Cipher Text Policy Attribute Based Broadcast Encryption for Multi-Privileged Groups

Muthulakshmi Angamuthu[1], Akshaya Mani[2], and Anitha Ramalingam[3]
[1]Department of Mathematics, PSG College of Technology, India
[2]Department of Computer Science, Georgetown University, USA
[3]Department of Applied Mathematics and Computational Sciences, PSG College of Technology, India

Abstract: *In the current globalization scenario, many group communication applications have become vital and the users not only subscribe to a single resource, but they use multiple resources and hence ending up with multi-privileged groups. In some group communication applications, it is desirable to encrypt the contents without exact knowledge of the set of intended receivers. Attribute based encryption offers this ability and enforces access policies defined on attributes, within the encryption process. In these schemes, the encryption keys and/or cipher texts are labelled with sets of descriptive attributes defined for the system users, and a particular user private key can decrypt only if the two match. This paper presents a cipher text policy attribute based broadcast encryption scheme for multi-privileged group of users. The proposed scheme has been proved secure using random oracle model.*

Keywords: *Attribute based broadcast encryption, decisional bilinear diffie hellman problem and decisional diffie hellman problem, multi-privileged groups, cipher text policy.*

Received June 8, 2014; accepted March 15, 2015

1. Introduction

A traditional public-key cryptosystem provides confidentiality through public key encryption, and authenticity through digital signatures. In such a system, each of the participants maintain a pair of keys, in order to perform either of the two operations-encryption or signing. The notion of Identity-Based Encryption (IBE) was proposed as an economical alternative to public-key infrastructures. A generalization of IBE is Attribute Based encryption (ABE) which enables fine-grained access control towards confidential data instead of the traditional coarse-grained one and there by facilitate granting differential access rights to a set of users and allow flexibility in specifying the access rights of individual users.

In many distributed systems, a user should only be able to access data, on possession of certain set of attributes, which is achieved using ABE scheme. They are classified into two cases: Cipher-Policy Attribute Based Encryption (CP-ABE) and Key-Policy Attribute Based Encryption (KP-ABE). In CPABE, attributes will be assigned to a ciphertext (when creating the ciphertext) and policies will be assigned to users/keys by an authority (who creates the keys). A key can decrypt only those cipher texts whose attributes satisfy the policy.

The formal definition of an Attribute Based Broadcast Encryption (ABBE) scheme consists of the following three phases [9]:

- *Setup* $(k,l,B(u_i)_{1\le i\le l})$: with input, a security parameter k, the total number of users l, and the attribute repartition $B(u_i)$ for each user, returns an encryption key and decryption keys corresponding to each receiver.
- *Encrypt* (*ek; A*): Taking the encryption key ek and an access policy A as input, it returns a header and a session key SK from a finite set of encryption keys.
- *Decrypt* ($A; hdr; dk_i$): With a decryption key dk_i, a header and an access policy A as input, it returns the session key SK if and only if $B(u_i)$ satisfies A.

Otherwise, it outputs the symbol $\perp$ (*null*).

The rapid progress in the technologies underlying multicast networking has led to the development of many group oriented applications, such as pay-per-view, online teaching, teleconferencing and communal gaming. In these applications group members subscribe to different data streams and members have different access privileges. In multi-privileged groups, multiple data streams are to be broadcast to the users based on their privileges. A Data Group (DG) in a multi-privileged group consists of the users who can access a particular resource and a Service Group (SG) consists of users who are authorized to access exactly the same set of resources.

This paper, presents an ABBE scheme, which is based on Decisional Bilinear Diffie Hellman (DBDH) problem and Decisional Diffie Hellman (DDH) Problem.

2. Related Work

Attribute based encryption was first introduced by Sahai and Waters [17]. An IBE with fuzzy identity under attributes has been proposed in [3]. The first collusion-resistant ABE scheme which produces constant size cipher texts was presented in [6]. Sun *et al*. [18], have proposed a KPABBE by combining with Waters dual system encryption, ABE and BE system. An encryption scheme for multi-privileged group communications, combining a collusion-resistant BE and a KP-ABE system, was proposed in [20].

An access control mechanism using CPABE and user revocation capability has been discussed in [7]. A first Traceable CP-ABE system supporting any monotone access structures, was proposed in [10]. An ABBE scheme which associates a polynomial with every user based on the data streams he needs to access and a cipher text associated with another polynomial based on the attribute set was proposed in [11].

An ABE scheme that allows a user's private key to be expressed in terms of any access formula over attributes was provided in [15]. The first construction of a CP-ABE scheme having a security proof based on a number theoretic assumption was given in [5]. An ABBE scheme that attains information theoretical minimal storage overhead was provided in [26].

A CP-ABE scheme with access formula involving $\wedge$ and $\vee$ boolean operators, was provided in [8]. A scheme that allows an encryptor to use any AND gate as access policy on the ciphertext was provided in [4]. A lightweight ABE scheme based on ECC, a scheme with access policy in terms of LISS matrix over the attributes, a HABE model to achieve fine-grained access control in cloud computing, an ABE schemes with constant-size cipher texts were presented in [1, 2, 21, 25], respectively.

