Augmented Broadcaster Identity-based Broadcast Encryption

Jianhong Zhang, Yuwei Xu, Zhipeng Chen
Institution of Image Processing and Pattern Recognition
North China University of Technology
Beijing, China 100144
ywxupaper@163.com

Journal of Digital Information Management

ABSTRACT: *Identity-based Broadcast Encryption (IBBE) has the inherent key escrow problem that Private Key Generator (PKG) can fully determine the user's private key, which is an obstacle of the application of IBBE. The existing approaches to solving key escrow problem need the user to submit identity to multiple PKGs or interactions between PKG and the user in the private key extraction phase. For Point-to-Multipoint Identity-based Broadcast Encryption (P2MIBBE) that the computing capabilities of receiver are limited, these approaches are impracticable. We propose a new approach what we call Augmented Broadcaster Identity-based Broadcast Encryption (AB-IBBE). It requires neither multiple PKGs nor calculation of receiver in the private key extraction phase. We construct a universal scheme to realize AB-IBBE, such that any IND-ID-CPA secure IBBE scheme can be extended to an IND-ID-CPA secure AB-IBBE scheme.*

Categories and Subject Descriptors:
E.3 [**DATA ENCRYPTION];** Data Encryption Standard*:* C.2.1 **[Network Architecture and Design**] Wireless Communication D.4.6 **[Security and Protection**] Cryptographic Controls

General Terms: Broadcasting, Encryption

Keywords: Key Escrow, Identity-based Broadcast Encryption

Received: 4 February 2013, Revised 22 March 2013, Accepted 27 March 2013

1. Introduction

Broadcast Encryption (BE) is a cryptographic systems, when a broadcaster sends messages through broadcast channel, enables the broadcaster to encrypt messages for a set of authorized receivers, and only authorized receivers can recover plaintexts.

Broadcast encryption can be divided into two kinds of com-munication modes, depending on the difference of computing power between the broadcaster and the receiver. One is Multipoint-to-Multipoint Broadcast Encryption (M2MBE), in which the broadcaster and the receiver have similar calculation abilities. The other is Point-to-Multipoint Broadcast Encryption (P2MBE), such as satellite broadcasts, cable TV subscriptions, digital rights management systems, etc. In P2MBE, the computing power of the broadcaster and the receiver are unbalanced. The broadcaster has powerful computing resources; however, the computing capabilities of the receiver are limited.

Identity-based Broadcast Encryption (IBBE) is the combination of BE and Identity-based Encryption (IBE). The receiver's public key in an IBBE scheme can be arbitrary string (E-mail address, mobile number, etc.). It makes that IBBE do not need complex certificate management like traditional Public Key Infrastructure (PKI). As in IBE, IBBE has the inherent key escrow problem that Private Key Generator (PKG) can fully determine the user's private keys. The user must completely trust PKG, whereas PKG could engage in malicious activities including indeed decrypt any ciphertext for any user and re-distribute user's private keys for any identity, which slows down the application of IBBE.

To overcome key escrow problem of IBBE, a natural way is to adopt the corresponding approaches of IBE. Up to now, four approaches can be used to mitigate key escrow

problem in IBE.

One approach is Distributed PKG strategy. Using techniques of threshold cryptography, the master key is distributed among multiple PKGs. Nevertheless, this approach increases infrastructure spending and communication overhead. The second approach is Self-certified Cryptography (SCC). In SCC, each user's public key is derived from the signature of the user's secret key with identity, and signed by authority's secret key. The user needs to choose a secret key and use it to sign. The third approach is Certificateless Public Key Cryptography (CL-PKC). In CL-PKC, the user's private keys consist of two parts, which are generated by PKG and the user independently. And the user must generate and publish the partial public key which corresponds to the partial private key. The fourth approach is Accountable Authority Identity-based Encryption (A-IBE). In the private key generation phase of an A-IBE scheme, the user must select a random number, give to PKG a proof of knowledge of random number, and compute its private key.

If using Distributed PKG strategy, the user has to submit identity to multiple PKGs, which is a heavy burden in practice. Apparently, SCC and CL-PKC are not pure Identity-based En-cryption, which are cryptographic systems between traditional public cryptographic system and Identity-based Encryption. What's more, in SCC, CL-PKC and A-IBE, private key of the user is produced by interaction between PKG and user. The interaction not only increases communication overhead, but also brings the user's calculation.

However, in Point-to-Multipoint Identity-based Broadcast Encryption (P2MIBBE), the computing capability of the receiver is limited. Hence, for receivers of P2MIBBE, the above four approaches are impracticable. In this paper, we propose a practical approach to solving key escrow problem of P2MIBBE.

1.1 Related Work

Broadcast Encryption (BE) was introduced by Fiat and Naor [1]. Several graceful BE schemes [2-6] have been introduced. Identity-based Broadcast Encryption (IBBE) was introduced by Delerablée [7] in 2007. Delerablée's scheme achieves IND-sID-CPA security, and the ciphertext length and private key size are constant. Recently, IBBE attracts more and more attention [8-10]. The evaluation standard of an IBBE scheme includes four important parameters, key size, ciphertext length, the user's calculation and security.

