Journal of Computer and Communications, 2019, 7, 23-30
http://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

An Efficient Identity-Based Homomorphic Broadcast Encryption

Mei Cai

IT Department, Jinan University Library, Guangzhou, China
Email: tmclib@jnu.edu.cn

How to cite this paper: Cai, M. (2019) An Efficient Identity-Based Homomorphic Broadcast Encryption. *Journal of Computer and Communications*, **7**, 23-30.
https://doi.org/10.4236/jcc.2019.72002

Received: January 8, 2019
Accepted: February 8, 2019
Published: February 11, 2019

Abstract

Broadcast encryption (BE) allows a sender to broadcast its message to a set of receivers in a single ciphertext. However, in broadcast encryption scheme, ciphertext length is always related to the size of the receiver set. Thus, how to improve the communication of broadcast encryption is a big issue. In this paper, we proposed an identity-based homomorphic broadcast encryption scheme which supports an external entity to directly calculate ciphertexts and get a new ciphertext which is the corresponding result of the operation on plaintexts without decrypting them. The correctness and security proofs of our scheme were formally proved. Finally, we implemented our scheme in a simulation environment and the experiment results showed that our scheme is efficient for practical applications.

Keywords

Identity-Based, Broadcast Encryption, Homomorphic, Communication

1. Introduction

After been introduced by Fiat and Naor [1], broadcast encryption (BE) is widely studied and improved. BE allows a sender to broadcast its message to a set of receivers in a single ciphertext. Compared with generating individual ciphertext for each of receivers, BE scheme is much efficient in terms of storage and computation. Due to the advantages, BE scheme is widely used in many applications, such as TV services [2], Cloud Storage [3], Emails [4] and so on. In order to eliminate the complicated certificate management of BE scheme in traditional public key setting, Baek *et al.* extended BE into identity-based setting and proposed the first identity-based broadcast encryption (IBBE) scheme [5].

Instead of using receivers' public keys, the sender can encrypt its message under receivers' identity set in IBBE scheme. This eliminates traditional public key infrastructure (PKI) for managing user's public key. This scheme brings convenience, but the efficiency is not practical since the ciphertext size is related to size receiver set. To solve this problem, Delerablée proposed the first constant size ciphertext IBBE scheme [6]. After that, Gentry *et al.* focused on the security of IBBE scheme and proposed the first IND-CAP secure IBBE scheme in standard model [7]. Their scheme also has short ciphertext. In 2016, He *et al.* proposed an efficient IBBE scheme which achieves anonymous and IND-CCA security simultaneously [8]. The ciphertext size of their scheme is not constant. However, due to their promising construction, the running time of decryption of their scheme is almost constant.

Although BE and IBBE schemes have many advantages for practical applications, it is still not enough for variety of applications. Now we consider a subscription system. The service provider encrypts its different kinds of messages under corresponding subscribers' identity sets and sends ciphertexts through networks. For one receiver, who subscribes two different messages, it must receive two ciphertexts and decrypt them respectively.

However, in some scenarios, these two messages should be calculated into one. If the network devices, such as a gateway or a fog node, can calculate ciphertexts and transforms them into a new one without decrypting them, the communication cost will be significantly reduced. Unfortunately, there is still no concrete identity-based homomorphic broadcast encryption construction.

In this paper, we propose present the formally definition of identity-based homomorphic broadcast encryption (IBHBE). Then we give a concrete construction based on [8]. The proposed scheme is formally proved for correctness and security, which achieves IND-CPA security in random oracle model. Finally, we also show that our scheme is efficient for practical applications.

The remainder of the paper is organized as followed. In Section 2, we review the preliminaries used in this paper. Then we propose our IBHEB construction and prove the correctness and security in Section 3. The performance evaluation is given in Section 5. Finally, we conclude this paper in Section 5.

