Leyou ZHANG[1], Qing WU[2], Yupu HU[1]

Mathematics of Xidian University (1), Xi'an University of Posts and Telecommunications(2)

Efficient Dynamic Data Encryption Algorithm for Mobile Ad Hoc Network

Abstract. *Two proper threshold broadcast encryption schemes are proposed for the mobile ad hoc network. The initial scheme achieves constant size private keys and O(n-t)-size ciphertexts. Under n+1-Decision Bilinear Diffie-Hellman Exponent (n+1-BDHE) assumption, it is provable security in the selective-identity model. Based on the dual system encryption, we propose our main construction. It also has constant size private keys and O(n-t)-size ciphertexts. But it achieves full security under the static assumptions which are more natural than them in the existing schemes.*

Streszczenie. *W artykule zaprezentowano dwie metody szyfrowania danych w mobilnych sieciach Ad Hoc. (**Skuteczny dynamiczny algorytm szyfrowania danych w mobilnych sieciach Ad Hoc**)*

Keywords: threshold broadcast encryption, identity-based encryption, dual system encryption, dynamic encryption, provable security
Słowa kluczowe: szyfrowanie danych, sieci mobilne

Introduction

The concept of Broadcast Encryption (BE) was introduced by Fiat and Naor in [1]. In a broadcast encryption scheme a broadcaster encrypts a message for some subset S of users who are listening on a broadcast channel. Any user in S can use his private keys to decrypt the broadcasts. Any user outside the privileged set S should not be able to recover the message. The threshold broadcast encryption(TBE) problem is generalization of the concept of broadcast encryption. It was first introduced by Ghodosi et al. [2]. TBE has some advantages over traditional threshold encryptions. It is specified as follows:(1) The trusted party is eliminated and the system can be set up by individual users independently; (2) The broadcaster can choose the privileged set and the threshold value at the time of encryption which allows a certain dynamism in the system.

Identity-Based encryption was first proposed by Shamir[3], which a major advantage was that it allowed one to encrypt a message by using recipient's identifiers such as an email address. Now it has been an active area. The first practical identity-based encryption (IBE) scheme was proposed in 2001 by Boneh and Franklin [4], which was provably secure against adaptive chosen ciphertext attack in random oracle model. Then, many other kinds of identity-based encryption were proposed [5-9]. Identity-based cryptography significantly reduces the system complexity and the cost for establishing and managing the public key authentication framework known as PKI (Public Key Infrastructure). As a result, we focus on the construction of identity-based threshold broadcast encryption (IBTHBE) in this paper. To the best of our knowledge, very few works have dealt with this problem. In [10], Chai and Cao et al propose a scheme based on identity. But the length of the ciphertexts is n +1 and the security relies on the random oracles. Vanesa Daza et al propose another scheme [11]. However, its security is still relying on the random oracles. The recent work [12] has short ciphertexts, but the security of their scheme based on the identity (IBTHBE) is also relying on the random oracles. In [13], authors also proposed an efficient scheme in the standard model. But the security only achieves a weak security model-selective-identity model. In [14], an efficient scheme was proposed. However, the public key size is too long and computation cost is high, which is not suitable to the ad hoc networks. In addition, the security is based on a strong hardness assumption.

As a natural extension of the efforts to improve schemes in the standard model, we propose two new efficient identity-based threshold broadcast encryption schemes in this paper. The proposed schemes are constructed in the standard model. In the selective-identity security model, we reduce the security of our first scheme to the n+1-Decision Bilinear Diffie-Hellman Exponent (n+1-DBDHE) assumption. Based on the dual system encryption[15,16], the second scheme achieves the full security under the static assumption. In addition, two schemes have the dynamic feature which is suitable to mobile ad hoc networks. In the proposed schemes, any user can dynamically join the system as a possible recipient, and the sender can dynamically choose the set of recipients S and the threshold value t.

Decisional bilinear Diffie-Hellman Exponent assumption (BDHE)

The decisional bilinear Diffie-Hellman Exponent (BDHE) problem is defined as follows. Algorithm B is given as input a random tuple

$(g, h_0, y_1, \cdots, y_n, y_{n+2}, \cdots, y_{2n+2}, T)$, where $y_i = g^{\alpha^i}$. Algorithm B's goal is to output 1 when $T = e(g,h_0)^{\alpha^{n+1}}$ and 0 otherwise. Let $TU = (g, h_0, y_1, \cdots, y_n, y_{n+2}, \cdots, y_{2n+2})$. Algorithm B that outputs $b \in \{0,1\}$ has advantage ε in solving decision BDHE in G if

$$|Pr[B(TU, e(g,h_0)^{\alpha^{n+1}}) = 0] - Pr[B(TU, T) = 0]| \leq \varepsilon .$$

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

Identity-based Threshold Broadcast Encryption (IDTHBE)

More formally, an IDTHBE consists of five algorithms.