Distributed PKG strategy was introduced by Boneh and Franklin [11]. Self-certified Cryptography (SCC) was introduced by Girault [12]. Al-Riyami and Paterson [13] introduced Certificateless Public Key Cryptography (CL-PKC). Subsequently, several CL-PKC schemes [14-16] have been proposed. In 2007, Goyal [17] formalized the notion of Accountable Authority Identity-based Encryption (A-IBE) and present two schemes. In the private key generation phase, the interaction betweens the user and PKG is executed by using Zero-knowledge Proof of Knowledge of Discrete Log in the first scheme, and 1-out-2 Oblivious Transfer in the second scheme. In 2009, Libert and Vergnaud [18] improved Goyal's first proposal. In 2010, Xu et al. [19] improved Goyal's second scheme through 1-out-n Oblivious Transfer.

In 2008, Guo and Zhang [20] introduced an accountable authority IBBE scheme, which was a combination of Goyal's [17] first scheme and Delerablée's [7] IBBE scheme. In 2009, Libert and Vergnaud [18] used their improvement of Goyal's first proposal to reform Boneh and Hamburg's IBBE scheme. In 2012, Zhao and Zhang [21] introduced an IBBE scheme that can reduce trust of PKG, which still needs interaction between PKG and the receiver. The interaction is executed by Zero-knowledge Proof and blind-signing method. These schemes are not suitable for P2MIBBE, because the limited compute capacity of the receiver.

1.2 Our Contributions

We propose a new approach to solving key escrow problem for Point-to-Multipoint Identity-based Broadcast Encryption (P2MIBBE), what we call Augmented Broadcaster Identity-based Broadcast Encryption (AB-IBBE). In consideration of unbalanced computing power between the broadcaster and the receiver in P2MIBBE. We enhance the broadcaster's functions. Let the receiver's private key consist of two parts, one part is produced by PKG and the other part is produced by the broadcaster. Compared with the existing approaches, our approach can make it require neither submitting identity to multiple PKGs nor interactions between PKG and the receiver, and the receiver does not need any calculating operation in the private key extraction phase. In the practical engineering application, compared with security, traceability is often trivial. Hence, we do not discuss traceability in this paper.

We formalize the definition of Augmented Broadcaster Identity-based Broadcast Encryption (AB-IBBE), which includes a registration process when a receiver wants to obtain a broadcaster's service. We present the security notions for AB-IBBE. The security game consists of the DishonestPKG game and the IND-ID-CPA game.

We construct a universal scheme for realizing AB-IBBE, such that any IND-ID-CPA secure IBBE scheme can be extended to an IND-ID-CPA secure AB-IBBE scheme. The construction of our universal scheme is based on Dual System Encryption [22], which is a new methodology for proving security of encryption systems. In this paper, we use a new technique of realizing dual system encryption that was introduced by Lewko and Waters [23], where complexity assumptions are three static hardness assumptions (i.e. they do not depend on the number of queries made by an attacker).

2. Preliminaries

2.1 Composite Order Bilinear Groups

Boneh et al. [24] first introduced composite order bilinear groups. Subsequently, [23] used them. Here, we only briefly review the definition and necessary properties.

Take the input as a security parameter λ, group generator $\mathcal{G}$ outputs a description of bilinear group system $\mathbb{G} = (N = p_1 p_2 p_3, G, G_T, e(-,-))$ where $p_1 p_2 p_3$ are three distinct primes, G and G_T are cyclic groups with $|G| = |G_T| = N$. $e: G \times G \rightarrow G_T$ is a bilinear map such that:

1. (Bilinearity) For arbitrary $g, h \in G, a, b \in Z_N$, then $e(g^a, h^b) = e(g, h)^{ab}$.

2. (Non-degeneracy) $\exists\, g \in G$ such that $|e(g, g)| = N$.

3. (Computability) There is a polynomial time algorithm to compute group operation in G, G_T, and map e.

Let G_{p_i} denote the subgroups of G, where $|G_{p_i}| = p_i$, $i = 1, 2, 3$. Let g denote a generator of G. Then, $g^{p_1 p_2}$, $g^{p_1 p_3}$ and $g^{p_2 p_3}$ are generators of G_{p_3}, G_{p_2} and G_{p_1} respectively. $\forall h_1 \in G_{p_1} \forall h_2 \in G_{p_2} \exists G_{p_i}, h_j \in G_{p_j}, \exists \alpha_1, \alpha_2$ such that $e(h_1, h_2) = e(g^{p_1 p_3 \alpha_3}, g^{p_2 p_3 \alpha_4}) = (g^{\alpha_3}, g^{p_3 \alpha_2})^{p_1 p_2 p_3} = 1$. Then for $h_i \in G_{p_i}$ and $h_j \in G_{p_j}$ with $(i \neq j)$, $e(h_i, h_j)$ is an identity element in G_T. That is to say, G_{p_1}, G_{p_2}, G_{p_3} have orthogonality property.