An integrated key graph for all members having different access privileges in hierarchical multi-group key management scheme was presented in [19]. A dynamic access control scheme for group communications, supporting multiple service groups with different access privileges was proposed in [12]. A group key management scheme called ID-based Hierarchical Key Graph Scheme (IDHKGS) for secure multi-privileged group communications employing a key graph was proposed by Wang *et al*. [22, 23]. Group key management for multi-privileged groups using batch rekeying and Non-split balancing higher order trees were discussed in [13, 14]. A key agreement scheme to enable secure group communications, using IBBE methodology is presented in [24]. This paper presents a CPABE scheme for multi-privileged group of users.

3. Definitions and Computational Assumptions

This section presents the definitions and computational assumptions needed for the proposed scheme.

- *Access policy*: An access control policy would be a policy that defines the kind of users who would have permissions to read the documents. For example, in an academic setting, the grade-sheets of a class may be accessible only to a professor handling the course and some teaching assistants of that course. The various credentials of the predicate are called attributes and the predicate itself which represents the access policy as the access structure.
- *Decisional diffie hellman assumption*: Let G be a multiplicative cyclic group of order p, with generator g. A probabilistic polynomial-time adversary has a negligible probability of distinguishing (g^a ,g^b ,g^{ab}), for random $a, b \in Z^*_p$ and (g^a, g^b, g^c), for random $a, b, c \in Z^*_p$.
- *Decisional diffie hellman problem*: distinguishing the two distributions ($X=g^a$,$Y=g^b$,$dh(X,Y)=g^{ab}$) and($X=g^a$,$Y=g^b$,$Z=g^c$) for random $X, Y, Z \in G$ is the DDH problem. The DDH assumption states that the DDH problem is hard.

4. Attribute based Broadcast Encryption for Multi-Privileged Groups

Consider a group of users with multiple privileges under different service groups $S\ G_j$, $1 \le j \le m$,, where m denotes the number of service groups. Let n_j denote the number of users in SG_j and ID_{ij}, $1 \le i \le n_j$, denotes the identity of the i^{th} user in the service group SG_j. Let G, G_T be two cyclic groups of prime order p and $\hat{e}$ is a bilinear pairing defined as $\hat{e}: GXG \to G_T$. Let H_1 be a cryptographic hash function defined as $H_1 : \{0,1\}^* \to G$ and P be the master public key. Let N =$\{a_1, a_2, a_3, ...a_t\}$be the set of attributes. We consider access structures that consist of AND gates only and whose inputs are literals. It is denoted as $\wedge_{a_i \in I} \tilde{a}_1$ where $I \subseteq$ N and every $\tilde{a}_1$ is a literal $(\tilde{a}_1 = a_i \ or \ not(a_i))$. The various phases of the proposed scheme are given below.

- *Setup*: The Key Distribution Center (KDC) runs Setup with security parameter k and the set of all attributes N as input and gives the public parameters as output tuple. The KDC chooses a cryptographic hash function $H_1 : \{0,1\}^* \to G$ and constructs the bilinear mapping $\hat{e}: GXG \to G_T$. The KDC selects a random integer pr from Z^*_p as the master secret key using which it computes the master public key P. It also generates the public parameters

$g^{h_i p}$ for positive attributes, $g^{h_i n}$ for negative attributes and $g^{h_i d}$ for don't care attributes. It outputs the tuple $< p, G, G_T, \hat{e}, P, H_1, \{g^{h_i p}\}_{1\le i\le t}, \{g^{h_i n}\}_{1\le i\le t}, \{g^{h_i d}\}_{1\le i\le t} >$ as the public parameter.

- *Extract*: The users authenticate themselves with their ID's and the KDC gets their corresponding secret key SK according to the set of attributes they possess. Extract takes as input the identity ID_{ij} of the user, the master private key pr, and the set S of attributes possessed by the users. The KDC computes the secret key $S_{ID_{ij}}$ corresponding to the identity ID_{ij} as $H_1 (ID_{ij})^{PY}$.

  The KDC computes the key for the attributes possessed by the user as below: For each of the attributes in N, the KDC chooses random $r_i \in Z_p^*$ and computes $\sum_{i=1}^{n} r_i = rpr$

  The KDC sets

$$Dj = \begin{cases} (g^{r_i + h_i p})^{pr^{-1}}, \text{if } a_i \in S \\ (g^{r_i + h_i n})^{pr^{-1}}, \text{if } a_i \in \mathrm{N} \setminus \mathrm{S} \end{cases}$$

  For all $a_i \in$ N, the KDC sets $F_i = (g^{r_i + h_i d})^{pr^{-1}}$. It also sets $\hat{D} = g^{-r}$ and gives the secret key $SK =< S_{ID_{ij}}, D_i, F_i, \hat{D} >$.

