

Attribute-based encryption with hidden threshold access structure

Fugeng Zeng^{1, 2*} Chunxiang Xu²

¹School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, 611731, China

²School of Science and Engineering, Qiongzhou University, Hainan 572000, China

Received 19 October 2014, www.cmnt.lv

Abstract

This paper proposes attribute-based encryption schemes in which threshold access structures are hidden. With these schemes, an encryptor can encrypt data with hidden attributes. After receiving the ciphertext from the encryptor, a decryptor first tests which block of ciphertext is associated with which attribute. Decryption will be successful if the attributes associated with the secret key of the decryptor satisfy the access structure associated with the encrypted data. The security of the proposed construction is proved in the selective model based on the decisional bilinear Diffie-Hellman assumption. The proposed scheme shows greater flexibility than other hidden access control encryption schemes.

Keywords: attribute-based encryption; hidden access structure; threshold

1 Introduction

Attribute-based encryption (ABE) is a promising and increasingly versatile paradigm. ABE was first introduced by Sahai and Waters [1] in the context of the generalization of identity-based encryption (IBE) called fuzzy IBE, which is an ABE that allows only a single threshold access structure. Two kinds of ABE were subsequently proposed: key-policy ABE (KP-ABE), in which a ciphertext is associated with a list of attributes and secret keys are associated with a decryption policy; and ciphertext-policy ABE (CP-ABE), in which attributes are associated with secret keys and access structures are associated with ciphertexts. Goyal et al. [2] was the first to construct the KP-ABE, which allows any monotone access structure. As access structures are described by attributes, the concept of CP-ABE is thus closely related to role-based access control. CP-ABE is more complex to design than KP-ABE because it requires both the encryptor and the key generalization center to satisfy the construction. Bethencourt et al. [3] presented the first CP-ABE system that supported an arbitrary monotone access structure; however, the security of their scheme was only proved in the generic group model, which does not comprise a standard number of theory assumptions.

In almost every ABE scheme, the access policy is sent together with the ciphertext, i.e., the scheme does not provide a hidden access structure. The approaches discussed so far require the access policy to be attached with the ciphertext such that the decryptor knows the policy and performs the decryption process. However, this approach sacrifices the anonymity of the receiver.

Hence, the list of intended receivers can be easily obtained by any intermediate user from the ciphertext policy. To solve this problem, Nishide et al. proposed two CP-ABE schemes with partially hidden ciphertext policies, implying that the possible values of each attribute in the system should be known to an encryptor in advance. In addition, the encryptor can hide a subset of possible values for each attribute in the ciphertext policy to be used for successful decryption [4]. However, the number of hidden attributes uses an AND-gate access policy. Thus far, ABE with a hidden access structure [5-6] is based on an AND-gate access policy.

We propose an ABE with a hidden threshold access structure (ABEHT), whose access policy is highly flexible. In addition, the security of our construction is proved in the selective model based on the decisional bilinear Diffie-Hellman (DBDH) assumption.

2 Preliminaries

We provide some preliminaries.

2.1 BILINEAR PAIRINGS [7]

Let G_0 and G_1 be the cyclic groups of prime order p with a multiplicative group action, and let g be a generator of G_0 . Let $e : G_0 \times G_0 \rightarrow G_1$ be a map with the following properties:

- (1) Bilinearity. $e(g^a, g^b) = e(g, g)^{ab} \forall a, b \in \mathbb{Z}_p^*$
- (2) Non-degeneracy. $e(g, g) \neq 1$.

* Corresponding author's E-mail: zengfugeng@gmail.com

(3) Computability. An efficient algorithm exists to compute $e(u, v)$ for all $u, v \in G_0$.

2.2 DISCRETE LOGARITHM PROBLEM

Given two group elements g and h , find an integer $a \in \mathbb{Z}_p^*$ such that $h = g^a$ whenever such integer exists.

2.3 DBDH ASSUMPTION

The DBDH problem in G is a problem, given an input of a tuple $(g, g^a, g^b, g^c, Z) \in G^4 \times G_T$ to decide whether $Z = e(g, g)^{abc}$. Algorithm A has advantage ε in solving the DBDH problem in G if

$$|\Pr[A(g, g^a, g^b, g^c, e(g, g)^{abc}) = 0] - \Pr[A(g, g^a, g^b, g^c, e(g, g)^z) = 0]| \geq \varepsilon(k), \quad (1)$$

where $e(g, g)^z \in G_T \setminus \{Z = e(g, g)^{abc}\}$. We say that the DBDH assumption holds in G if no PPT algorithm has an advantage of at least ε in solving the DBDH problem in G [1].

2.4 SYNTAX OF ABEHT

Our ABEHT schemes consist of the following four algorithms.