2.2 Three Static Hardness Assumption

These static hardness assumptions were used and proved in [23]. They are static means that they do not depend on the number of queries made by an attacker.

Assumption 1 (Subgroup decision problem for 3 primes) Given bilinear map system $\mathbb{G} = (N = p_1 p_2 p_3, G, G_T, e(.,.))$. Randomly select $g \in G_{p_1}, X_3 \in G_{p_3}, T_1 \in G_{p_1 p_2}, T_2 \in G_{p_1}$, and set $D = (\mathbb{G}, g, X_3)$. It is hard to distinguish T_1 from T_2.

The advantage of algorithm B in breaking Assumption 1 is defined as $Adv_1 = |Pr[B(D, T_1) = 1] - B(D, T_2) = 1|$.

Definition 1 Assumption 1 holds if Adv_1 is negligible in polynomial time.

Assumption 2 Given a bilinear map system $\mathbb{G} = (N = p_1 p_2 p_3, G, G_T, e(.,.))$. Randomly select $g, X_1 \in G_{p_1}, X_2 Y_2 \in G_{p_2}, X_3 Y_3 \in G_{p_3}, T_1 \in G, T_1 \in G_{p_1 p_3}$ and set $D = (\mathbb{G}, g, X_1 X_2, X_3, Y_2 Y_3)$. It is hard to distinguish T_1 from T_2.

The advantage of algorithm B in breaking *Assumption 2* is defined as $Adv_2 = |Pr[B(D, T_1) = 1] - B(D, T_2) = 1|$.

Definition 2 Assumption 2 holds if Adv_2 is negligible in polynomial time.

Assumption 3 Given a bilinear map system $\mathbb{G} = (N = p_1 p_2 p_3, G, G_T, e(-,-))$. Randomly select $\alpha, s \in Z_N, g \in G_p, X_2, Y_2, Z_2 \in G_{p_2}, X_3 \in G_{p_3}, T_1 = e(g, g)^{\alpha s}, T_2 \in G_T$, and set $D = (\mathbb{G}, g, g^{\alpha} X_2, X_3, g^s Y_2, Z_2)$. It remains hard to distinguish T_1 from T_2.

The advantage of algorithm B in breaking Assumption 3 is defined as $Adv_3 = |Pr[B(D, T_1) = 1] - B(D, T_2) = 1|$.

Definition 3 Assumption 3 holds if Adv_3 is negligible in polynomial time.

2.3 The Definition of AB-IBBE

An Augmented Broadcaster Identity-based Broadcast Encryption (AB-IBBE) scheme consists of four components.

Setup This is a probabilistic algorithm. Take the input as the security parameter λ and m the maximal size of the authorized receivers' set. It outputs a master secret key MSK-P and a public key PK-P.

Extract This algorithm is a probabilistic algorithm consists of two sub-algorithms that are executed by PKG and a broadcaster respectively.

Extract-P Takes as input the master secret key MSK-P, and a receiver's identity $ID_i \in S$. It outputs the receiver's partial key $sk_{ID_i} - P$.

Extract-B The receiver with identity ID_i registers to a broadcaster. The broadcaster outputs the receiver's partial private key $sk_{ID_i} - B$.

In the end, the receiver obtains integrated private key

$$sk_{ID_i} = \{sk_{ID_i} - P, sk_{ID_i} - B\}$$

Note that the broadcaster may not publish the partial public key which corresponds to the partial private key $sk_{ID_i} - B$.

Encrypt This is a probabilistic algorithm consist of two steps.

1. Takes as input the public key PK-P, and an authorized receivers' set $S = \{ID_1, ID_2, ..., ID_s\}$, where $s \leq m$, it outputs $(\overline{Hdr}, K)$.

2. Takes as input authorized receivers' set S and $(\overline{Hdr}, K)$, it outputs (Hdr, K), where Hdr is an encryption of $\overline{Hdr}$.

Then, K is used to be encryption key of a symmetric encryption algorithm.

Decrypt This is a deterministic algorithm consist of two steps.

1. Takes as input $sk_{ID_i} - B$, authorized receivers' set S and Hdr, it outputs $\overline{Hdr}$ if $ID_i \in S$.

2. Takes as input PK-P, $sk_{ID_i} - B$, S, and $\overline{Hdr}$, it outputs K.

Then, K is used to recover ciphertexts.

2.4 The Security Notions for AB-IBBE

To define security for an Augmented Broadcaster Identity-based Broadcast Encryption (AB-IBBE) system, we first define the DishonestPKG game and the IND-ID-CPA game.

The DishonestPKG game

Setup The adversary runs Setup algorithm to obtain MSK-P, PK-P, and sends PK-P to the challenger.