- *Encrypt*: the sender selects the sets of identities of the users S_1, S_2, S_3, …, S_m from the corresponding service groups to whom the messages M_1, M_2, $M_3, \ldots M_m$ respectively has to be broadcast. The sender also defines a policies W_1, W_2, $W_3, \ldots W_m$ for the corresponding service groups, from the set of attributes. The sender runs encrypt to get the cipher text C_j generated from the message M_j for each service group SG_j using the corresponding session key SK_j and T_j generated from policy. K_{ij} is computed for each selected user in S_j using bilinear pairing with Y_1 where Y_1 is computed as g^{y_1}, with a random $y_1 \in Z_p^*$. The lcm of all K_{ij}'s is computed as Lcm_j for the set S_j. The system of congruences, $X \equiv SK_j \pmod{Lcm_j}$ where SK_j= $e(g,g)^{skj}$, $sk_j \in_R Z_p^*$ is solved using CRT to get X_j. With the policy W_j and $Y_2 = g^{y_2}$, where $y_2 \in Z_p^*$, it performs the following:

$$Tj = \begin{cases} \hat{e}(g,g)^{(h_i p) y_2}, \text{for positive attributes} \\ \hat{e}(g,g)^{(h_i n) y_2}, \text{for negative attributes} \\ \hat{e}(g,g)^{(h_i d) y_2}, \text{for don't care attributes} \end{cases}$$

  Then the product of T_i's is computed to get T_j and the message is encrypted as $C_j = (T_j \oplus SK_j) M_j$. The sender broadcasts <Hdr,C> where

$$Hdr =< X, W, Y_1, Y_2 >, X = \{X_j, 1 \le j \le m\},$$
$$W = \{W_j, 1 \le j \le m\} \text{ and } C = \{C_j, 1 \le j \le m\}$$

- *Decrypt*: after receiving the tuple <Hdr, C>, the user with identity ID_{ij} computes the key K_{ij} using bilinear pairing from his secret key $S_{ID_{ij}}$ and Y_1. The user recovers SK_j by performing X_j modulo K_{ij}. The user also computes T_j using his keys for the attributes. The user with the corresponding secret key computes,

$$Dj = \begin{cases} (g^{r_i + h_i p})^{pr^{-1}}, \text{for the positive attributes in the policy} \\ (g^{r_i + h_i n})^{pr^{-1}}, \text{for the negative attributes in the policy} \\ (g^{r_i + h_i d})^{pr^{-1}}, \text{for other attributes, not in the policy} \end{cases}$$

  using which he finds $T_i = \hat{e}(D_i, Y_2)$ for each D_i. Then the user also computes $\hat{e}(\hat{D}, Y_2)$ and gets T_j. Then the user decrypts the cipher text C_j using SK_j and T_j to obtain the message M_j.

Algorithm 1 illustrates the proposed algorithm in pseudocode.

Algorithm 1: Proposed algorithm

Setup (k, N = {a_1, a_2, a_3, …a_t})

S1: *Construct a bilinear mapping* $\hat{e}: GXG \to G_T$ *where* G, G_T *are cyclic groups of prime order p, with* $|p| = k$.

S2: *Select a generator* $g \in G$ *and* $pr \in \in Z_p^*$

S3: *Compute* $P = g^{pr}$.
The master public, secret key(msk) pair is (P, pr).

S4: *Choose a hash function* $H_1 : \{0,1\}^* \to G$

S5: The public parameters corresponding to the three types of occurrences of the attributes are, $g^{h_1 p}, g^{h_2 p}, \ldots g^{h_t p}$, *for positive attributes*
$g^{h_1 n}, g^{h_2 n}, \ldots g^{h_t n}$, *for negative attributes*
$g^{h_1 d}, g^{h_2 d}, \ldots g^{h_t d}$, *for don't care case of attributes.*

S6: *Output the public parameters as*
$< p, G, G_T, \hat{e}, P, H_1, \{g^{h_i p}\}_{1\le i\le t}, \{g^{h_i n}\}_{1\le i\le t}, \{g^{h_i d}\}_{1\le i\le t} >$

Extract (ID_{ij}, pr, S={a_i})

S1: *Compute the secret key of user with identity* ID_{ij} *as* $S_{ID_{ij}} = H_1(ID_{ij})^{pr}$.

S2: *Select random* $r_i \in Z_p^*$ *for every attribute* $a_i \in N$, *such that* $\sum_{i=1}^{n} r_i = rpr$

S3: For each $a_i \in N$, *set*, $D_i = (g^{r_i + h_i p})^{pr^{-1}}$ *if* $a_i \in S$, *otherwise set* $D_i = (g^{r_i + h_i n})^{pr^{-1}}$

S4: *For each* $a_i \in N$, *set* $F_i = (g^{r_i + h_i d})^{pr^{-1}}$

S5: *Set* $\hat{D} = g^{-r}$.