Setup The randomized *Setup* algorithm takes as input a security parameter k and outputs some public parameters *params*, which will be common to all the users of the system.

Extract The key generation algorithm is run by each user ID_i. It takes as input some public parameters params and returns a correspondence private key d_{ID_i}.

Threshold Encryption The encryption algorithm takes as input a set of public keys corresponding to a set P of n receivers, a threshold t satisfying $1 \leq t \leq n$, and a message M. The output is a ciphertext C, which contains the description of P and t.

Partial Decryption Partial Decryption algorithm takes as input a ciphertext C for the pair (P, t) and a secret key d_{ID_i}

of a receiver. The output is a partial decryption value k_i or a special symbol $\perp$.

Decryption The deterministic final decryption algorithm takes as input a ciphertext *C* for the pair (*P*, *t*) and *t* partial decryptions corresponding k_i to receivers in some subset $S \subset P$. The output is a message *m* or a special symbol $\perp$.

Security Model

Setup The challenger runs Setup. Then challenger gives the resulting common parameter to *A*, and keeps master key secret. *A* issues the threshold parameters (*n*, *t*).

***Phase* 1** *A* issues private key extraction and decryption queries adaptively. The adversary *A* adaptively issues queries $q_1, \cdots, q_{s0}$, where q_i is one of the following:

• On a private key extraction query upon ID_i, the challenger runs *Extract* to generate the private key associated to ID_i, then sends it to *A*.

• On a decryption queries, the challenger runs *Decryption* to generate decryption shares and gives them to *A*.

Challenge When *A* decides that phase 1 is over, it submits a set of identities S^*, a threshold value *t* and two messages (M_0, M_1)on which it wants to be challenged. The adversary's choice of S^* is restricted to the identities that he did not request a private key for in Phase 1. The challenger runs *Encrypt* algorithm to obtain (Hdr^*, *K*) =*Encrypt*(S^*, *PK*, *t*) and returns them to *A*. Note, *A* may already learned about the private keys of at most $t-1$. There is the natural constraint that S^* contains at most $t-1$ corrupted identities.

***Phase* 2** The adversary continues to issue queries $q_{s0+1}, \cdots, q$, where q_i is one of the following:

• *Extraction query* (ID_i), as in phase 1;

• *Decryption query*, as in phase 1, but with the constraint that $Hdr \neq Hdr^*$. The challenger responds as in phase 1.

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

We say that if the above indistinguishability game allow no decryption oracle query, then the IDTHBE scheme is only chosen plaintext(IND-fullID-CPA) secure. If the challenge identity is outputted before the setup algorithm, it is called selective-identity security model. There have been many methods to convert an IND-fullID-CPA scheme to an IND-fullID-CCA scheme. Therefore, we only focus on constructing the IND-fullID-CPA scheme in this paper.

Our initial Constructions

We first give an initial construction which will derive a high efficient scheme in the next section.

Let $S = \{ID_1, \cdots, ID_n\}$ be *n* players where $ID_i \in Z_p$. These users want to form an ad hoc network. Our construction works as follows:

***Setup*:** To generate the system parameters, the PKG picks randomly generators $\{g, g_2, h, h_i, 1 \le i \le n\}$ in G and an element α from Z_p. Note that any user ID_i will be associated to a different element t_i. This can be done by defining $t_i = f(ID_i)$ for some *n*-1 degree polynomial function $f(x)$, where $f(0) = \alpha$. PKG sets $T_i = g^{t_i}$ for $1 \le i \le n$ and $g_1 = g^{\alpha}$. The public parameters *PK* are

$$PK = (g, g_1, g_2, T_i, h, h_i, 1 \le i \le n)$$

and α is master key.

Extract(ID$_i$) : To generate a private key for a user $ID_i \in Z_p$, the PKG picks randomly $r_i \in Z_p$ and computes private keys as follows:

$$d_{ID_i} = (d_{i0}, d_{i1}, d_{i2}) = (g_2^{t_i}(hh_i^{ID_i})^{r_i}, g^{r_i}, H^{r_i}),$$

where $H = \prod_{j=1, j\neq i}^{n} h_j^{ID_j}$.

***Threshold Encryption*:** To encrypt a message M for a set $S = \{ID_1, \cdots, ID_n\}$ of *n* players, with threshold $t \le n$ for the decryption, the idea is to set up an (n, N)-threshold secret sharing scheme where $N = 2n - t$. The *n* public keys $(T_1, \cdots, T_n)$ of users implicitly define a $n-1$ degree polynomial. The idea is to compute the values of this polynomial in the points $x = 0$ (This will lead to obtain the value of g_1).Then a sender acts as follows:

• Select a random element $s \in Z_p^*$ and compute $C_1 = g^s, C_2 = e(g_1, g_2)^s M$ and $C_3 = (\prod_{i=1}^{n} h_i^{ID_i} h)^s$.