2. Preliminaries

2.1. Bilinear Maps

On defining a group generator $\mathcal{G}$, it takes a security parameter and outputs a description of a bilinear map group $\mathcal{G}=\left(p,\mathbb{G},\mathbb{G}_T,e\right)$, where p is a prime, $\mathbb{G}$ and $\mathbb{G}_T$ are multiplicative cyclic groups of order *p*, and *e* is a map $e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$, such that:

- Bilinearity: For all $u,v\in\mathbb{G}$ and $\forall a,b\in\mathbb{Z}_p$, there has $e\left(u^a,v^b\right)=e\left(u,v\right)^{ab}$.
- Non-degeneracy: For any generator *g* of $\mathbb{G}$, $e\left(g,g\right)\neq 1_{\mathbb{G}_T}$.
- Computability: $\forall u,v\in\mathbb{G}$, there exists an efficient algorithm to compute $e\left(u,v\right)$.

2.2. Decisional Bilinear Diffie-Hellman Problem

The decisional bilinear Diffie-Hellman (DBDH) problem is defined as follows.

Definition 1. (Decisional Bilinear Diffie-Hellman Problem). Given a group generator $\mathcal{G}$, and its output $\mathcal{G} = (p, \mathbb{G}, \mathbb{G}_T, e)$. For $a, b, c \in \mathbb{Z}_p$, a generator g of $\mathbb{G}$ and (g^a, g^b, g^c), define whether $Z = e(g,g)^{abc}$ or not. For a probabilistic polynomial time (PPT) adversary $\mathcal{A}$, the advantage of solving the DBDH problem is:

$$Adv_{\mathcal{A}}^{DBDH} = \left| Pr\left[\mathcal{A}\left(g, g^a, g^b, g^c, e(g,g)^{abc}\right) = 1\right] - Pr\left[\mathcal{A}\left(g, g^a, g^b, g^c, Z\right) = 1\right]\right|,$$

where $Z \xleftarrow{\$} \mathbb{G}_T$.

We say the DBDH problem holds in bilinear map $\mathcal{G} = (p, \mathbb{G}, \mathbb{G}_T, e)$ if for any PPT adversary, the advantage of solving DBDH problem $Adv_{\mathcal{A}}^{DBDH}$ is negligible.

2.3. Identity-Based Homomorphic Broadcast Encryption

An identity-based homomorphic broadcast encryption (IBHBE) scheme is an identity-based encryption, which supports a set of receivers to decrypt ciphertext. Suppose that the message space is $\mathcal{M}$, an identity-based broadcast encryption has four probability polynomial time (PPT) algorithms and one protocol:

- **Setup** (λ). It takes input a security parameter λ, and outputs the public parameter *pp* and a master secret key *msk*.
- **Extract** (*msk*, *ID*). It takes input a master secret key *msk* and an identity *ID*, and outputs a private key sk_{ID}.
- **Encrypt** (*pp*, *S*, *m*). It takes input the public parameter *pp*, a receiver set *S*, and a message *m*, and outputs a ciphertext *CT*.
- **Decrypt** (*pp*, sk_{ID}, *CT*). It takes input the public parameter *pp*, a secret key sk_{ID}, and a ciphertext *CT*, and outputs a message *m*.
- **Eval** (*pp*, CT_0, CT_1). By interacting with a receiver with identity $ID \in S_0 \cap S_1$, any entity can use the evaluation protocol to a helper value *t* for these two ciphertexts. Then the entity can use the helper value to calculate the two ciphertext into a new one, which is a valid ciphertext of the corresponding operation result of the two plaintexts of ciphertext.