S6: *The secret key* $SK =< S_{ID_{ij}}, D_i, F_i, \hat{D} >$

Encrypt($\{M_j \mid 1 \le j \le m\}, W_j, \{Sj = \{ID_{ij} \mid 1 \le i \le n_j, 1 \le j \le m\}$)

S1: Choose random $y_1 \in Z_p^*$ and compute $Y_1 = g^{y_1}$

S2: For each set S_j perform the following:

S2-1: Select random $sk_j \in Z_p^*$ and compute $SK_j = \hat{e}(g,g)^{sk_j}$

S2-2: Select random $y_2 \in Z_p^*$ and compute g^{y_2} and $Y_2 = g^{y_2}$

S2-3: For each selected user i of S_j with identity ID_{ij} compute $K_{ij} = \hat{e}(H_1(ID_{ij}),P)^{y_1}$

S2-3: Compute $Lcm_j = lcm\{K_{ij}\}$

S2-4: Compute $X = SK_j (\mathrm{mod}\, Lcm_j)$ using CRT and get X_j

S2-5: For the policy $W_j = \wedge_{a_i \in I} \tilde{a}_i$ perform the following:

For each $a_i \in I, T_i = \hat{e}(g,g)^{(h_i p) y_2}$, if $\tilde{a}_i = a_i$.

For each $a_i \in I, T_i = \hat{e}(g,g)^{(h_i n) y_2}$, if $\tilde{a}_i = not(a_i)$.

For each $a_i \in N \backslash I$, $T_i = \hat{e}(g,g)^{(h_i d) y_2}$

S2-6: Compute $T_j = \prod_{i=1}^{t} T_i$

S2-7: Compute $C_j = (T_j \oplus SK_j) M_j$

S3: Set $W = \{W_j, 1 \le j \le m\}$ and $C = \{C_j, 1 \le j \le m\}$ and $X = \{X_j, 1 \le j \le m\}$

S4: Set Hdr = < X, W, Y_1, Y_2 >

S5: Broadcast <Hdr, C> to the receivers.

Decrypt (SK, Hdr, C)

The receiver with identity ID_{ij}, in the service group SG_j performs the following steps:

S1: Computes $K_{ij} = \hat{e}(S_{ID_i}, Y_1)$

S2: Computes $SK_j = X_j \bmod K_{ij}$

S3: For each $a_i \in I$, if $\tilde{a}_i = a_i$ and $a_i \in S$, then

$T_i = \hat{e}(D_i, Y_2) = \hat{e}((g^{r_i + h_i p})^{pr^{-1}}, Y_2)$

Similarly if $\tilde{a}_i = not(a_i)$ and $a_i \notin S$, then

$T_i = \hat{e}(D_i, Y_2) = \hat{e}((g^{r_i + h_i n})^{pr^{-1}}, Y_2)$

For each $\tilde{a}_i \in I$, compute

$T_i = \hat{e}(F_i, Y_2) = \hat{e}((g^{r_i + h_i d})^{pr^{-1}}, Y_2)$

S4: Computes $T_j = \left(\prod_{i=1}^{t} T_i \right) * \hat{e}(\hat{D}, Y_2)$

S5: Decrypts the cipher text C_j and gets M_j by computing $M_j = (C_j \oplus SK_j)/T_j$

5. Proof of Correctness

The correctness of decryption of the proposed scheme is justified below:

The KDC computes the key K_{ij}, using $H_1(ID_{ij})$ a random $y_1 \in Z_p^*$ and g^{pr} as below:

$$K_{ij} = \hat{e}(H_1(ID_{ij}),P)^{y_1} = \hat{e}(g^{h_{ij}}, g^{pr})^{y_1} = \hat{e}(g,g)^{y_1 pr h_{ij}} \quad (1)$$

$$X \equiv SK_j (\mathrm{mod}\, Lcm_j) \quad (2)$$

X_j is computed using CRT with Equation (2).

Assuming that the policy described considers the attributes from a_1 to a_x as positive, from a_{x+1} to a_l as negative and the remaining attributes from a_{l+1} to a_t as don't care. That is $\tilde{a}_i = a_i$ for i = 1 to x, $\tilde{a}_i = not(a_i)$ for i = x +1 to l and the remaining $\tilde{a}_i$ from i = l + 1 to t are considered as don't care case. The KDC also computes each of the following

$$T_i = \hat{e}(g,g)^{(h_i p) y_2}, 1 \le i \le x \quad (3)$$

$$T_i = \hat{e}(g,g)^{(h_i n) y_2}, x+1 \le i \le l \quad (4)$$

$$T_i = \hat{e}(g,g)^{(h_i d) y_2}, l+1 \le i \le t \quad (5)$$

The product of Equations (3), (4), and (5) yields

$$T_j = \prod_{i=1}^{t} T_i = \hat{e}(g,g)^{\sum_{i=1}^{x} (h_i p) y_2 + \sum_{i=x+1}^{l} (h_i n) y_2 + \sum_{i=l+1}^{t} (h_i d) y_2} \quad (6)$$

