b_0}E(\alpha)+(\alpha-ID_i)C_i(\alpha)})^{\frac{1}{\beta}}.$$
$$lab_i = \{h_i = g^{D_i(\alpha)}, h_i^{\alpha} = g^{\alpha D_i(\alpha)}, \ldots, h_i^{\alpha^m} = g^{\alpha^m D_i(\alpha)}\}.$$

Now we need to show that the adversary can compute d_{ID_i} as follows.

$$d_{1,i} = (\prod_{j=0}^{m-2} g^{b_{i,j}\alpha^j})^{\frac{1}{\beta}} = (g^{\sum_{j=0}^{m-2} b_{i,j}\alpha^j})^{\frac{1}{\beta}} = (g^{C_i(\alpha)})^{\frac{1}{\beta}},$$
$$d_{2,i} = -ID_i(ID_i - \mathsf{ID}_i)C_i(x) - b_i = -b_i = -D_i(\mathsf{ID}_i),$$

$$d_{3,i} = (\prod_{j=0}^{m-1} g^{-\frac{b_i}{b_0}b_{0,j}\alpha^j} \cdot \prod_{j=0}^{m-2} g^{b_{i,j}(\alpha-ID_i)\alpha^j})^{\frac{1}{\beta}}$$
$$= (g^{-\frac{b_i}{b_0}E(\alpha)+(\alpha-ID_i)C_i(\alpha)})^{\frac{1}{\beta}},$$

$$h_i = g^{b_i} \prod_{j=0}^{m-2} (g^{\alpha^{j+2}} g^{-ID_i\alpha^{j+1}})^{b_{i,j}} = g^{\alpha(\alpha-ID_i)\sum_{j=0}^{m-2} b_{i,j}\alpha^j} g^{b_i} = g^{D_i(\alpha)},$$
$$h_i^{\alpha} = g^{b_i\alpha} \prod_{j=0}^{m-2} (g^{\alpha^{j+3}})^{b_{i,j}} (g^{\alpha^{j+2}})^{-ID_i b_{i,j}} = g^{\alpha D_i(\alpha)},$$
$$\cdots\cdots,$$
$$h_i^{\alpha^m} = g^{b_i\alpha^m} \prod_{j=0}^{m-2} (g^{\alpha^{j+m+2}})^{b_{i,j}} (g^{\alpha^{j+m+1}})^{-ID_i b_{i,j}} = g^{\alpha^m D_i(\alpha)}.$$

It is a valid private key, because

$$d_{1,i} = (g^{C_i(\alpha)})^{\frac{1}{\beta}} = g^{\frac{D_i(\alpha)-b_i}{\alpha\beta(\alpha-ID_i)}} = g^{\frac{D_i(\alpha)-D_i(ID_i)}{\alpha\beta(\alpha-ID_i)}} = (h_i g^{d_{2,i}})^{\frac{1}{\alpha\beta(\alpha-ID_i)}},$$
$$d_{2,i} = -D_i(\mathsf{ID}_i) = -ID_i(ID_i - \mathsf{ID}_i)C_i(x) - b_i = -b_i,$$
$$d_{3,i} = (g^{(-\frac{b_i}{b_0})(F(\alpha)-b_0)+D_i(\alpha)-b_i})^{\frac{1}{\alpha\beta}} = g^{\frac{(-\frac{b_i}{b_0})F(\alpha)+D_i(\alpha)}{\alpha\beta}} = (l_0^{f(d_{2,i})} h_i)^{\frac{1}{\alpha\beta}}.$$
$$lab_i = \{h_i = g^{D_i(\alpha)}, h_i^{\alpha} = g^{\alpha D_i(\alpha)}, \ldots, h_i^{\alpha^m} = g^{\alpha^m D_i(\alpha)}\}.$$

We conclude that $d_{1,i}, d_{2,i}, d_{3,i}, h_i$ are random distributed for the adversary since $E(x), b_0, \beta, C_i(x), b_i$ are randomly chosen. Thus, d_{ID_i} is randomly distributed and indistiguishable from the real scheme for the adversary because of the randomness of $E(x), b_0$ and $C_i(x), b_i, \beta$.

Challenge. A sends (S^*, K_0, K_1) to B, where the identities of S^* have not been executed the joining query in Phase 1.

B randomly chooses $K_w, w \in \{0, 1\}$, and sends Hdr^* to A, where

$$c_1^* = (g'^{\alpha^{q+2}})^{\beta \prod_{i \in S^*}(\alpha - ID_i)}, c_2^* = (g')^{-\alpha^{q+2}}, c_3^* = Z^{-1},,$$
$$c_4^* = K_w \cdot Z^{b_0} \cdot e(g'^{\alpha^{q+2}}, g^{E(\alpha)}), Hdr^* = (c_1^*, c_2^*, c_3^*, c_4^*, S^*).$$

Let $s^* = \log_g g' \cdot \alpha^{q+1}$. If $Z = e(g', g)^{\alpha^{q+1}}$,

$$c_1^* = (g^{s^*\alpha})^{\beta} \prod_{i \in S^*} (\alpha - ID_i) = (k_0^{s^*}) \prod_{i \in S^*} (\alpha - ID_i),$$
$$c_2^* = (g')^{-\alpha^{q+2}} = (g^{\alpha})^{-s^*},\ c_3^* = e(g', g)^{-\alpha^{q+1}} = e(g, g)^{-s^*},$$
$$c_4^* = K_w \cdot e(g'^{\alpha^{q+1}}, g^{F(\alpha)}) = K_w \cdot e(g, l_0)^{s^*}.$$

Since $\log_g g', \alpha$ are uniformly random, s^* is uniformly random, and so Hdr^* is a valid and appropriately-distributed challenge to A.