• Choose a set $\overline{S}$ of $n-t$ dummy players, such that $\overline{S} \cap S = \phi$. For each user $ID_i' \in \overline{S}$, compute $T_i' = \prod_{ID_i \in S} T_i^{\lambda_{ij}}$ and $K_i = \frac{1}{e(T_i', g_2^s)}$, where λ_{ij} denotes the Lagrange coefficients.

The ciphertexts are $(C_1, C_2, C_3, \{K_i\}_{ID_i' \in \overline{S}})$.

Note: $K_i = \frac{1}{e(T_i', g_2^s)} = \frac{1}{e(g^{t_i'}, g_2^s)}$ by using Lagrange interpolation where $t_i' = f(ID_i')$.

***Partial Decryption*:** Given the ciphertexts $(C_1, C_2, C_3, \{K_i\}_{ID_i' \in \overline{S}})$, the receiver $ID_i \in S$ with his corresponding private d_{ID_i} computes as follows:

$$K_i = \frac{e(C_3, d_{i1})}{e(d_{i0} d_{i2}, C_1)} = \frac{1}{e(g^{t_i}, g_2)^s}.$$

***Decryption*:** Given the valid ciphertexts $(C_1, C_2, C_3, \{K_i\}_{ID_i' \in \overline{S}})$, a subset $S_1 \subset S$ with $|S_1| = t$ and corresponding *t* partial decryption K_j, the algorithm computes with the whole set $S' = S_1 \bigcup \overline{S}$ as follows:

$$K = \prod_{ID_i \in S'} K_i^{\lambda_{i0}} = \frac{1}{e(g_1, g_2)^s} \text{ and } M = K \cdot C_2.$$

Our main construction

The initial construction will be provable security in the selective-identity model. In this section, based on the dual system encryption over the composite group, we will give our main construction which will achieve the full security.

Let G be cyclic groups of order $N=p_1p_2p_3$ and *l* denote the maximum number of the set of possible users. Let S = $\{ID_1, \cdots, ID_n\}$ be n players where $ID_i \in Z_N$. These users want to form an ad hoc network. Our scheme works as follows.

Our construction works as follows:

***Setup*:** To generate the system parameters, the PKG picks randomly generators $\{g, g_2, h\}$ in G_{p_1} and an element α from Z_N. Note that any user ID_i will be associated to a different element t_i. This can be done by defining $t_i = f(ID_i)$ for some *n*-1 degree polynomial

function $f(x)$, where $f(0)=\alpha$. PKG sets $T_i = g^{t_i}$ for $1 \le i \le n$ and $g_1 = g^{\alpha}$. The public parameters *PK* are

$$PK = (g, g_1, g_2, T_1, \cdots, T_n, h)$$

and α is master key.

Extract(ID$_i$) **:** To generate a private key for a user $ID_i \in Z_N$, the PKG picks randomly $r_i \in Z_N$ and $R_{i0}, R_{i1} \in G_{p_3}$ computes private keys as follows:

$$d_{ID_i} = (d_{i0}, d_{i1}) = (g_2^{t_i}(hg^{ID_i})^{r_i} R_{i0}, g^{r_i} R_{i1}).$$

Threshold Encryption**:** It is same as initial scheme.

Decryption**:** It is same as initial scheme.

Correctness(Partial Decryption): In fact, if the ciphertexts $C = (C_0, C_1, C_2)$ is valid, then one can obtain the following equation holds.

$$\frac{e(C_3, d_{i1})}{e(d_{i0}\prod_{j=1, j\neq i}^{n} d_{i1}^{ID_j}, C_1)} = \frac{e((h\prod_{i=1}^{n} g^{ID_i})^s, g^{r_i} R_{i1})}{e(g_2^{t_i}(hg^{ID_i})^{r_i} R_{i0}\prod_{j=1, j\neq i}^{n}(g^{r_i} R_{i1})^{ID_j}, g^s)}$$

$$= \frac{e((h\prod_{i=1}^{n} g^{ID_i})^s, g^{r_i}) e((h\prod_{i=1}^{n} g^{ID_i})^s, R_{i1})}{e(g_2^{t_i}(hg^{ID_i})^{r_i}\prod_{j=1, j\neq i}^{n}(g^{r_i})^{ID_j}, g^s) e(R_{i0}, g^s) e(\prod_{j=1, j\neq i}^{n}(R_{i1})^{ID_j}, g^s)}$$

$$= \frac{1}{e(g_2^{t_i}, g)^s}.$$

In the previous equations, the orthogonality property of $G_{p_1}, G_{p_2}, G_{p_3}$ is used. It is described simply as follows.