Finally the KDC computes,

$$C_j = (T_j \oplus SK_j) M_j \quad (7)$$

The selected receiver with the message <Hdr, C>, having the attributes satisfying the policy, computes the keys K_{ij}, using the secret key $S_{ID_{ij}}$ and Y_1 as below:

$$K_{ij} = \hat{e}(S_{ID_{ij}}, Y_1) = \hat{e}(g^{h_{ij} pr}, g^{y_1}) = \hat{e}(g,g)^{y_1 pr h_{ij}} \quad (8)$$

$$T_i = \hat{e}(D_i, Y_2) = \hat{e}((g^{r_i + h_i p})^{pr^{-1}}, Y_2) = \hat{e}(g,g)^{(r_i + h_i p) pr^{-1} pry_2}) = \hat{e}(g,g)^{(r_i + h_i p) y_2}, 1 \le i \le x \quad (9)$$

$$T_i = \hat{e}(D_i, Y_2) = \hat{e}((g^{r_i + h_i n})^{pr^{-1}}, Y_2) = \hat{e}(g,g)^{(r_i + h_i n) pr^{-1} pry_2}) = \hat{e}(g,g)^{(r_i + h_i n) y_2}, x+1 \le i \le l \quad (10)$$

$$T_i = \hat{e}(D_i, Y_2) = \hat{e}((g^{r_i + h_i d})^{pr^{-1}}, Y_2) = \hat{e}(g,g)^{(r_i + h_i d) pr^{-1} pry_2}) = \hat{e}(g,g)^{(r_i + h_i d) y_2}, l+1 \le i \le t \quad (11)$$

$$T_i = \hat{e}(\hat{D}, Y_2) = \hat{e}(g^{-r}, g^{pry_2}) = \hat{e}(g,g)^{-rpry_2} \quad (12)$$

Product of 9, 10, 11 and 12 yields

$$\hat{e}(g,g)^{\sum_{i=1}^{x} (h_i p) y_2 + \sum_{i=x+1}^{l} (h_i n) y_2 + \sum_{i=l+1}^{t} (h_i d) y_2} * \hat{e}(g,g)^{\sum_{i=1}^{t} r_i y_2} * \hat{e}(g,g)^{-rpry_2}$$

$$= \hat{e}(g,g)^{\sum_{i=1}^{x} (h_i p) y_2 + \sum_{i=x+1}^{l} (h_i n) y_2 + \sum_{i=l+1}^{t} (h_i d) y_2} * \hat{e}(g,g)^{y_2 \sum_{i=1}^{t} r_i} * \hat{e}(g,g)^{-rpry_2}$$

$$= \hat{e}(g,g)^{\sum_{i=1}^{x} (h_i p) y_2 + \sum_{i=x+1}^{l} (h_i n) y_2 + \sum_{i=l+1}^{t} (h_i d) y_2} * \hat{e}(g,g)^{rpry_2} * \hat{e}(g,g)^{-rpry_2}$$

$$= \hat{e}(g,g)^{\sum_{i=1}^{x}(h_i p)y_2 + \sum_{i=x+1}^{l}(h_i n)y_2 + \sum_{i=l+1}^{t}(h_i d)y_2} = T_j \quad (13)$$

Using K_{ij} from Equation 8,
$SK_j = X_j \bmod K_{ij}$

$$C_j \oplus SK_j = \hat{e}(g,g)^{\sum_{i=1}^{x}(h_i p)y_2 + \sum_{i=x+1}^{l}(h_i n)y_2 + \sum_{i=l+1}^{t}(h_i d)y_2} * M_j \quad (14)$$

Dividing Equation 14 by 13 gives M_j. Hence the correctness is proved.

6. Discussion

There are not many ABBE schemes of constant size header. The security properties of the proposed scheme are analyzed in this section.

- *Forward secrecy and backward secrecy*: The members who have quit the group should not be able to know the later session keys and the users who have newly joined the group should not be able to access the previous broadcast contents. The cipher text is computed using two session keys SK_j and T_j which are randomly generated for every session. After recovering SK_j only, the user can decrypt using the attributes. The computational part of SK_j, from X_j helps in preserving forward and backward secrecy of the scheme. For every session, new values of K_{ij} are computed for all the selected users. These $K'_{ij}s$ are determined by a random $y_1 \in Z_p^*$ and hence Lcm_j, which depends on K_{ij} also changes for every session. Therefore the system of congruences and hence its solution changes in every session, preserving forward and backward secrecy. So a new user cannot deduce the previous keys as his identity was not included in the computation of X_j. Similarly an old user, who is not currently a member of the group cannot obtain the key SK_j as his identity ID_{ij} was not included in the computation of SK_j.
- *Stateless users*: The users are stateless as their private keys are independent of the broadcast. The private keys of the users do not change for each session and cannot be updated through the lifetime of the system and hence the users are stateless.
- *Constant Size Cipher text*: In the proposed scheme, the sender sends Hdr = < *X, W, Y*$_1$, *Y*$_2$ > where *X* = { X_j ; $1 \le j \le m$}, *W* = { W_j, $1 \le j \le m$}. The size of the cipher text is independent of the number of users and number of attributes. The scheme provides a constant size header for each group consisting of four elements for decryption purpose for each service group.