Query phase 1 The adversary adaptively issues queries $q_1, q_2, ..., q_t$. In each query q_i, the adversary selects receivers' set S adaptively, where $|S| \le m$, and $ID_i \in S$. The challenger runs in Extract-B algorithm, and sends $sk_{ID_i} - B$ to the adversary.

Challenge When the adversary decides that phase 1 is over, it chooses two messages Hdr_0, Hdr_1 and a challenger identity set S^*, where $|S^*| \le m$, and has no revealed identity in query phase 1. The challenger chooses random $\eta \in \{0, 1\}$, runs the first step of Encrypt algorithm to obtain Hdr^*, and sends Hdr^* to A.

Query phase 2 The adversary adaptively issues queries $q_{t+1}, q_{t+1}, ..., q_\pi$. These queries are the same as query phase 1 with constraint $ID_i \notin S$.

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

The advantage of the adversary A is defined as:

$$Adv_{DPKG}(t, \pi, m, A) = |Pr[\eta' = \eta] - \frac{1}{2}|$$

In the DishonestPKG game, PKG acts as an adversary that makes an effort to recover the key K. Owing to PKG, it can output the receiver's partial key $sk_{ID_i} - P$, so that PKG can decrypt $\overline{Hdr}$ optionally. To Limit PKG to recover K, we must limit PKG to obtain $\overline{Hdr}$.

The IND-ID-CPA game

Setup The challenger runs Setup algorithm to obtain MSK-P, PK, and sends PK to the adversary.

Query phase 1 The adversary adaptively issues queries $q_1, q_2, ..., q_t$. In each query q_i, the adversary selects users' set S adaptively, where $|S| \le m$, and $ID_i \in S$. The challenger runs Extract algorithm, and sends sk_{ID_i} to the adversary.

Challenge When the adversary decides that phase 1 is over, the challenger runs Encrypt algorithm to obtain (Hdr^*, K), and chooses random $b \in \{0,1\}$. Let $K_b = K$, and K_{1-b} is arbitrary element in keyspace. The challenger sends (Hdr^*, K_0, K_1) to the adversary.

Query phase 2 The adversary adaptively issues queries $q_{t+1}, q_{t+1}, ..., q_\pi$. These queries are the same as query phase 1 with constraint $ID_i \notin S$.

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

The advantage of the adversary A is defined as:

$$Adv_{IIC}(t, \pi, m, A) = |Pr[\eta' = \eta] - \frac{1}{2}|$$

Definition 4 An Augmented Broadcaster Identity-based Broadcast Encryption (AB-IBBE) scheme is IND-ID-CPA secure if both $Adv_{DPKG}(t, \pi, m, A)$ and $Adv_{IIC}(t, \pi, m, A)$ are negligible in polynomial time.

3.Our Universal AB-IBBE Scheme

3.1 Our Construction

In this section, we give a universal construction for realizing Augmented Broadcaster Identity-based Broadcast Encryption (AB-IBBE). Using our universal AB-IBBE scheme, any IND-ID-CPA secure IBBE scheme can be converted into an AB-IBBE scheme. Let I be an IND-ID-CPA secure IBBE scheme. The symbol with suffix I stand for the content of I, such as MSK-I stands for the master secret key of I.

Setup It is the same as the Setup algorithm of I. In the end, it outputs a master secret key $MSK - P = MSK - I$ and a public key $PK - P = PK - I$.

Extract This algorithm is a probabilistic algorithm consists of two sub-algorithms that are executed by PKG and a broadcaster respectively.

Extract-P It is the same as the Extract algorithm of I. It outputs the receiver's partial key $sk_{ID_i} - P = sk_{ID_i} - I$.

Extract-P A receiver with identity ID_i registers to a broadcaster. Let $S = \{ID_1, ID_2, ..., ID_s\}$, where $s \le m$. S is the set of the registered receivers' identities, and $ID_i \in S$. The broadcaster constructs one bilinear map system $\mathbb{G} = (N = p_1 p_2 p_3, G, G_T, e(.,.))$, where p_1, p_2, p_3 are three distinct primes. Let G_{p_i} denote the subgroup of G, where $|G_{p_i}| = p_i$ and $i = 1, 2, 3$. Randomly chooses $g, h, u_1, ..., u_m \in G_{p_1}$, $\alpha \in Z_N$, $r_i \in Z_N$, and $R_i, R_i' \in G_{p_3}$. It outputs

$$sk_{ID} - B = \{d_{i,0}, d_{i,1}, d_{i,2}\} = \{e(.,.), g^{r_i} R_i, g^{\alpha} (h \prod_{j=1}^{s} u_j^{ID_j})^{r_i} R_i'\}$$

In the end, the receiver obtains integrated private key

$$sk_{ID_i} = \{sk_{ID_i} - P, sk_{ID_i} - B\}$$

Encrypt This is a probabilistic algorithm consist of two steps.