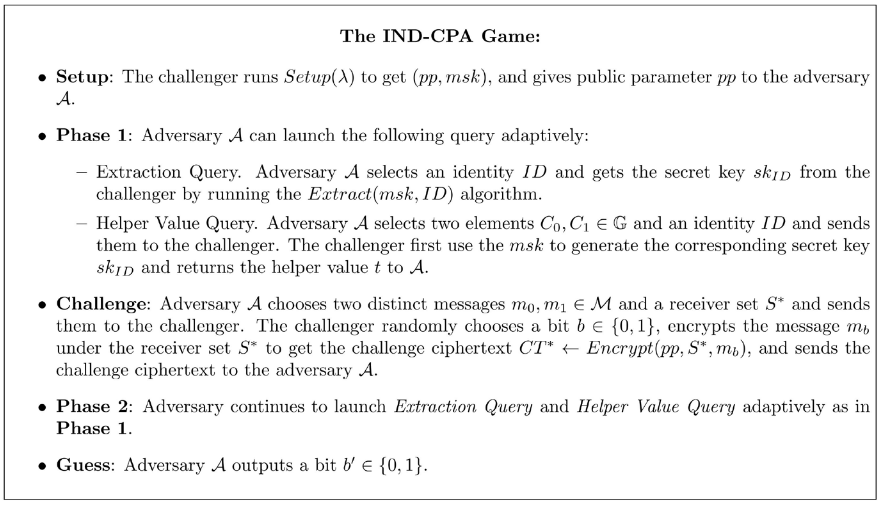
Correctness. For all identity sets S_0, S_1, messages m_0, m_1, identity *ID*, if $(pp, msk) \leftarrow Setup(\lambda)$, $sk_{ID} \leftarrow Extract(msk, ID)$, $CT_0 \leftarrow Encrypt(pp, S_0, m_0)$, and $CT_1 \leftarrow Encrypt(pp, S_1, m_1)$, there has

- If $ID \in S_0$, then $Decrypt(pp, sk_{ID}, CT_0) = m_0$.
- If $ID \in S_0 \cap S_1$, then $Decrypt\left(pp, sk_{ID}, Eval\left(pp, CT_0, CT_1; sk_{ID}\right)\right) = m_0 + m_1$.

Security Model of IBBE. We consider IBBE under IND-CPA security model, which is captured in the following game (**Figure 1**).

Note that, in **Challenge** step, the adversary cannot choose a receiver set S^* which contains any identity is queried in **Phase 1**. Similarly, in **Phase 2**, the adversary cannot launch Extraction Query on any identity belonged to the receiver set S^* or any Helper Value Query on the challenge ciphertext.

Definition 2. We say an IBBE scheme Π is IND-CPA secure, if for any probabilistic polynomial time (PPT) adversary $\mathcal{A}$, the advantage to win the **IND-CPA Game** $Adv_{\mathcal{A},\Pi}^{IND\text{-}CPA}$ is negligible; where,



The IND-CPA Game:

- **Setup**: The challenger runs $Setup(\lambda)$ to get (pp, msk), and gives public parameter pp to the adversary $\mathcal{A}$.
- **Phase 1**: Adversary $\mathcal{A}$ can launch the following query adaptively:
  - Extraction Query. Adversary $\mathcal{A}$ selects an identity ID and gets the secret key sk_{ID} from the challenger by running the $Extract(msk, ID)$ algorithm.
  - Helper Value Query. Adversary $\mathcal{A}$ selects two elements $C_0, C_1 \in \mathbb{G}$ and an identity ID and sends them to the challenger. The challenger first use the msk to generate the corresponding secret key sk_{ID} and returns the helper value t to $\mathcal{A}$.
- **Challenge**: Adversary $\mathcal{A}$ chooses two distinct messages $m_0, m_1 \in \mathcal{M}$ and a receiver set S^* and sends them to the challenger. The challenger randomly chooses a bit $b \in \{0,1\}$, encrypts the message m_b under the receiver set S^* to get the challenge ciphertext $CT^* \leftarrow Encrypt(pp, S^*, m_b)$, and sends the challenge ciphertext to the adversary $\mathcal{A}$.
- **Phase 2**: Adversary continues to launch *Extraction Query* and *Helper Value Query* adaptively as in **Phase 1**.
- **Guess**: Adversary $\mathcal{A}$ outputs a bit $b' \in \{0,1\}$.

Figure 1. The IND-CPA game.

$$Adv_{\mathcal{A},\Pi}^{IND-CPA} = \left| Pr\left[b = b'\right] - \frac{1}{2} \right| \tag{1}$$

3. Identity-Based Homomorphic Broadcast Encryption

In this section, we first introduce our identity-based homomorphic broadcast encryption. Then we give the correctness and security proofs of the construction.

