Ciphertext-Policy Attribute Based Encryption with Large Attribute Universe

Siyu Xiao, Aijun Ge, Fushan Wei and Chuangui Ma

Abstract Ciphertext-policy attribute-based encryption(CP-ABE) has become a crucial technical for cloud computing in that it enables one to share data with users under the access policy defined by himself. Generally, the universe of attributes is not fixed before the system setup in practice. So in this paper, we propose a CP-ABE scheme with large attribute universe based on the scheme presented by Chen et al. The number of attributes is independent of the public parameter in our scheme, and it inherents the excellent properties of both constant ciphertext and constant computation cost.

1 Introduction

With the development of cloud computing technology, more and more clients are willing to store and distribute their large scale of data on a cloud server. Meanwhile, there has already emerged many well-known service providers such as Google storage cloud, Amazon' S3 and so on. Despite the fact that such cloud service offers great convenience to users, it has indeed introduced some non-negligible threats. For example, cloud storage system is fully public to which everyone can have access, so the data privacy seems impossible in this way.

One method to figure this out is encrypting the data before it being outsourced to the cloud. Thus, malicious clients won't gain any useful information about the data even if they corrupt the service provider. Nevertheless, this will make it diffi-

Siyu Xiao, Aijun Ge, Fushan Wei
State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, China
e-mail: siyuxiao32@163.com, geaijun@163.com, weifs831020@163.com

Chuangui Ma
Department of Basic Courses, Army Aviation Institute, Beijing, China
State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, China
e-mail: chuanguima@sina.com

F. Xhafa et al. (eds.), *Advances on P2P, Parallel, Grid, Cloud and Internet Computing*, Lecture Notes on Data Engineering and Communications Technologies 1, DOI 10.1007/978-3-319-49109-7_11

cult for users to selectively share their encrypted data under a fine-grained policy. Suppose at some point, a user wants to distribute a sensitive encrypted document, and only the ”women” in ”finance department” of her company have the ability to decrypt. The concept introduced by [1] called Attribute-Based Encryption(ABE) makes some important step to solve this problem. In an ABE scheme, each user’s key and each ciphertext are associated with a set of attributes respectively. If and only if there exists a match between the user’s attributes and the ciphertext’s attributes, he can have the ability to decrypt. Later, many researchers make further efforts to achieve more fine-grained access policy.

ABE can be divided into Ciphertext-Policy ABE(CP-ABE) and Key-Policy ABE(KP-ABE). In CP-ABE scheme, the secret key is associated with a set of attributes while the ciphertext is associated with an access policy. A user then can have the ability to decrypt a ciphertext if and only if his attributes related to the secret key satisfy the policy . In KP-ABE scheme, the ciphertext is associated with a set of attributes and the secret key is associated with an access policy. A user then can have the ability to decrypt a given ciphertext if and only if the underlying set of attributes related to the ciphertext satisfies the policy. In this paper, we mainly consider CP-ABE in which data owners can decide whether or not one have the authority to share his data. [2] proposed a CP-ABE with constant-size ciphertext and constant computation cost, but their scheme is established on small attribute universe. That is to say, the number of attributes is fixed before the system setup, which is not satisfying current tendency, for example, in big data sharing, where the user authority is decided by his attributes. In this paper, we aim to figure out a solution on large attribute universe.

When it comes to the security of ABE, the most important thing we consider is to resist collusion. A group of members cannot decrypt a ciphertext if neither of them can. For example, if an access policy associated with a ciphertext is ”cryptography AND doctor”, then a cryptography master and a economics doctor cannot decrypt this ciphertext even though they can get attributes ”cryptography” and ”doctor” via collusion. How to avoid collusion attacks is always a hot research area, and also a difficult research area.

Our Results. We propose a CP-ABE scheme supporting large attribute universe. In this scheme, the number of attributes is independent of the public parameter as long as each user’s personal number of attributes is less than the upper bound. Furthermore, it inherits the excellent properties in [2] and has constant ciphertext length as well as consant computation cost. The security of our scheme can be proved under the n-BDHE assumption.