1. It is the same as the Encrypt algorithm of I. It outputs $(\overline{Hdr}, K) = (Hdr - I, K - I)$.

2. Takes as input authorized receivers' set S and $(\overline{Hdr}, K)$, it outputs (Hdr, K), where

$$Hdr = (C_0, C_1, C_2) = (e(g, g)^{\alpha s}\overline{Hdr}, (h\prod_{j=1}^{s} u_j^{ID_j})^k, g^k)$$

Then, K is used to be encryption key of a symmetric encryption algorithm.

Decrypt This is a deterministic algorithm consist of two steps.

1. Takes as input $sk_{ID_i} - B$, authorized receivers' set S and Hdr, it computes. $\overline{Hdr} = \dfrac{e(d_{i,1}, C_1)C_0}{e(d_{i,2}, C_2)}$

2. It is the same as the Decrypt algorithm of I, and outputs K.

Then, K is used to recover ciphertexts.

Efficiency In our construction, the size of $sk_{ID_i} - B$ is $O(1)$. Compared with $\overline{Hdr}$, Hdr only increases two group elements. In addition, the broadcaster does not need publish the partial public key which corresponds to the partial private key $sk_{ID_i} - B$.

3.2 Correctness Analysis

Due to the orthogonality property of group G_{p_1} and G_{p_2}, such that $e(R_i, (h\prod_{j=1}^{s} u_j^{ID_j})^k = 1, e(R_i', g^k) = 1$. Hence,

$$\frac{e(d_{i,1}, C_1)C_0}{e(d_{i,2}, C_2)} = \frac{e\left(g^{r_i} R_i, \left(h\prod_{j=1}^{s} u_j^{ID_j}\right)^k\right) e(g, g)^{\alpha k}\overline{Hdr}}{e\left(g^{\alpha}\left(h\prod_{j=1}^{s} u_j^{ID_j}\right)^{r_i} R_i', g^k\right)}$$

$$= \frac{e\left(g^{r_i}, \left(h\prod_{j=1}^{s} u_j^{ID_j}\right)^k\right) e\left(R_i, \left(h\prod_{j=1}^{s} u_j^{ID_j}\right)^k\right) e(g, g)^{\alpha k}\overline{Hdr}}{e(g^{\alpha}, g^k) e\left(\left(h\prod_{j=1}^{s} u_j^{ID_j}\right)^{r_i}, g^k\right) e(R_i', g^k)}$$

$$= \frac{e(g, g)^{\alpha k}\overline{Hdr}}{e(g^{\alpha}, g^k)} = \overline{Hdr}$$

3.3 Security Analysis

Security analysis consists of three theorems. The proof of Theorem 1 is based on dual system encryption and through three lemmas.

In dual system encryption [21, 22], the reduction is through a sequence of games. These games are progressively liberalized limits, in the end, reduced to impossible. Both private keys and ciphertexts have two types, which are normal and semi-functional. Semi-functional private keys and semi-functional ciphertexts are only used in proof. Normal secret keys can decrypt normal and semi-functional ciphertexts. Semi-functional secret keys can decrypt normal ciphertexts. However, semi-functional secret keys can not decrypt semi-functional ciphertexts.

First choose a generator g_2 of G_{p_2}, and define semi-functional keys and semi-functional ciphertexts in the following manner.

Semi-functional keys Choose random $\beta_i, \beta_i' \in Z_N$ for ID_i. Transform normal key $sk_{ID_i} - B = \{d_{i,0}, d_{i,1}, d_{i,2}\}$ into semi-functional key $sk_{ID_i} - B = \{d_{i,0}', d_{i,1}', d_{i,2}'\} = \{d_{i,0}, d_{i,1} g_2^{\beta_i}, d_{i,2} g_2^{\beta_i \beta_i'}\}$.

Semi-functional ciphertexts Choose random $\gamma_i, \gamma_i' \in Z_N$ for ID_i. Transform normal ciphertext $Hdr = (C_0, C_1, C_2)$ into semi-functional ciphertext $Hdr' = (C_0', C_1', C_2') = (C_0, C_1 g_2^{\gamma_i \gamma_i'}, C_2 g_2^{\gamma_i})$.

The proof of the security will use a sequence of games. Let π denotes the number of key queries, and $0 \le k \le \pi$. We define these games as:

$Game_{Real}$: The real IND-ID-CPA secure DishonestPKG game.

$Game_k$: The game is the same as $Game_{Real}$ except that: (1) the challenge ciphertext is semi-functional. (2) The first k keys are semi-functional, and the rest of keys are normal. In $Game_0$, the challenge ciphertext is semi-functional, and all keys are normal. Both the challenge ciphertext and keys of $Game_{\pi}$ are semi-functional.

$Game_{final}$: The game is the same as $Game_{\pi}$ except that the challenge ciphertext is a semi-functional encryption on a random element of G_T.

Lemma 1 Suppose there exists an algorithm A such that $Adv_{Game\ Real} - Adv_{Game\ 0} = \varepsilon$. Then there exists an algorithm B with advantage ε in breaking Assumption 1.