Setup (1^k). This algorithm takes the security parameter K as input and generates a public key PK and a master secret key MK.

KeyGen (MK, S). This algorithm takes MK and an attribute list γ as input and generates a secret key SK_γ associated with γ .

Encrypt (PK, M, α). This algorithm takes PK, encrypts message M with α , and generates a ciphertext CT. The threshold access structure α is excluded in the ciphertext.

Decrypt (CT, SK_L). This algorithm involves two steps: first, the decryptor tests, which blocks of ciphertext are associated with which attributes; second, the algorithm takes CT and SK_γ associated with γ as inputs and returns the message M if γ and α have more than d overlap attributes.

2.5 SECURITY MODEL

We describe the security models for our ABEHT based on [1], and we use the following security game. An ABEHT scheme is selectively secure if no probabilistic polynomial-time adversary has non-negligible advantage in the following game.

Init: The adversary runs A and receives the challenge identity γ an n element set of members of \mathbb{Z}_p^* .

Setup: The challenger runs the setup phase of the algorithm and informs the adversary about the public parameters.

Phase 1: The adversary is allowed to issue queries for private keys for many identities α_j , where $\forall j, |\alpha_j \cap \gamma| < d$.

Challenge: The adversary submits two equal-length messages M_0 and M_1 . The challenger flips a random coin β and encrypts M_β with γ . The ciphertext is forwarded to the adversary.

Phase 2: Phase 1 is repeated.

Guess. The adversary outputs a guess β' of β . The advantage of adversary A in this game is defined as $\Pr[\beta = \beta'] - \frac{1}{2}$.

3 Our construction

Let G_1 be a bilinear group of prime order p , and let g be a generator of G_1 . Let $e: G_1 \times G_1 \rightarrow G_2$ denote the bilinear map. We restrict the encryption attributes to a length n for some fixed n .

We define $\Delta_{i,S}$ for $i \in \mathbb{Z}_p^*$ as a Lagrange coefficient and a set $S \in \mathbb{Z}_p^*$. Identities are sets of n elements of $\Delta_{i,S}(x) = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$. Alternatively, we

can describe an identity as a collection of n strings of arbitrary length and use a collision resistant hash function h to hash strings into members of \mathbb{Z}_p^* . Our construction is as follows:

Setup (n, d): First, choose $g_1 = g^\alpha$, $g_2 \in G_1$. Next, choose t_1, t_2, \dots, t_{n+1} uniformly at random from G_1 . Let N be the set $\{1, 2, \dots, n+1\}$. We define a

function T as $T(x) = g_2^{x^n} \prod_{i=1}^{n+1} t_i^{\Delta_{i,N}(x)}$. We can view T as

the function $T(x) = g_2^{x^n} g^{h(x)}$ for some n degree polynomial h . Choose z_1, z_2, z_3, y uniformly at random from \mathbb{Z}_p^* , $y_i = g^{z_i}$ $i \in \{1, 2, 3\}$, $Y = g^y$. Publish the public key as

$$PK = (g, g_1, g_2, y_1, y_2, y_3, Y, t_1, t_2, \dots, t_{n+1}), \quad (2)$$

and the private key as $MK = \{\alpha, y\}$.

Key Generation: To generate a private key for identity ω , randomly choose $d-1$ degree polynomial q such that $q(0) = \alpha$. Choose r_{1i}, r_{2i} uniformly at random from Z_p^* . The private key is as follows:

$$d = (\{d_{1i}, d_{2i}, d_{3i}, d_{4i}\}_{i \in \omega}, y) \\ = (\{g_2^{q(i)} T(i)^{r_{1i}} y_3^{r_{2i}}, g^{r_{1i} z_1 + r_{2i} z_2}, g^{r_{1i}}, g^{r_{2i}}\}_{i \in \omega}, y) \quad (3)$$

Encryption: Encryption with the public key ω' and message $M \in G_2$ is as follows:

First, choose random values s_1, s_2 . Then, express the ciphertext as

$$E = (c_1 = Y^{s_1}, c_2 = g^{s_2}, \{c_{3i} = T_i^{s_1} y_1^{s_2}\}_{i \in \omega'}, \\ c_4 = y_3^{s_1} y_2^{s_2}, c_5 = Me(g_1, g_2)^{s_1}). \quad (4)$$

Decryption: After receiving a ciphertext E, first verify the equation

$$e(g, T_i^{s_1} y_1^{s_2}) = e(g^{s_1}, T(i)) e(g^{s_2}, y_1). \quad (5)$$

We can observe that identity ω' is encrypted with a key for identity ω' , and we have a key for identity ω , where $|\omega' \cap \omega| \geq d$. Define

$$F_i = \frac{e(d_{3i}^y, c_{3i}) e(d_{4i}^y, c_4)}{e(d_{1i}, c_1) e(d_{2i}^y, c_2)} = \frac{1}{e(g_2^{q(i)}, Y^{s_1})}. \quad (6)$$

Such that

$$M = c_5 \prod_{i \in S} F_i^{\Delta_{i,S}(0)/y}. \quad (7)$$

4 Proof of security

We prove that the security of our scheme in the selective ID model reduces to the hardness of the DBDH assumption.