Phase 2. A adaptively issues joining query (ID_i), where $\mathsf{ID}_i \notin S^*$.

Guess. A submits a guess $w' \in \{0, 1\}$. If $w' = w$, B outputs 0 (indicating that $Z = e(g', g)^{\alpha^{q+1}}$); else, it outputs 1.

Probability Analysis: When Z is sampled from P_{wABDHE}, Hdr^* is a valid ciphertext for the randomness of s^*, A can guess $w' = w$ with probability $1/2 + \varepsilon'$. When Z is sampled from R_{wABDHE}, $c_4^* = K_w \cdot Z^{b_0} \cdot e(g'^{\alpha^{q+2}}, g^{E(\alpha)})$. Since $g', Z, b_0, E(x)$ are uniformly random, c_4^*/K_w is random for the adversary except probability $1/p$, and so A can only guess $w' = w$ with probability $1/2 + 1/p$.

Time Complexity: Each joining query requires $O(m)$ exponentiations in G_1. Since A makes at most $q - 1$ such queries, $t' = t + O(t_{exp} \cdot mq)$.

In the reduction, B's success probability and time complexity are the same as that of A, except for additive factors depending on p and q respectively. So, the DIBBE system has a tight security reduction without random oracles. This completes the proof for Theorem 1.

4.2 Comparison

In this section, we compare the known DIBBE schemes in Table 1.

Table 1. Comparison among DIBBE schemes

Scheme	Non-Interactive	Random oracles	Security model	Public key size	Ciphertext size	Decrypt time	Pairing
[5]	yes	yes	sID	$O(m)$	$O(1)$	$O(m)$	2
[11]	yes	yes	ID	$O(m)$	$O(1)$	$O(m)$	2
[4]	yes	no	sID	$O(m)$	$O(1)$	$O(m)$	2
[8]	yes	no	ID	$O(\sqrt{m})$	$O(\sqrt{m})$	$O(m)$	2
[12]	no	no	ID	$O(m)$	$O(1)$	$O(m)$	2
Ours	yes	no	ID	$O(m)$	$O(1)$	$O(m)$	4

In Table 1, "sID, ID" denote "selective-ID" and "adaptive-ID" security model respectively, and m represents the maximal number of receivers for one encryption.

From Table 1, we conclude that the scheme in [5] and [11] are provably secure in the random oracle model, and the scheme of [4] is selective-ID secure without random oracles. In [8,12], the scheme only achieves sublinear size ciphertext or the PKG needs to interact with each user for many times though the schemes are fully secure without random oracles. Our scheme is non-interactive with constant size ciphertext and also fully secure without random oracles. Thus, the proposed scheme has stronger security than that of the previous ones without decreasing the efficiency.

5 Conclusion

In this paper, we construct a non-interactive dynamic IBBE scheme with constant size ciphertexts, which achieves full security without random oracles. The PKG does not need to execute any interactive operation with each user. The security reduction is based on decision q-wABDHE assumption, it remains an open problem to construct a fully secure non-interactive DIBBE scheme based on a more natural assumption, which has a tight reduction without random oracles.

Acknowledgement. This work was supported by the Natural Science Foundation of China (61202367, 61073190, 60832010), and the Research Fund for the Doctoral Program of Higher Education of China (20113108110010).

References

1. Fiat, A., Naor, M.: Broadcast Encryption. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 480–491. Springer, Heidelberg (1994)
2. 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)
3. Waters, B.: Efficient Identity-Based Encryption Without Random Oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005)
4. Libert, B., Vergnaud, D.: Towards Black-Box Accountable Authority IBE with Short Ciphertexts and Private Keys. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 235–255. Springer, Heidelberg (2009)
5. Delerablee, 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)
6. Delerablee, C., Paillier, P., Pointcheval, D.: Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys. In: Takagi, T., Okamoto, T., Okamoto, E., Okamoto, T. (eds.) Pairing 2007. LNCS, vol. 4575, pp. 39–59. Springer, Heidelberg (2007)

7. Gentry, C.: Practical Identity-Based Encryption Without Random Oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445–464. Springer, Heidelberg (2006)
8. 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)
9. 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)
10. 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)
11. Sakai, R., Furukawa, J.: Identity-Based Broadcast Encryption, `http://eprint.iacr.org/2007/217`
12. Zhao, X., Zhang, F.: Fully CCA2 Secure Identity-Based Broadcast Encryption with Black-Box Accountable Authority. Journal of Systems and Software 85, 708–716 (2012)