Scheme in [11] sends the polynomial of order of attributes in the header whereas the proposed scheme needs only four elements, two from *G*, one from G_T and an access structure to be multicast in the header. Hence the header size of proposed scheme is relatively smaller as compared to scheme in [11]. The size of the header is similar to that of the scheme by in [26].

7. Security Analysis

In this section, confidentiality of the scheme is proved in random oracle model. Also the efficiency of the scheme is analyzed and compared with that of some of the existing schemes. Even though standard model security proof is possible for the proposed attribute based encryption scheme, we need random oracle model since the identities of the selected users are hashed using hash functions that are random. The security of the proposed scheme reduces to solving the DBDH problem and DDH Problem. The security of the proposed scheme is proved against indistinguishability under chosen plain text attack (IND-CPA attack).

The proof is modeled using a game between the adversary $\mathcal{A}$ and the challenger C.

- *Theorem 1*: If A is an adversary against the proposed ABBE scheme with advantage ε', then using A, two more adversaries A_{DBDH} and A_{DDH} can be constructed against DBDH and DDH respectively with advantages ε_1 and ε_2 respectively where $\varepsilon_1 + \varepsilon_2 \ge \varepsilon'$.
- *Proof*: A reductionist argument is presented assuming that there exists a PPT adversary A that has non-negligible advantage against the proposed scheme. Let C, be the challenger who simulates the results to answer for queries from the adversary.
- *Initialization*: During this phase, the adversary A sends the challenger C the set of identities S_j^* of the users and the access structure W^* on which A wants to be challenged.
- *Setup*: During this phase, C generates the public parameters. C chooses a random g^a from *G* and sets it as the master public key. C also sets the public parameters for the positive attributes, negative attributes and the don't care attributes as $\{g^{ah_i p}\}_{1\le i\le t}, \{g^{ah_i n}\}_{1\le i\le t}, \{g^{ah_i d}\}_{1\le i\le t}$ .C chooses a hash function $H_1 : \{0,1\}^* \to G$, a pairing $\hat{e}: GXG \to G_T$. C outputs the public parameters $< p, g, P, \{g^{ah_i p}\}_{1\le i\le t}, \{g^{ah_i n}\}_{1\le i\le t}, \{g^{ah_i d}\}_{1\le i\le t}, H_1, \{g^{h_i p}\}_{1\le i\le t}, \hat{e}, G, G_T >$.
- *Phase 1*: The adversary A submits a list of attributes S^* along with an identity ID_{ij} for private key query where $ID_{ij} \notin S_j^*$. Adversary can query the random oracle H_1 at any time. C maintains a hash list H_1T which consists of the five tuples $(ID_{ij}, h_{ij}, H_1(ID_{ij}), mark, S_{ID_{ij}}), h_{ij} \in Z_p^*$ and all

variables are initially assigned null. Let the probability of marking an identity ID_{ij} be δ. When an identity ID_{ij} is marked, value one is assigned to mark in H_1T. Given a ID_{ij} query, C searches for that ID_{ij} in H_1T and outputs the corresponding $H_1(ID_{ij})$, if it is present. Otherwise C does the following:

1. Selects random r, $h_{ij} \in Z_p^*$
2. Computes $H_1(ID_{ij})$ as $g^{h_{ij}}$, for marked cases and $H_1(ID_{ij})$ as $g^{rh_{ij}}$, for unmarked cases.
3. Stores the tuple (ID_{ij}, h_{ij}, $H_1(ID_{ij})$) in H_1T.
4. Gives the result $H_1(ID_{ij})$ to the adversary.

For the list submitted by the adversary, the challenger generates a private key of the user ID_{ij} with attributes as below: C chooses a random $h_{ij} \in Z_p^*$ and computes $SK_{ID_{ij}} = (g^a)^{h_{ij}}$. For the attribute set *S*, C considers $\{r_p = ar_i^{'}\}_{1 \le i \le t}$ where $r_i^{'} \in_R Z_p^*$ for all the attributes. C generates the private key $\{g^{r_i^{'}+h_i p}\}$ for the set S and $\{g^{r_i^{'}+h_i n}\}$ for the set $\mathcal{N} \setminus$ S. C also generates $\{g^{r_i^{'}+h_i d}\}_{1 \le i \le t}$ for all the attributes and sets $\hat{D} = g^{-(\sum r_i^{'})}$.