3.1. Our Construction

Our IBHBE scheme contains four PPT algorithm and a one-round protocol.

- **Setup (*λ*):** The algorithm takes input a security parameter λ, and outputs a bilinear map $(p, \mathbb{G}, \mathbb{G}_T, e) \leftarrow \mathcal{G}(\lambda)$. Here, p is a prime number, $\mathbb{G}$ and $\mathbb{G}_T$ are p order multiplicative cyclic groups, and e is a bilinear map $e:(\mathbb{G}, \mathbb{G}) \rightarrow \mathbb{G}_T$. Then, it randomly picks generator $g \in \mathbb{G}$ and $\alpha \in \mathbb{Z}_p$, computes $g_1 = g^{\alpha}$. It also defines message space $\mathcal{M} = \mathbb{Z}_q$ and two secure hash functions $H_1:\{0,1\}^* \rightarrow \mathbb{G}$, $H_2:\mathbb{G}_T \rightarrow \mathbb{Z}_q$, where q is a prime number. Then it sets the master secret key $msk = \alpha$ and opens the public parameter pp as $(p, \mathbb{G}, \mathbb{G}_T, e, q, g, g_1, H_1, H_2)$.
- **Extract (*msk*, *ID*):** For a system user with identity *ID*, the algorithm generates the user's secret key as $sk_{ID} = H_1(ID)^{msk} = H_1(ID)^{\alpha}$.
- **Encrypt (*pp*, *S*, *m*):** Any user can run the encryption algorithm. For a message $m \in \mathcal{M}$ and a receiver set $S = \{ID_1, ID_2, \cdots, ID_n\}$, the algorithm first chooses random number $r \in \mathbb{Z}_p$, and computes $C = g^r$. Then for each $ID_i \in S$, it computes $t_i = H_2\left(e\left(H_1(ID_i)^r, g_1\right)\right)$, $F(x) = \prod_{i=1}^{n}(x - t_i) + m \bmod q$. It computes the expansion formula of $F(x)$ as $F(x) = \sum_{j=0}^{n} a_j \cdot x^j \bmod q$. Then the ciphertext is $CT = (C, \boldsymbol{A})$, where $\boldsymbol{A}$ is a vector,
$$\boldsymbol{A} = (a_0, a_1, \cdots, a_n) \tag{2}$$
- **Decrypt (*pp*, *sk*$_{ID}$, *CT*):** When decrypting ciphertext *CT* with the secret key

sk_{ID}, the algorithm first computes $\tau = H_2\left(e\left(sk_{ID}, C\right)\right)$. Then it sets a vector $\boldsymbol{T}$ as

$$\boldsymbol{T} = \left(\tau^0, \tau^1, \cdots, \tau^n\right). \tag{3}$$

Finally, it outputs the message as $m = \boldsymbol{A} \cdot \boldsymbol{T} \bmod q$.

- **Eval (*pp*, *CT*$_0$, *CT*$_1$):** Parse CT_0 and C_1 as $\left(C_0, \boldsymbol{A}_0\right)$ and $\left(C_1, \boldsymbol{A}_1\right)$, which are encrypted under identity sets S_0 and S_1 respectively. Then, an external entity, such as a gateway, can generate a new ciphertext for a specified receiver with identity $ID \in S_0 \cap S_1$. This protocol is shown in Figure 2. Here, the operation $\circ$ means the hadamard product of two vectors. $\left(\boldsymbol{A} \circ \boldsymbol{B}\right)_i = \left(\boldsymbol{A}_i \cdot \boldsymbol{B}_i\right)$.

3.2. Correctness Proof

As claimed in Section 2.3, the correctness of our IBHBE scheme has two aspects. Next we give the detailed proof.

Proof. The correctness proof is described as follows.