Proof B first receives $g \in G_{p_1}, X_3 \in G_{p_3}$, and T.

Setup It selects $\alpha, a_1, ..., a_m, b \in Z_N$ randomly, and sets $PK = (g, h = g^b, u_1 = g^{a_1}, ..., u_m = g^{a_m}, v = e(g, g)^{\alpha})$.

Query phase 1 A adaptively issues queries $q_1, q_2, ..., q_t$. In each query q_i, A adaptively selects users' set S, where $|S| \le m$, $ID_i \in S$ and makes a key query for ID_i. B selects $r_i, t_i, w_i \in Z_N$ randomly, sets

$$sk_{ID}' - B = \{d_{i,0}', d_{i,1}', d_{i,2}'\} = (e(.,.), g^{r_i} X_3^{t_i}, g^{\alpha} (h\prod_{j=1}^{|S|} u_j^{ID_j})^{r_i} X_3^{w_i})$$

Challenge A chooses two messages Hdr_0, Hdr_1, and a challenger identity set S^* with no revealed identity in query phase 1, where $|S^*| \le m$. B chooses random $\eta \in \{0, 1\}$, and sets

$$Hdr^* = \{C_0', C_1', C_2'\} = Hdr_\eta e(T, g)^\alpha, T^{\sum_{j=1}^{|S^*|} a_j ID_j^* + b}, T)$$

Query phase 2 A adaptively issues queries $q_{t+1}, q_{t+2}, ..., q_\pi$. These queries are the same as query phase 1 with constraint $ID_i \notin S^*$.

Guess A outputs a guess $\eta' \in \{0, 1\}$,and wins the game if $\eta' = \eta$. If $T \in G_{p_1}$, Hdr^* is a normal ciphertext, and if $T \in G_{p_1 p_2}$, Hdr^* is a semi-functional ciphertext. Therefore, B canuse the outputs of A to distinguish T_1 from T_2 with advantage ε.

Lemma 2 Suppose there exists an algorithm A such that $Adv_{Game_{k-1}} - Adv_{Game_k} = \varepsilon$, where $1 \le k \le \pi$. Then there exists an algorithm B with advantage ε in breaking *Assumption* 2.

Proof B first receives $g, X_1X_2, X_3, Y_2Y_3, T$, where $g, X_1 \in G_p$, $X_2, Y_2 \in G_p, X_3, Y_3 \in G_p$. It works as follows:

Setup It selects $\alpha, a1,...,a_m, b \in Z_N$ randomly, and sets $PK = (g, h = g^b, u_1 = g^{a_1}, ..., u_m = g^{a_m}, v = e(g, g)^\alpha)$.

Query phase 1 A adaptively issues queries $q_1, q_2, ..., q_t$. In each query q_i, A adaptively selects users' set S, where $|S| \le m$, $ID_i \in S$ and makes a key query for ID_i. A selects random $r_i, t_i, w_i \in Z_N$.

1) For $i < k$, B sets

$$sk'_{ID} - B = \{d'_{i,0}, d'_{i,1}, d'_{i,2}\} = (e(.,.), g^{r_i}(Y_2Y_3)^{t_i}, g^\alpha (h\prod_{j=1}^{|S|} u_j^{ID_i})^{r_j} (Y_2Y_3)^{w_i})$$

2) For $i = k$, B sets

$$sk'_{ID} - B = \{d'_{i,0}, d'_{i,1}, d'_{i,2}\} = (e(.,.), T, g^\alpha T^{\sum_{j=1}^{|S^*|} a_j ID_j^* + b} X_3^{w_i})$$

3) For $i > k$, B sets

$$sk'_{ID} - B = \{d'_{i,0}, d'_{i,1}, d'_{i,2}\} = (e(.,.), g^{r_i} X_3^{t_i}, g^\alpha (h\prod_{j=1}^{|S|} u_j^{ID_j})^{r_i} X_3^{w_i})$$

Challenge A chooses two messages Hdr_0, Hdr_1, and a challenger identity set S^* with no revealed identity in query phase 1, where $|S^*| \le m$. B chooses $\eta \in \{0, 1\}$ randomly, and sets

$$Hdr^* = \{C_0', C_1', C_2'\} = Hdr_\eta e(X_1, X_2, g)^\alpha, (X_1, X_2)^{\sum_{j=1}^{|S^*|} a_j ID_j^* + b}, X_1, X_2)$$

Query phase 2 A adaptively issues queries $q_{t+1}, q_{t+2}, ..., q_\pi$. These queries are the same as query phase 1 with constraint $ID_i \notin S^*$.

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

If $T \in G_{p_1 p_2}$, the above procedure is $Game_{k-1}$, and if $T \in G$, the above procedure is $Game_k$. Therefore, B can use the outputs of A to distinguish T_1 from T_2 with advantage ε.

Lemma 3 Suppose there exists an algorithm A such that $Adv_{Game_\pi} - Adv_{Game_{final}} = \varepsilon$. Then there exists an algorithm B with advantage ε in breaking *Assumption* 3.