Lemma 1[17] When $h_i \in G_{p_i}, h_j \in G_{p_j}$ for $i \neq j$, $e(h_i, h_j)$ is the identity element in G_1 .

By using this lemma, one can obtain

$$e(R_{i0}, g^s) = e(\prod_{j=1, j\neq i}^{n}(R_{i1})^{ID_j}, g^s) e((h\prod_{i=1}^{n} g^{ID_i})^s, R_{i1}) = 1.$$

Table 1. Comparison of the Efficiency with the others Scheme

Schemes	C-Size	pk Size	Parings	S.M
[10]	n +1	1	1 +2 t	Full
[11]	$n-t$	1	3 t +2 t	Full
[12]	n	2	(0+ t)+1	Full
[13]	$O(n-t)$	2	2	s-ID
[14]	$O(n-t)$	2	0+ t	Full
Initial	$O(n-t)$	3	0+ t	s-ID
Main	$O(n-t)$	2	0+ t	Full

Efficiency Analysis

In our scheme, the size of ciphertexts is $O(n-t)$ and the size of private key is constant as it consists of two group elements. This is the efficient construction which has full security in the standard model for the identity-based threshold broadcast encryption. In addition, if the values $e(g_1, g_2)$ and $e(T_i, g_2)$ can be precomputed and cached, so no pairing computations are needed at the phase of *Threshold Encryption*. Another advantage in our scheme is the natural security basis. The security of our initial scheme is achieved in the decision BDH assumption. And the security of our main scheme is reduced to three static assumptions. Table 1 gives the efficiency comparison between ours and the others IDTHBEs. From the table 1, our main construction has a natural security basis over [14]. In addition, our main scheme has much shorter public keys than the scheme in [14].

Note: R.O. denotes the random oracles. C-Size is the size of ciphertext and pk is the private keys. SM denotes the security model. Full and s-ID are full security and selective-identity model.

Security Analysis

At first, we give the security proof of initial scheme.

Theorem 1 Suppose the decision BDHE assumption holds. Then the proposed initial scheme above is semantically secure against selective identity, chosen plaintext attacks.

Proof Suppose an adversary *A* can attack the initial scheme with advantage ε . We will show that there is an algorithm *B* that solves the decision BDHE problem in *G* with the advantage ε . For a generator $g \in G$ and $\alpha \in Z_p$, set $y_i = g^{\alpha^i} \in G$. Algorithm *B* is given as input a random tuple (g, h_0, $y_1, \cdots, y_n, y_{n+2}, \cdots, y_{2n+2}$, T). Algorithm *B*'s goal is to output 1 when $T = e(g,h_0)^{\alpha^{n+1}}$ and 0 otherwise. Algorithm *B* works by interacting with *A* in a threshold selective-identity game as follows:***Init*****:** *A* outputs a set $S^* = (ID_1^*, \cdots, ID_n^*)$ of identities that it wants to attack, and a set $\tilde{S}$ of identities that it wants to corrupt, with $|\tilde{S}| \le n-1$ and $|\tilde{S} \cap S^*| \le t-1$.

Setup**:** *B* does the following:

- First, *B* picks a random $\gamma \in Z_p^*$, sets $g_1 = y_1 = g^{\alpha}$ and $g_2 = y_n g^{\gamma}$. Then *B* selects randomly $\gamma_1, \gamma_2, \cdots, \gamma_n$ in Z_p^* and sets $h_i = g^{\gamma_i} / y_{n-i+1}$ for $1 \le i \le n$. In addition, *B* selects randomly $\upsilon \in Z_p^*$ and sets $h = g^{\upsilon}\prod_{i=1}^{n} y_{n-i+1}^{ID_i^*}$.
- Next, *B* selects $n-1$ random integers $\alpha_1, \alpha_2, \cdots, \alpha_{n-1} \in Z_p$. Let $f(x)$ be the degree $n-1$ polynomial implicitly defined to satisfy $f(0)=\alpha$ and $f(ID_i) = \alpha_i$ for $ID_i \in \tilde{S}$, note that *B* does not know f since it does not know α . For $ID_i \in \tilde{S}$, *B* computes $T_i = g^{\alpha_i}$. Otherwise, *B* computes $\alpha_i = f(ID_i) = \lambda_0\alpha + \sum_{j=1}^{n-1}\lambda_j\alpha_j$ with the Lagrange coefficients λ_j . Note that these Lagrange coefficients are easily calculated since they do not depend on f . Then *B* sets $T_i = g_1^{\lambda_0}\prod_{ID_j \in \tilde{S}} T_j^{\lambda_j}$. Finally, *B* gives the public keys *PK*=($g, g_1, g_2, h, T_1, \cdots, T_n, h_1, \cdots, h_n$) to *A*.