Theorem 1: If an adversary breaks our scheme in the ABEHT game, then a simulator can be constructed to play the DBDH game with a non-negligible advantage.

Proof: Suppose the existence of a polynomial-time adversary A that can attack our scheme in the selective-ID model with advantage \mathcal{E} . We build a simulator B that can play the DBDH game with advantage $\mathcal{E}/2$.

The simulation is as follows: We first let the challenger set the groups G_1 and G_2 with an efficient bilinear map e and generator g . The challenger flips a fair binary coin β' outside the view of B. If $\beta' = 0$, then the challenger set $(A, B, C, Z) = (g^a, g^b, g^c, e(g, g)^{abc})$ otherwise, set $(A, B, C, Z) = (g^a, g^b, g^c, e(g, g)^z)$ for random a, b, c, z .

Init: B will run A and receive the challenge identity γ , an n element set of members of Z_p^* .

Setup: The simulator assigns the public parameters $g_1 = A$ and $g_2 = B$. It then chooses a random n degree polynomial $f(x)$ and calculates an n degree polynomial $u(x)$ such that $u(x) = -x^n$ for all $x \in \gamma$, where $u(x) \neq -x^n$ for some other x . Given that $-x^n$ and $u(x)$ are two n degree polynomials, they either agree on most n points or are the same polynomial. Our construction assures that $\forall u(x) = -x^n$ if and only if $x \in \gamma$. Then, for i from 1 to $n+1$, the simulator sets $t_i = g_2^{u(i)} g^{f(i)}$. Given that $f(x)$ is a random n degree polynomial, all t_i are chosen independently at random as in the construction and as our implicit choice. Choose z_1, z_2, z_3, y uniformly at random from Z_p^* , $y_i = g^{z_i}$, $i \in \{1, 2, 3\}$, $Y = g^y$.

Phase 1: A requests for private keys in which the identity set overlap between the identities for the requested keys and γ is less than d .

Suppose A requests a private key γ' . We first define three sets Φ, Φ', S in the following manner: let $\Phi = \gamma \cap \gamma'$, Φ' be any set such that $\Phi \subseteq \Phi' \subseteq \gamma$, $|\Phi'| = d-1$, and $S = \gamma' \setminus \{0\}$.

Next, we define the decryption key components d as $d = (\{d_{1i}, d_{2i}, d_{3i}, d_{4i}\}_{i \in \omega}, y) = (\{g_2^{q(i)} T(i)^{r_{1i}} y_3^{r_{2i}}, g^{r_{1i} z_1 + r_{2i} z_2}, g^{r_{1i}}, g^{r_{2i}}\}_{i \in \omega}, y)$, where $q(i), r_{1i}, r_{2i}$ is chosen uniformly at random from Z_p^* .

The simulator also needs to calculate the decryption key values for all $i \in \gamma' - \Phi'$. We calculate these points to be consistent with our implicit choice of $q(x)$. The key components are calculated as

$$d_{1i} = g_2^{q(i)} T(i)^{r_{1i}} y_3^{r_{2i}} = \left(\prod_{j \in \Phi'} g_2^{q(i) \Delta_{i,S}(j)} \right) g_2^{q(i) \Delta_{i,S}(0)} \\ (g_2^{i^n + u(i)} \cdot g^{f(i)})^{(r_{1i} - \frac{a}{i^n + u(i)}) \Delta_{i,S}(0)} y_3^{r_{2i}} = \left(\prod_{j \in \Phi'} g_2^{q(i) \Delta_{i,S}(j)} \right) \\ (g_1^{\frac{-f(i)}{i^n + u(i)}} \cdot (g_2^{i^n + u(i)} \cdot g^{f(i)})^{r_{1i}})^{\Delta_{i,S}(0)} y_3^{r_{2i}}, \quad (8)$$

where $r_{1i} = (r_{1i} - \frac{a}{i^n + u(i)}) \Delta_{i,S}(0)$, $r_{2i} = r_{2i}$.