Proof B first receives $g, g^\alpha X_2, X_3, g^s Y_2, X_3, Z_2, T$, where $g \in G_{p_1}, X_2, Y_2, Z_2 \in G_{p_2}, X_3 \in G_{p_3}, a, s \in Z_N$.

Setup It selects $a_1,...,a_m, b \in Z_N$ randomly, and sets $PK = (g, h = g^b, u_1 = g^{a_1}, ..., u_m = g^{a_m}, v = e(g X_2, g)^\alpha)$.

Query phase 1 A adaptively issues queries $q_1, q_2, ..., q_t$. In each query q_i, A adaptively selects users' set S, where $|S| \le m$, $ID_i \in S$ and makes a key query for ID_i. B selects $c_i, r_i, t_i, w_i \in Z_N$ randomly, and sets

$$sk'_{ID} - B = \{d'_{i,0}, d'_{i,1}, d'_{i,2}\} = (e(.,.), g^{r_i} Z_2^{z_i} X_3^{t_i}, g^\alpha X_2 (h\prod_{j=1}^{|S|} u_j^{ID_j})^{r_i} Z_2^{c_i} Y_3^{w_i})$$

$Game_{k-1}$

Challenge A chooses two messages Hdr_0, Hdr_1, and a challenger identity set S^* with no revealed identity in query phase 1, where $|S^*| \le m$. B chooses $\eta \in \{0, 1\}$randomly, and sets

$$Hdr^* = \{C_0', C_1', C_2'\} = M_\eta T(g^s Y_2)^{\sum_{j=1}^{|S^*|} a_j ID_j^* + b}, g^s Y_2)$$

Query phase 2 A adaptively issues queries $q_{t+1}, q_{t+2}, ..., q_\pi$. These queries are same as query phase 1 with constraint $ID_i \notin S^*$.

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

If $T = e(g, g)^{\alpha s}$, then Hdr^* is a semi-functional ciphertext of Hdr_η. If T is a random element of G_T, then Hdr^* is a semi-functional ciphertext of random message. Therefore, B can use the outputs of A to distinguish T_1 from T_2 with advantage ε.

Theorem 1 If Assumption 1, 2 and 3 are right, then $Adv_{DPKG}(t, \pi, m, A)$ is negligible in polynomial time.

Proof: According to Lemma 1-3, if assumption 1, 2 and 3

hold, then $Game_{Real}$ and $Game_{final}$ are indistinguishable. The adversary's advantage in $Game_{Real}$ is negligible. Hence, $Adv_{DPKG}(t, \pi, m, A)$ is negligible in polynomial time.

Theorem 2 If I is IND-ID-CPA secure, then $Adv(t, \pi, m, A)$ is negligible in polynomial time.

Proof: We use proof by contradiction to prove this theorem. Suppose there exists polynomial time algorithm A which can win the IND-ID-CPA game for AB-IBBE with advantage ε. Then we can use A to construct a polynomial time algorithm B with advantage ε, such that B can win the IND-ID-CPA game for I. This contradicts that I is IND-ID-CPA secure. Therefore, $Adv(t, \pi, m, A)$ is negligible in polynomial time.

Theorem 3 Our Augmented Broadcaster Identity-based Broadcast Encryption (AB-IBBE) scheme is IND-ID-CPA secure.

Proof According to Theorem 1, Theorem 2 and Definition 4, Theorem 3 is obvious.

4. Conclusions

In order to solve *key escrow* problem for Point-to-Multipoint Identity-based Broadcast Encryption (P2MIBBE), we propose Augmented Broadcaster Identity-based Broadcast Encryption (AB-IBBE) and construct a universal scheme for realizing AB-IBBE. In the private key extraction phase, it requires neither submitting identity to multiple PKGs nor interaction between PKG and the receiver, and the receiver does not need any calculating operation. Designing a scheme that the receiver can join and leave dynamically or achieves IND-ID-CCA security is an open problem.

5. Acknowledgements

This work was supported by Beijing Natural Science Foundation (No: 4122024), and the Nova Programma (No: 2007B-001).

References

[1] Fiat, A., Naor, M. (1994). Broadcast Encryption. *In*: Proceedings of Advances in Cryptology- Crypto' 93, LNCS, 773, p. 480-491. Berlin: Springer-Verlag.

[2] Naor, D., Naor, M., Lotspiech, J. (2001). Revocation and Tracing Schemes for Stateless Receivers. *In*: Proceedings of Crypto' 01, LNCS, p. 41-62. Berlin: Springer-Verlag.

[3] Dani, H., Adi, S. (2002). The lsd broadcast encryption scheme. *In*: Proceedings of Advances in Cryptology-Crypto' 02, LNCS, 2442, p. 47-60. Berlin: Springer-Verlag.