- For the first aspect, the condition to decrypt a ciphertext under identity set S_0 is that the receiver can computer a valid value x equaled one of t_i. When a receiver with identity ID tries to decrypt a ciphertext $CT_0 = \left(C, \boldsymbol{A}\right)$ encrypted under identity set S_0, it computes

$$\begin{aligned}\tau &= H_2\left(e\left(sk_{ID}, C\right)\right) = H_2\left(e\left(H_1\left(ID\right)^\alpha, g^r\right)\right)\\ &= H_2\left(e\left(H_1\left(ID\right)^r, g^\alpha\right)\right) = H_2\left(e\left(H_1\left(ID\right)^r, g_1\right)\right).\end{aligned}$$

If $ID \in S_0$, the value τ must be one of t_i to construct $F\left(x\right)$. Then we have

$$\begin{aligned}\boldsymbol{A} \cdot \boldsymbol{T} &= \sum\nolimits_{j=0}^{n} a_j \cdot \tau^j \bmod q\\ &= \prod\nolimits_{i=1}^{n}\left(\tau - t_i\right) + m \bmod q\\ &= m \bmod q\end{aligned}$$

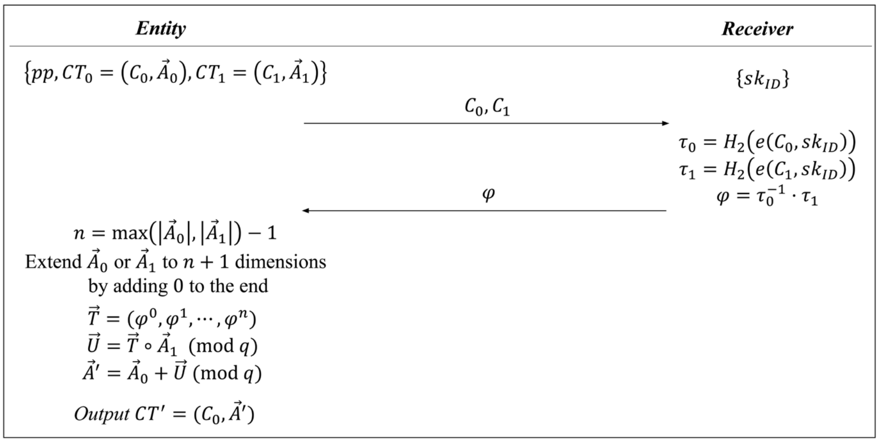

Entity
Receiver
$\{pp, CT_0 = (C_0, \vec{A}_0), CT_1 = (C_1, \vec{A}_1)\}$
$\{sk_{ID}\}$
C_0, C_1
$\tau_0 = H_2(e(C_0, sk_{ID}))$
$\tau_1 = H_2(e(C_1, sk_{ID}))$
$\varphi = \tau_0^{-1} \cdot \tau_1$
φ
$n = \max(|\vec{A}_0|, |\vec{A}_1|) - 1$
Extend $\vec{A}_0$ or $\vec{A}_1$ to $n + 1$ dimensions by adding 0 to the end
$\vec{T} = (\varphi^0, \varphi^1, \cdots, \varphi^n)$
$\vec{U} = \vec{T} \circ \vec{A}_1 \pmod q$
$\vec{A}' = \vec{A}_0 + \vec{U} \pmod q$
Output $CT' = (C_0, \vec{A}')$

Figure 2. The eval protocol.

- Now we consider the second aspect. Suppose two ciphertexts CT_0, CT_1 are encrypted under two identity sets S_0, S_1. If the receiver's identity ID is in $S_0 \cap S_1$, then it can compute τ_0 and τ_1 which can be used to decrypt CT_0 and CT_1 respectively. Suppose the new ciphertext output from evaluation protocol is $CT' = (C_0, \boldsymbol{A}')$. The receiver first computes $\tau = \tau_0$, then decrypts the ciphertext by calculating