Query phase **1:** *A* issues up to q_s private key generation queries to the uncorrupt servers. Each query q_i works as follows: Suppose *A* asks for the private key corresponding to an identity $ID_i \in S'(ID_i \notin S^*)$. The restriction ensures that $ID - ID_i^* \neq 0$. *B* first computes the Lagrange coefficients $\lambda_0, \lambda_1, \cdots, \lambda_{n-1}$ such that $t_i = f(ID_i) = \lambda_0\alpha + \sum_{j=1}^{n-1}\lambda_j\alpha_j$. Then *B* selects a random $r \in Z_p$ and computes the corresponding private keys as follows:

$$d_{ID_i} = (d_{i0}, d_{i1}, d_{i2})$$

$$= (g_1^{\lambda_0\gamma} g_2^{\sum_{j=1}^{n-1}\lambda_j\alpha_j} (g^{\gamma_i ID_i + \upsilon}\prod_{j=1, j\neq i}^{n} y_{n-j+1}^{ID_j^*})^{\tilde{r}_i} (y_{n-i+1}^{ID_i - ID_i^*})^r,$$

$$g^r y_i^{\frac{\lambda_0}{ID_i - ID_i^*}}, (\prod_{j=1, j\neq i}^{n}(\frac{g^{\gamma_j}}{y_{n-j+1}})^{ID_j})^r (\prod_{j=1, j\neq i}^{n}(\frac{y_j^{\gamma_j}}{y_{n-j+i+1}})^{ID_j})^{\frac{\lambda_0}{ID_i - ID_i^*}})$$

One can verify $d_{ID_i} = (d_{i0}, d_{i1}, d_{i2})$ is the valid simulation. In fact,

$$g_1^{\lambda_0\gamma} g_2^{\sum_{j=1}^{n-1}\lambda_j\alpha_j} (g^{\gamma_i ID_i+\upsilon}\prod_{j=1,j\neq i}^{n} y_{n-j+1}^{ID_j^*})^{\tilde{r}_i} (y_{n-i+1}^{ID_i-ID_i^*})^r$$

$$= y_{n+1}^{\lambda_0} g_1^{\lambda_0\gamma} g_2^{\sum_{j=1}^{n-1}\lambda_j\alpha_j} (y_{n-i+1}^{ID_i-ID_i^*})^r \Big/ y_{n+1}^{\lambda_0} (g^{\gamma_i ID_i+\upsilon}\prod_{j=1,j\neq i}^{n} y_{n-j+1}^{ID_j^*})^{\tilde{r}_i}$$

$$= g_2^{\lambda_0\alpha} g_2^{\sum_{j=1}^{n-1}\lambda_j\alpha_j} (y_{n-i+1}^{ID_i-ID_i^*})^r \Big/ y_{n+1}^{\lambda_0} (g^{\gamma_i ID_i+\upsilon}\prod_{j=1,j\neq i}^{n} y_{n-j+1}^{ID_j^*})^{\tilde{r}_i}$$

$$= g_2^{\lambda_0\alpha+\sum_{j=1}^{n-1}\lambda_j\alpha_j} (y_{n-i+1}^{ID_i-ID_i^*})^r (y_{n-i+1}^{ID_i-ID_i^*})^{\frac{\lambda_0\alpha^i}{ID_i-ID_i^*}} (g^{\gamma_i ID_i+\upsilon}\prod_{j=1,j\neq i}^{n} y_{n-j+1}^{ID_j^*})^{\tilde{r}_i}$$

$$= g_2^{\lambda_0\alpha+\sum_{j=1}^{n-1}\lambda_j\alpha_j} (y_{n-i+1}^{ID_i-ID_i^*})^{\tilde{r}_i} (g^{\gamma_i ID_i+\upsilon}\prod_{j=1,j\neq i}^{n} y_{n-j+1}^{ID_j^*})^{\tilde{r}_i}$$

$$= g_2^{\lambda_0\alpha+\sum_{j=1}^{n-1}\lambda_j\alpha_j} (g^{\gamma_i ID_i+\upsilon} y_{n-i+1}^{ID_i-ID_i^*} g^{\upsilon}\prod_{j=1,j\neq i}^{n} y_{n-j+1}^{ID_j^*})^{\tilde{r}_i}$$

$$= g_2^{t_i}(h_i^{ID_i}h)^{\tilde{r}_i}\ ((g^{\gamma_i}/y_{n-i+1})^{ID_i} g^{\upsilon}\prod_{j=1}^{n} y_{n-j+1}^{ID_j^*})^{\tilde{r}_i} = g_2^{t_i}(h_i^{ID_i}h)^{\tilde{r}_i};$$

$$g^r y_i^{\frac{\lambda_0}{ID_i-ID_i^*}} = g^r g^{\frac{\lambda_0\alpha^i}{ID_i-ID_i^*}} = g^{\tilde{r}_i};$$

$$(\prod_{j=1,j\neq i}^{n}(\frac{g^{\gamma_j}}{y_{n-j+1}})^{ID_j})^r (\prod_{j=1,j\neq i}^{n}(\frac{y_j^{\gamma_j}}{y_{n-j+i+1}})^{ID_j})^{\frac{\lambda_0}{ID_i-ID_i^*}} = (\prod_{j=1,j\neq i}^{n} h_j^{ID_j})^{\tilde{r}},$$

where $\tilde{r}_i = r + \frac{\lambda_0\alpha^i}{ID_i - ID_i^*}$.