Correctness of the keys generated by C is described below:

The private key $SK_{ID_{ij}}$ of the original scheme is $(g^{h_{ij}})^{pr}$ which is $g^{h_{ij} pr}$ where g^{pr} is the master public key. Similarly C has considered g^a as the master public key and has generated $(g^a)^{h_{ij}}$ as the secret key of the user, which shows the correctness of the key $SK_{ID_{ij}}$ generated by C. The private key component corresponding to the attributes in the original scheme are $(g^{r_i^{'}+h_i p})^{pr^{-1}}$ for the attributes in *S*. Hence

$$\hat{e}(g^{(r_i^{'}+h_i p)pr^{-1}}, g^{pr}) = \hat{e}(g,g)^{r_i+h_i p} \quad (15)$$

Similarly the key component generated by the challenger C is $g^{r_i^{'}+h_i P}$ which in turn gives

$$\hat{e}(g^{(r_i+h_i p)}, g^a) = e(g,g)^{r_i^{'}+h_i pa} = e(g,g)^{r_i+h_i pa} \quad (16)$$

Equations 16 and 17 prove the correctness of the keys D_i, F_i generated by the challenger.

- *Challenge query*: The adversary A gives two messages M_0, M_1 to the challenger. The challenger generates a cipher text for the set S_j^* using W^* and outputs the same.
- *Phase 2*: In addition to extract queries, the adversary is also given access to H_1 query, which doesn't give any additional advantage.
- *Guess*: The adversary makes a guess for b. If $b' = b$ then the adversary wins the game.

If $|P(b'=b) - 1/2| > \varepsilon$, then it means, the adversary has correctly solved the DBDH problem to find the correc SK_j. Since $C_j \oplus SK_j$ is the first part of decryption, where $SK_j = X_j \bmod K_{ij}$ and K_{ij} can be correctly found upon solving DBDH by distinguishing between $(g, g^{pr}, g^{h_{ij} pr}, g^{y_1}, \hat{e}(g,g)^{h_{ij} pr y_1})$ and $(g, g^{pr}, g^{h_{ij} pr}, g^{y_1}, z)$ The second part of decryption needs the adversary to distinguish between $(g, g^{pr}, g^{y_2}, g^{pr y_2})$ and $(g, g^{pr}, g^{y_2}, g^c)$, solving the DDH problem. If the adversary wins the game, then it can be used by the adversaries to solve DBDH problem and DDH problem with advantages ε_1 and ε_2 respectively, where $\varepsilon_1 + \varepsilon_2 \ge \varepsilon'$. Hence the security proof.

8. Conclusions and Future Works

An attribute based broadcast encryption scheme for multi privileged group of users is proposed in this paper. The proposed scheme produces a constant size header to be broadcast. The proposed scheme provides stateless users, and it preserves forward as well as backward secrecy of users. The size of the header of the proposed scheme is relatively less than the scheme in [11]. The security of the proposed scheme has been analyzed under random oracle model and has been proved to be IND-CPA secure under Decisional Bilinear Diffie Hellman problem and Decisional Diffie Hellman problem. The proposed scheme has been modelled using AND gates whereas schemes supporting any access structure could be developed in future.

References

[1] Attrapadung N., Herranz J., Laguillaumie F., Libert B., Panafieu E., and Ràfols C., "Attribute-Based Encryption Schemes with Constant-Size Ciphertexts," *Theoretical Computer Science*, vol. 422, pp. 15-38, 2012.

[2] Balu A. and Kuppusamy K., "An Expressive and Provably Secure Ciphertext-Policy Attribute-Based Encryption," *Information Sciences*, vol. 276, pp. 354-362, 2014.

[3] Bethencourt J., Sahai A., and Waters B., "Ciphertext-Policy Attribute-Based Encryption," *in Proceedings of IEEE Security and Privacy*, Berkley, pp. 321-334, 2007.

[4] Cheung L. and Newport C., "Provably Secure Ciphertext Policy ABE," *in Proceedings of Conference on Computer and Communications Security*, Virginia, PP. 456-465, 2007.

[5] Goyal V., Jain A., Pandey O., and Sahai A., "Bounded Ciphertext Policy Attribute Based Encryption," *International Colloquium on*

Automata Languages and Programming, vol. 5126, pp. 579-591, 2008.

[6] Herranz J., Laguillaumie F., and Ràfols C., "Constant Size Ciphertexts in Threshold Attribute-based Encryption," *in Proceedings of International Conference on Practice and Theory in Public Key Cryptography*, Berlin, pp. 19-34, 2010.

[7] Hur J. and Noh D., "Attribute-based Accesscontrol with Efficient Revocation in Data Outsourcing Systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 7, pp. 1214-1221, 2010.

[8] Ibraimi L., Tang Q., Hartel P., and Jonker W., "Efficient and Provable Secure Ciphertext-Policy Attribute-Based Encryption Schemes," *in Proceedings of the 5th International Conference on Information Security Practice and Experience*, Berlin, pp. 1-12, 2009.