$$\begin{aligned}\boldsymbol{A}' \cdot \boldsymbol{T} &= \sum\nolimits_{j=0}^{n} a'_j \cdot \tau^j \bmod q \\ &= \sum\nolimits_{j=0}^{n} a_{0,j} \cdot \tau_0^j + \sum\nolimits_{j=0}^{n} u_{0,j} \cdot \tau_0^j \bmod q \quad // \left(\boldsymbol{A}' = \boldsymbol{A}_0 + \boldsymbol{U}, a'_j = a_{0,j} + u_j\right) \\ &= m_0 + \sum\nolimits_{j=0}^{n} a_{1,j} \cdot \varphi^j \cdot \tau^j \bmod q \\ &= m_0 + \sum\nolimits_{j=0}^{n} a_{1,j} \cdot (\varphi \cdot \tau)^j \bmod q \\ &= m_0 + \sum\nolimits_{j=0}^{n} a_{1,j} \cdot \tau^j \bmod q \quad // \left(\varphi = \tau_0^{-1} \cdot \tau_1\right) \\ &= m_0 + m_1\end{aligned}$$

Then we finish the correctness proof of our IBHBE scheme construction.

3.3. Security Proof

In this section, we give the formalized security proof of our IBHBE scheme under random oracle model.

Theorem 1. Suppose H_1 and H_2 are random oracles, and the DBDH problem holds, then our IBHBE construction is IND-CPA secure.

Proof. Suppose there exists a PPT adversary $\mathcal{A}$ has non-negligible advantage to win the IND-CAP game, then an other PPT adversary $\mathcal{B}$ can use $\mathcal{A}$'s ability to break the DBDH problem.

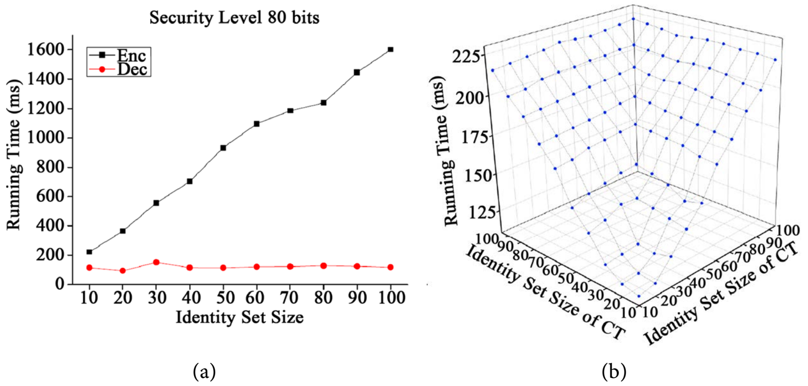
Note that, the first part of a valid ciphertext is a mask value of a valid ciphertext of Boneh and Franklin's identity-based encryption scheme [9]. Since the scheme [9] is IND-CPA secure against PPT adversary, then the no one can distinguish random values between t_is, which are used to construct the function $F(x)$.

Now we focus on the elements of $\mathcal{A}$. We have $a_0 = \sum_{i=1}^{t}(-t_i) + m$. As we already know t_i is indistinguishable from random number. Therefore, no one can restore even one-bit information of m from a_0 since $\prod_{i=1}^{n}(-t_i)$ is also random.

4. Performance

In this section, we give the performance experiments of our construction. All the programs were executed on a personal laptop equipped with Ubuntu 16.04 operation system, Inter(R) Core(TM) i5-8200 CPU @ 2.5 GHz processor and 8G DDR3-RAM. A 1000 Mbps LAN is used to support the evaluation protocol. The programs are implemented with java (JDK 1.8) and jPBC library [10]. We set security parameter with $\lambda = 80$, choose bilinear group with a 160-bit, and $|p| = |q| = 512$. All experiment results are averaged over 1000 runs.

We first estimate the encryption and decryption algorithm with setting identity set size from 10 to 100. The result shown in **Figure 3(a)** indicates that the



(a) (b)

Figure 3. Experimental results. (a) Running time of enc and Dec protocol; (b) Running time of eval protocol.

decryption algorithm is constant complexity and the encryption algorithm is linearly dependent with the size of identity set. The result also indicates that our scheme is efficient since the running time of encrypting a message under 50 receivers set is also less than 1 second.