Challenge**:** *A* outputs two same-length messages M_0 and M_1 on which it wishes to be challenged. *B* picks a random $b \in \{0,1\}$ and constructs the challenge ciphertexts as follows:

$$C^* = (C_1^*, C_2^*, C_3^*, \{K_i\})$$

$$= (h_0, M_b e(g_1, h_0^{\gamma})T, h_0^{\upsilon+\sum_{i=1}^{n} ID_i^*\gamma_i}, \{K_i\}_{ID_i\in S_0})$$

where S_0 is a set of $n - t$ dummy users. In addition, K_i is computed in the following manner:

B first chooses a set S_0 of $n-t$ dummy users such that $S_0 \bigcap S^* = \phi$. For each dummy user $ID_i \in S_0$, *B* computes the Lagrange coefficients λ_{ji} with $1 \le j \le n$ such that $t_j' = f(ID_j) = \sum_{ID_i^*\in S^*}\lambda_{ji}\alpha_i'$, where α_i' is known to *B* since *B* can compute it by using $(\alpha_1, \alpha_2, \cdots, \alpha_{n-1})$ and satisfies $g^{\alpha_i'} = T_i$. Then *B* computes $T_j' = \prod_{ID_i^*\in S^*} T_i^{\lambda_{ji}}$. Finally, *B* computes $K_i = \frac{1}{e(h_0^{\sum_{i=1}^{n}\lambda_{ji}\alpha_i'}, g_2)}$. Let $h_0 = g^s$ for some unknown $\mu \in Z_p$. If $T = e(g,h_0)^{\alpha^{n+1}}$, one can obtain that C^* is a valid encryption for M_b. In fact, $C_1^* = g^c$,

$$C_2^* = M_b e(g_1, h_0^{\gamma})T = M_b e(g_1, h_0^{\gamma})\ e(g,h_0)^{\alpha^{n+1}}$$

$$= M_b e(g_1, h_0^{\gamma})\ e(g^{\alpha^{n+1}}, h_0) = M_b(e(g_1, g^{\gamma})e(g^{\alpha^n}, g_1))^s$$

$$= M_b e(g_1, g^{\gamma} y_n)^s = M_b e(g_1, g_2)^s.$$

$$C_3^* = h_0^{\upsilon+\sum_{i=1}^{n} ID_i^*\gamma_i} = (g^{\upsilon+\sum_{i=1}^{n} ID_i^*\gamma_i})^s = (\prod_{j=1}^{n} g^{ID_j^*\gamma_j} g^{\upsilon})^s$$

$$= (\prod_{j=1}^{n}(g^{\gamma_j}/y_{n-j+1})^{ID_j^*} g^{\upsilon}\prod_{j=1}^{n}(y_{n-j+1})^{ID_j^*})^s = (\prod_{i=1}^{n} h_i^{ID_i} h)^s.$$

and

$$K_i = \frac{1}{e(h_0^{\sum_{i=1}^{n}\lambda_{ji}\alpha_i'}, g_2)} = \frac{1}{e(g^{\sum_{i=1}^{n}\lambda_{ji}\alpha_i'}, g_2)^s} = \frac{1}{e(\prod_{i=1}^{n} T_i^{\lambda_{ji}}, g_2)^s} = \frac{1}{e(T_i', g_2)^s}.$$

If T is a random element of G_1, C^* gives no information about *B*'s choice of *b*.

***Phase* 2:** The adversary continues to issue queries and *B* responds as in phase 1.

Guess**:** *A* outputs a guess $b' \in \{0,1\}$ and wins the game if $b' = b$. If $b' = b$, *B* will output 1 to indicate that *B* solves the DBDHE problem, otherwise it outputs 0 to mean that it learns nothing from C^*.

When *A* outputs 1, it means $|Pr(b = b') - \frac{1}{2}| \ge \varepsilon$. Otherwise $Pr(b = b') = \frac{1}{2}$. Therefore, we have

$$|\Pr(B(TU, e(g,g_0)^{\alpha^{n+1}}) = 0) - \Pr(B(TU,T) = 0)| \ge |\frac{1}{2} \pm \varepsilon - \frac{1}{2}| = \varepsilon.$$

Static Hardness Assumption

In this section, we give our complex assumption. These assumptions have been used in [15,16].