[4] Goodrich, M. T., Sun, J. Z., Tamassia, R. (2004). Efficient tree-based revocation in groups of low-state devices. *In*: Proceedings of Advances in Cryptology-Crypto' 04, LNCS, 3152, p. 511-527. Berlin: Springer-Verlag.

[5] Boneh, D., Gentry, C., Waters, B. (2005). Collusion resistant broadcast encryption with short ciphertexts and private keys. *In*: Proceedings of Advances in Cryptology-CRYPTO' 05, LNCS, 3621, p. 258-275. Berlin: Springer-Verlag.

[6] Phan, D. H., Pointcheval, D., Shahandashti, S. F., Streer, M. (2005). Adaptive CCA Broadcast Encryption with Constant-Size Secret Keys and Ciphertexts. *In*: Proceedings of Advances in ACISP, LNCS, 7372, p. 308-321. Berlin: Springer-Verlag.

[7] Delerablée, C. (2007). Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys. *In*: Proceedings of Advances in Cryptology-ASIACRYPT'07, LNCS, 4833, p. 200-215. Berlin: Springer-Verlag.

[8] Boneh, D., Hamburg, M. (2008). Generalized Identity-based and Broadcast Encryption Schemes. *In*: Proceedings of Advances in Asiacrypt' 08, LNCS, 5350, p. 455-470. Berlin: Springer-Verlag.

[9] Gentry, C., Waters, B. (2009). Adaptive security in broadcast encryption systems. *In*: Proceedings of Advances in EURO-CRYPT' 09, LNCS, 5479, p. 171-188, Berlin: Springer-Verlag.

[10] Gentry, C., Waters, B. (2009). Adaptive Security in Broadcast Encryption Systems. *In*: Proceedings of Advances in Cryptology-Eurocrypt' 09, LNCS, 5479, p. 171-188. Berlin: Springer-Verlag.

[11] Boneh, D., Franklin, M. (2001). Identity-Based Encryption from the Weil Pairing. *In*: Proceedings of Advances in Cryptology-Crypto' 01, LNCS, 2139, p. 213-229. Berlin: Springer-Verlag.

[12] Girault, M. Self-certified public keys. *In*: *Proceedings of Advances in Cryptolog -Eurocrypt'* 91, LNCS, 547, p. 490-497. Berlin: Springer-Verlag.

[13] Al-riyami, S., Paterson, K. (2003). Certificateless Public Key Cryptosystems. *In*: *Proceedings of Advances in Cryptology-Asiacrypto,* LNCS, 2332, p. 452-471. Berlin: Springer-Verlag.

[14] Yum, D., Lee, P. (2004). Generic Construction of Certificateless Encryption. *In*: Computational Science and its Application-ICCSA, LNCS, 3043, p. 802-811.

[15] Libert, B., Quisquater, J. (2006). On Constructing Certigicateless Cryptosystems from Identity Based Encryption. *In*: Proceedings of the 9th international conference on Theory and Practice of Public-Key Cryptography, LNCS, 3958, p. 474-490. Berlin: Springer-Verlag.

[16] Liu, J., Au, M., Susilo, W. (2007). Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model. *In*: *ASIACCS,* p. 273-283.

[17] Goyal, V. (2007). Reducing Trust in the PKG in Identity-Based Cryptosystems. *In*: *Proceedings of Advances in Cryptology-Crypto,* LNCS, 4622, p. 430-447. Berlin: Springer-Verlag.

[18] Libert, B., Vergnaud, D. (2009). Towards black-box accountable authority IBE with short ciphertexts and private keys. *In*: *Proceedings of Advances in PKC'* 09*,* LNCS, 5443, p. 235-255. Berlin: Springer-Verlag.

[19] Xu, P., Cui, G. H., Fu, C., et al. (2010). A more efficient accountable authority IBE scheme under the DL assumption. Sci. china inf. Sci., 53:581-592.

[20] Guo, S., Zhang, C. (2008). Identity-based broadcast encryption scheme with untrusted pkg. *In*: *ICYCS,* p. 1613-1618. *IEEE Computer Society*.

[21] Zhao, X. W., Zhang, F. G. (2012). Fully CCA2 secure identity-based broadcast encryption with black-box accountable authority. T*he Journal of Systems and Software*, 85, 708-716.

[22] Waters, B. (2009). Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions. *In*: *Proceedings of Advances in Cryptology-Crypto'* 09*,* LNCS, 5677, p. 619-636. Berlin: Springer-Verlag. (The full paper appeared Cryptology ePrint Archive Report 2009/385)

[23] Lewko, A., Waters, B. (2010). New Techniques for Dual System Encryption and Fully Secure HIBE with Short Ciphertexts.*In*: *Proceedings of the* 7^{th} *Theory of Cryptography Conference,* LNCS, 5978, p. 455-479. Berlin: Springer-Verlag.

[24] Boneh, D., Goh, E., Nissim, K. Evaluating 2-DNF Formulas on Ciphertexts. *In*: *Theory of Cryptography,* LNCS, 3378, p. 328-342. Berlin: Springer-Verlag.