Then we demonstrate the evaluation protocol. As shown in Figure 3(b), the running time of evaluation protocol is related to the max size of two identity sets of ciphertexts. However, it is easy to learn from the result that the growth rate of the running time is very low. The running time of two identity sets up to 10 is less than 125 ms and it is less than 225 ms when identity sets up to 100. This result shows that the evaluation protocol is very efficient and has some complexity since heavy operations, *i.e.* bilinear pairing, do not increase with the size of receiver sets.

5. Conclusions

In this paper, we propose an identity-based homomorphic broadcast encryption scheme. In this IBHBE scheme, an external entity can transform two ciphertext into one new ciphertext without decrypting them, which can be decrypt by a receiver who belongs to the two receiver sets of the two ciphertexts. We also give formal proofs to prove that our scheme is correct and secure. The performance experiments show that our scheme is efficient for practical applications.

In our scheme, the evaluation on ciphertexts needs interactive between the executor and the receiver. Besides, our scheme is proved in random oracle model, which is an ideal model. Therefore, we leave an open problem here: how to construct a non-interactive IBHBE scheme in standard model?

Acknowledgements

We thank for editors and reviewers' valuable comments.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Fiat, A. and Naor, M. (1993) Broadcast Encryption. *Proceedings of the* 13*th Annual International Cryptology Conference*, Santa Barbara, 22-26 August 1993, 48-491.

[2] Delerablée, C., Paillier, P. and Pointcheval, D. (2007) Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys. *Proceedings of the First International Conference of Pairing-Based Cryptography*, Tokyo, 2-4 July 2007, 39-59.

[3] Jiang, L.M. and Guo, D.H. (2017) Dynamic Encrypted Data Sharing Scheme Based on Conditional Proxy Broadcast Re-Encryption for Cloud Storage. *IEEE Access*, **5**, 13336-13345. https://doi.org/10.1109/ACCESS.2017.2726584

[4] Xu, P., Jiao, T.F., Wu, Q.H., Wang, W. and Jin, H. (2016) Conditional Identity-Based Broadcast Proxy Re-Encryption and Its Application to Cloud Email. *IEEE Transactions on Computers*, **65**, 66-79. https://doi.org/10.1109/TC.2015.2417544

[5] Baek, J., Safavi-Naini, R. and Susilo, W. (2005) Efficient Multi-Receiver Identity-Based Encryption and Its Application to Broadcast Encryption. *Proceedings of the* 8*th International Workshop on Theory and Practice in Public Key Cryptography*, Les Diablerets, 23-26 January 2005, 380-397.

[6] Delerablée, C. (2007) Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys. *Proceedings of the* 13*th International Conference on the Theory and Application of Cryptology and Information Security*, Kuching, 2-6 December 2007, 200-215.

[7] Gentry, C. and Waters, B. (2009) Adaptive Security in Broadcast Encryption Systems (with Short Ciphertexts). *Proceedings of the* 28*th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Cologne, 26-30 April 2009, 171-188.

[8] He, K., Weng, J., Liu, J.-N., Liu, J.K., Liu, W. and Deng, R.H. (2016) Anonymous Identity-Based Broadcast Encryption with Chosen-Ciphertext Security. *Proceedings of the* 11*th ACM on Asia Conference on Computer and Communications Security*, Xi'an, 30 May-3 June 2016, 247-255.

[9] Boneh, D. and Franklin, M.K. (2001) Identity-Based Encryption from the Weil Pairing. *Proceedings of the* 21*st Annual International Cryptology Conference*, Santa Barbara, 19-23 August 2001, 213-229. https://doi.org/10.1007/3-540-44647-8_13

[10] Caro, A.D. and Iovino, V. (2011) jPBC: Java Pairing Based Cryptography. *Proceedings of the* 16*th IEEE Symposium on Computers and Communications*, Kerkyra, 28 June-1 July 2011, 850-855.