[9] Junod P. and Karlov A., "An Efficient Public-key Attribute-Based Broadcast Encryption Scheme Allowing Arbitrary Access Policies," *in Proceedings of the10thannual ACM Workshop on Digital Rights Management*, Chicago, pp. 13-24, 2010.

[10] Liu Z., Cao Z., and Wong S., "White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Any Monotone Access Structures," *IEEE Transactions On Information Forensics and Security*, vol. 8, no. 1, pp. 76-88, 2013

[11] Lubicz D. and Sirvent T., "Attribute-based Broadcast Encryption Scheme Made Efficient," *in Proceedings of International Conference on Cryptology in Africa*, Dakar, pp. 325-342, 2008.

[12] Ma D., Wu Y., Deng R., and Li T., "Dynamic Access Control for Multi-Privileged Group Communications," *in Proceedings of 6th International Conference on Information and Communications Security*, Malaga, pp. 508-519, 2004.

[13] Muthulakshmi A. and Anitha R., "Balanced keytree Management for Multi-Privileged Groups Using (N, T) Policy," *Security and Communication Networks*, vol. 5, no. 5, pp. 545-555, 2012.

[14] Muthulakshmi A., Anitha R., and Sumathi M., "Non-split Balancing Higher Order Tree for Multi-privileged Groups," *Wseas Transactions on Communications*, vol. 10, no. 10, pp. 308-321, 2011.

[15] Ostrovsky R., Sahai A., and Waters B.,"Attribute Based Encryption with Non-Monotonic Access Structure," *in Proceedings of ACM Conference on Computer and Communications Security*, Alexandria, pp. 195-203, 2007.

[16] Panafieu E., Ràfols C., Libert B., Laguillaumie F., Herranz J., and Attrapadung N., "Attribute-based Encryption Schemes with Constant-Size Ciphertexts," *Theoretical Computer Science*, vol. 422, pp. 15-38, 2012.

[17] Sahai A. and Waters B., "Fuzzy Identity Based Encryption," *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Denmark, pp. 457-473, 2005

[18] Sun J., Hu Y., and Zhang L., "A Key-Policy Attribute-Based Broadcast Encryption," *The International Arab Journal of Information Technology*, vol. 10, no. 5, pp. 444-452, 2013.

[19] Sun Y. and Liu K., "Scalable Hierarchical Access Control in Secure Group Communications," *Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies INFOCOM*, Hong Kong, pp. 1296-1306, 2004.

[20] Wang G., Du Q., Zhou W., and Liu Q., "A Scalable Encryption Scheme for Multi-privileged Group Communications," *The Journal of Supercomputing*, vol. 64, no. 3, pp. 1075-1091, 2011.

[21] Wang G., Liu Q., Wu J., and Guo M., "Hierarchical Attribute-based Encryption and Scalable User Revocation for Sharing Data in Cloud Servers," *Computers and Security*, vol. 30, no. 5, pp. 320-331, 2011.

[22] Wang G., Ouyang J., Chen H., and Guo M., "ID-Based Hierarchical Key Graph Scheme in Multi-Privileged Group Communications," *in proceedings of Global Telecommunications Conference IEEE*, Washington, pp. 172-176, 2007.

[23] Wang G., Ouyang J., Chen H., and Guo M., "Efficient Group key Management for Multi-Privileged Groups," *Computer Communication*, vol. 30, no. 11-12, pp. 2497-2509, 2007.

[24] Yang Y., Hu Y., Sun C., Chao L., and Zhang L.,"An Efficient Group Key Agreement Scheme for Mobile Ad-Hoc Networks," *The International Arab Journal of Information Technology*, vol. 10, no. 1, pp. 10-17, 2013.

[25] Yao X., Chen Z., and Tian Y., "A lightweight Attribute-based Encryption Scheme for the Internet of Things," *Future Generation Computer Systems*, vol. 49, pp. 104-112, 2015.

[26] Zhou Z. and Huang D., "On Efficient Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption," *in Proceedings of the ACM Conference on Computer and Communications Security*, Chicago, pp. 753-755, 2010.

Muthulakshmi Angamuthu has received her Ph.D from Anna University Chennai, is a reviewer for Security and Communication Networks by John Wiley & Sons and Computers & Electrical Engineering by Elsevier. She is a life member of Cryptology Research Society of India. Her research interests include Key management and Broadcast encryption.

Akshaya Mani is a first year PhD student in the Computer Science department at Georgetown University, Washington, DC. She received her integrated M.Sc. degree in Theoretical Computer Science from PSG College of Technology, India, had pursued research in the field of attribute-based cryptography at IITM. Currently, her interests span cryptography and network security.

Anitha Ramalingam is the Programme Coordinator for the five year integrated M.Sc. Theoretical Computer Science programme since 2007. She is the principal investigator of the Collaborative Directed Basic Research in "Smart and Secure Environment project", sponsored by NTRO since March 2007- August 2012. She is Life member of Cryptology Research Society of India, Indian Society of Technical Education and Member of ACM.