Assumption 1(Subgroup decision problem for 3 primes) Given (*N*= $p_1p_2p_3$, G, G_1,*e*), select randomly $g \in G_{p_1}$, $X_3 \in G_{p_3}$, $T_1 \in G_{p_1p_2}$, $T_2 \in G_{p_1}$ and set *D*=(*N*= $p_1p_2p_3$, G, G_1,*e*, *g*, X_3). It is hard to distinguish T_1 from T_2. The advantage of an algorithm is defined as

Assumption 2 Given (*N*= $p_1p_2p_3$, G, G_1,*e*), pick randomly $g, X_1 \in G_{p_1}$, X_2, $Y_2 \in G_{p_2}$, $X_3, Y_3 \in G_{p_3}$, set D=(*N*= $p_1p_2p_3$, G, G_1,*e*, *g*, X_1X_2, X_3, Y_2Y_3). Then select $T_1 \in G$, $T_2 \in G_{p_1p_3}$ at random. It is hard to distinguish T_1 from T_2.

Assumption 3 Given (*N*= $p_1p_2p_3$, G, G_1,*e*), pick randomly $g \in G_{p_1}$, X_2, $Y_2, Z_2 \in G_{p_2}$, $X_3 \in G_{p_3}$, $\alpha, s \in Z_N$, set D=(*N*= $p_1p_2p_3$, G, G_1, *e*, *g*, $g^{\alpha}X_2, X_3, g^sY_2, Z_2$). Then compute $T_1 = e(g,g)^{\alpha s}$ and pick randomly $T_2 \in G_1$. It is hard to distinguish T_1 from T_2.

Next, we will prove the security of the main scheme. We first define semi-functional keys and semi-functional ciphertexts. Let g_2 denote a generator of G_{p_2}.

Semi-functional keys: At first, a normal key $(\overline{d}_0, \overline{d}_1, \overline{d}_2)$ is obtained using the *Extract* algorithm. Then some random elements $\gamma_0, \gamma_1, \gamma_2$ are chosen in Z_N. The semi-functional keys are set as follows.

$$d_0 = \overline{d}_0 g_2^{\gamma_0}, d_1 = \overline{d} g_2^{\gamma_1}, d_2 = \overline{d}_2 g_2^{\gamma_2}.$$

Semi-functional ciphertexts: At first, a normal semi-functional ciphertext (C_0', C_1', C_2') is obtained using the *Encrypt* algorithm. Then two random elements λ_1, λ_2 are chosen in Z_N. The semi-functional ciphertexts are set as follows: $C_0 = C_0'$, $C_1 = C_1' g_2^{\lambda_1\lambda_2}$, $C_2 = C_2' g_2^{\lambda_2}$.

We organize our proof as a sequence of games:

Game*real*: This is a real threshold IBBE security game.

For $0 \le i \le q$, the Game*i* is defined as follows.

Game*i*: Let Ω denote the set of private keys which the adversary queries during the games. This game is a real IBBE security game with the two exceptions: (1) The challenge ciphertext will be a semi-functional ciphertext on the challenge set S^*. (2) The first *i* keys will be semi-functional private keys. The rest of keys in Ω will be normal.

Note: In $game_0$, the challenge ciphertext is semi-functional. In $game_q$, the challenge ciphertexts and all keys are semi-functional.

$Game_{final}$: This game is same with $Game_q$ except that the challenge ciphertext is a semi-functional encryption of random group element of G_1.

Lemma 2 Suppose that there exists an algorithm A such that $\mathrm{Adv}_{game_{real}} A - \mathrm{Adv}_{game_0} A = \varepsilon$. Then we can build an algorithm B with advantage ε in breaking Assumption 1.

Lemma 3 Suppose that there exists an algorithm A that makes at most q queries and such that $\mathrm{Adv}_{game_{k-1}} A - \mathrm{Adv}_{game_k} A = \varepsilon$ for $1 \le k \le q$. Then we can build an algorithm B with advantage ε in breaking Assumption 2.

Lemma 4 Suppose that there exists an algorithm A that makes at most q queries and such that $\mathrm{Adv}_{game_q} A - \mathrm{Adv}_{game_{final}} A = \varepsilon$. Then we can build an algorithm B with advantage ε in breaking Assumption 3.

By using the proof of Theorem 1 and techniques in [16], we can obtain the proof of these lemmas. For the concision, we omit them here. Then we have the following theorem.

Theorem 5 If Assumption 2, 3 and 4 hold, then our scheme is IND-ID-CPA secure.