Additionally, we have

$$d_{2i} = g^{r_{i1}z_1+r_{i2}z_2} = (g_1^{i^n+u(i)} g^{r_{i1}})^{\Delta_{i,S}(0)z_1} g^{r_{i2}z_2},$$

$$d_{3i} = g^{r_{i1}} = (g_1^{i^n+u(i)} g^{r_{i1}})^{\Delta_{i,S}(0)}, d_{4i} = g^{r_{i2}}. \quad (9)$$

Challenge: Adversary A submits two challenge messages M_1 and M_0 to the simulator. The simulator flips a fair binary coin β and returns an encryption of M_β . The ciphertext is output as follows: let $s_1 = c$; a random value s_2 is chosen. Then, the ciphertext is expressed as $E = (c_1 = C^y, c_2 = g^{s_2}, \{c_{3i} = C^{f(i)} y_1^{s_2}\}_{i \in \omega}, c_4 = C^{z_3} y_2^{s_2}, c_5 = M_\beta Z)$. If $\beta = 0$, then $Z = e(g, g)^{abc}$. Otherwise, if $\beta = 1$, then $Z = e(g, g)^z$.

Phase 2: The simulator acts exactly as it did in Phase 1.

Guess. The overall advantage of the simulator in the

DBDH game is $\Pr[\beta = \beta'] - \frac{1}{2}$.

References

[1] Sahai A, B.Waters 2005 Fuzzy identity-based encryption *Advances in Cryptology-EUROCRYPT* 457-73
 [2] Goyal V, Pandey O, Sahai A, Waters B.2006 Attribute based encryption for fine-grained access control of encrypted data *ACM CCS* 89-98
 [3] Bethencourt J, Sahai A, Waters B 2007 Ciphertext-policy attribute-based encryption *IEEE Symposium on Security and Privacy* 321-34
 [4] Nishide T, Yoneyama K, Ohta K 2008 Attribute-based encryption with partially hidden encryptor-specified access structures *Applied cryptography and network security* 111-29

According to the law of total probability [8],

$$\Pr[\beta = \beta'] - \frac{1}{2} = \Pr[\beta = \beta' | \beta=0] \Pr[\beta = 0] + \Pr[\beta = \beta' | \beta=1] \Pr[\beta = 1] - \frac{1}{2} = (\frac{1}{2} + \varepsilon) \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} - \frac{1}{2} = \frac{\varepsilon}{2}.$$

(10)

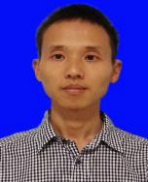

5 Conclusion

We propose ABE schemes in which threshold access structures are hidden and the access policy is highly flexible. We also prove the security of our construction through the selective model based on the DBDH assumption.

Acknowledgment

This work is supported by the Science and Technology on Communication Security Laboratory Foundation (Grant No. 9140C110301110C1103) and the National Natural Science Foundation of China (No. 61370203).

[5] Doshi N, Jinwala D 2012 Hidden access structure ciphertext policy attribute based encryption with constant length ciphertext *Advanced Computing, Networking and Security* 515-23
 [6] Rao Y S, Dutta R 2013 Recipient Anonymous Ciphertext-Policy Attribute Based Encryption *Information Systems Security* 329-44
 [7] Boneh D, Waters B 2007 Conjunctive, subset, and range queries on encrypted data *TCC 2007 LNCS* 4392 535-54
 [8] Kenneth B 2008 *Introduction to probability* R.CRC Press 179

| Authors | |
|---|--|
|  | <p>Fugeng Zeng ,1983.12, Chengdu ,Sichuan Province, P.R. China</p> <p>Current position, grades: Ph.D. degree candidate in information security at University of Electronic Science Technology of China (UESTC); Associate Professor at School of Science and Engineering, Qiongzhou University</p> <p>University studies: B.Sc. degree in mathematics and applied mathematics at Qiongzhou University in 2005, PR China and received M.Sc. degree in pure mathematics at Hainan Normal University in 2008. He is a Ph.D. degree candidate in information security at University of Electronic Science Technology of China (UESTC).</p> <p>Scientific interest: cryptography, network security and cloud computing security.</p> <p>Publications: more than 6 papers published in various journals.</p> <p>Experience: He has teaching experience of 7 years.</p> |
|  | <p>Chunxiang Xu,1965.01, Chengdu ,Sichuan Province, P.R. China</p> <p>Current position, grades: professor at University of Electronic Science Technology of China (UESTC).</p> <p>University studies: B.Sc., M.Sc. and Ph.D. degrees Xidian University, in 1985, 1988 and 2004 respectively, PR China.</p> <p>Scientific interest: cryptography, network security and cloud computing security.</p> <p>Publications: more than 70 papers published in various journals.</p> <p>Experience: She has teaching experience of 21 years, has completed more than eight scientific research projects.</p> |