Conclusions

Two new constructions of identity-based threshold broadcast encryption are proposed for ad hoc networks. In proposed schemes, the broadcaster can dynamically choose the set of recipients and the threshold value *t*. Both schemes have short ciphertexts, where the length of ciphertexts achieves O(*n*-*t*). In addition, we reduce their security to the decision *n*+1-BDHE problem and some static assumptions respectively.

Unfortunately, in our schemes, the total number of possible users must be fixed in the setup. It is an interesting problem to construct a scheme without the above constraints in the standard model.

Acknowledgement:

This work is supported in part by the Nature Science Foundation of China under grant (61100231, 60970119, 61100165), the National Basic Research Program of China(973) under grant 2007CB311201 and the Fundamental Research Funds for the Central Universities.

REFERENCES

[1] Fiat A., Naor M.. Broadcast Encryption. *Proc. of CRYPTO*, LNCS 773(1994), pp. 480-491.

[2] Ghodosi H., Pieprzyk J. and Safavi-Naini R.. Dynamic threshold cryptosystems: a new scheme in group oriented cryptography. *Proc. of Theory and Applications of Cryptology*, (1996), pp. 370-379.

[3] Shamir A.. Identity-based Cryptosystems and Signature Schemes. *Proc. of CRYPTO*, LNCS 196(1984), pp. 47–53.

[4] Boneh D. and Franklin M.. Identity-based encryption from the well pairing. *Proc. of CRYPTO*, LNCS 2193(2001), pp. 213-229, 2001.

[5] Boneh D. and Boyen X.. Efficient selective-id secure identity based encryption without random oracles. *Proc. of Eurocrypt*, LNCS 3027(2004), pp. 223-238, 2004.

[6] Cocks C.. An identity based encryption scheme based on quadratic residues. *Proc. of Cryptography and coding,* LNCS 2260(2001), pp. 360-363.

[7] Boneh D. and Katz J.. Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity-Based Encryption. *Proc. of CT-RSA*, LNCS 3376(2005), pp. 87-103.

[8] Canetti R., Halevi S., and Katz J.. Chosen-ciphertext security from identity-based encryption. *Proc. of Eurocrypt*, LNCS 3027(2004), pp. 207-222.

[9] Chattterjee S. and Sarkar P.. Generalization of the Selectve-ID Security Model for HIBE Protocols. *Proc. of PKC*, LNCS 3958(2006), pp. 241-256, 2006.

[10] Chai Z., Cao Z. and Zhou Y.. Efficient ID-based Broadcast Threshold Decryption in Ad Hoc Network. *Proc. of IMSCCS,* IEEE Computer Society(2006), 2, pp. 148-154.

[11] Daza V., Herranz J. and Morillo P.. CCA2-Secure Threshold Broadcast Encryption with Shorter Ciphertexts. *Proc. of ProvSec*, LNCS 4784(2007), pp. 35-50.

[12] Delerablee C. and Pointcheval D.. Dynamic Threshold Public-Key Encryption. *Proc. of CRYPTO*, LNCS 5157(2008), pp. 317-334.

[13] Zhang L., Hu Y. and Wu Q.. Identity-based threshold BE in the standard model. *KSII Trans. on internet and information systems*, Vol. 4(2010), NO. 3, pp.400-410.

[14] Zhang L., Hu Y. and Wu Q.. Adaptively Secure Identity-based Threshold Broadcast Encryption without Random Oracles. *AMR*, Vols. 143-144(2011), pp. 347-352.

[15] Waters B.. Dual system encryption: realizing fully secure ibe and hibe under simple assumptions. *Proc. of Crypto*, LNCS 5677(2009), pp. 619-636.

[16] Lewko A. and Waters B.. New Techniques for Dual System Encryption and Fully Secure HIBE with Short Ciphertexts. *Proc. of the 7th Theory of Cryptography Conference*(2010), pp. 455–479..

[17] Katz J., Sahai A. and Waters B.. Predicate encryption supporting disjunctions, polynomial equations, and inner products. *Proc. of Eurocypt*, LNCS 4965(2008), pp. 146-162.

***Authors**: prof. Leyou Zhang, Post Office Box 245, Department of Mathematics, Xidian University, NO.2, South Taibai Road, Xi'an, Shaanxi, 710071, China, Email: leyouzhang77@yahoo.com.cn. prof. Qing Wu, School of automation, Xi'an University of Posts and Telecommunications, Weiguo Road, Chang'an District,Xi'an, Shaanxi, 710121, China, Email: xidianwq@yahoo.com.cn. prof. Yupu Hu, School of Telecommunications Engineering, NO.2, South Taibai Road, Xi'an, Shaanxi, 710071, China, Email: xidianzly@163.com.*

The correspondence address is:

Post Office Box 245, Department of Mathematics, Xidian University, NO.2 South Taibai Road, Xi'an, Shaanxi, 710071, China.

Email: leyouzhang77@yahoo.com.cn.