Related Work. Attribute-Based Encryption(ABE) is actually an extension of Identity-Based Encryption(IBE) to improve the flexibility of users sharing their data. It is first introduced by [1] and be further classified into CP-ABE and KP-ABE by [3]. The first KP-ABE scheme proposed by [3] achieves monotonic access policy. Later, [4] propose another KP-ABE scheme supporting non-monotone key polices to increase the expressiveness. In 2007, [5] present the first construction of CP-ABE realizing tree-based access policy, but its security is proved in generic group models. Then [6] propose a CP-ABE scheme with security in the standard model, however, it can just support AND gate operation. Until now, research on realizing fine-grained access policy ABE with security under the standard model is still a hot area, also a challenging area.

Besides the expressiveness and security, there also exists another point deserved our attention. That is the computation cost of the scheme, both in encryption and decryption. [7] initiate the study of CP-ABE with constant-size ciphertext but it supports just simple AND gate operation. Subsequent results [2] and [8] are the same. Afterwards, [9] propose a threshold CP-ABE scheme with constant-size ciphertext and can be extended to realize resistance against Chosen-Ciphertext-Attack(CCA). Fully secure threshold CP-ABE with constant-size ciphertext is achieved by [10] via a universal transformation from Inner Product Encryption(IPE) and can be further extended to a large attribute universe scheme. The only flaw is the foundation of composite-order bilinear groups. [11] propose a CP-ABE scheme with constant-size keys and expressive access policy so that lightweight devices can be used as storage for decryption keys. In this paper, motivated by all the existing results, we propose a construction of CP-ABE with large attribute universe based on prime-order bilinear groups, which inherits the good properties of constant-size ciphertext in [2] at the same time.

Organization. The remainder of the paper is organized as follows. In section 2, some preliminaries are reviewed including the definition of bilinear group and the syntax of CP-ABE. Next, we present our concrete scheme and give necessary proof of the security. Finally, we give conclusion in section 4.

2 Preliminary

2.1 Bilinear Group

Let $\mathscr{G}$ be an algorithm that take s input a security parameter k and outputs a tuple (p, G, G_T, g, e), where G and G_T are cyclic groups of order p for some large prime p, g is a generator of G. The map $e : G \times G \to G_T$ satisfies the following properties:
1. Bilinear: $e(u^a, v^b) = e(u, v)^{ab}$ for all $u, v \in G$ and $a, b \in Z_p$.
2. Non-degenerate: $e(g, g) \neq 1$.

We say G generated in this way is a bilinear group if the group operation in G and the map e are efficiently computable.

Let G be a bilinear map of prime order p defined above, g, h be two independent generators of G. Denote $\overrightarrow{y}_{g,\alpha,n} = (g_1, g_2, \dots, g_n, g_{n+2}, \dots, g_{2n}) \in G^{2n-1}$, where $g_i = g^{\alpha^i}$. For an adversary $\mathscr{A}$, we define $Adv_{G,\mathscr{A}}^{\text{n}-\text{BDHE}}(k)$ as follows:

$$|Pr[\mathscr{A}(g, h, \overrightarrow{y}_{g,\alpha,n}, e(g_{n+1}, h)) = 0] - Pr[\mathscr{A}(g, h, \overrightarrow{y}_{g,\alpha,n}, Z) = 0]|$$

where $Z \in G_T$ and $\alpha \in Z_p$ are all randomly chosen. We say that the decision n-BDHE assumption holds in G if $Adv_{G,\mathscr{A}}^{\text{n-BDHE}}(k)$ is negligible for arbitrary polynomial adversary $\mathscr{A}$.

The security proof of our scheme is based on the above decision n-BDHE assumption.

2.2 Ciphertext Policy ABE

A CP-ABE system consists of four probabilistic polynomial-time algorithms **Setup**, **KeyGen**, **Encrypt**, **Decrypt** as follows:

Setup(1^k): Takes input the security parameter k and outputs the system public parameter PP and master private key MK. PP is distributed to users while MK kept secret.
KeyGen(PP, MK, S): Takes input the private key MK and a attribute set S, outputs SK_S as the secret key for the user associated with S.
Encrypt(PP, M, Ω): Takes input a message M under the access policy Ω, the algorithm outputs a ciphertext C_Ω using the public parameter PP.
Decrypt(PP, SK_S, C_Ω): Takes input the users' secret key SK_S and ciphertext C_Ω associated with access policy Ω, outputs the message M if S satisfies Ω and $\perp$ otherwise.

For an access policy Ω, we mean it is a rule that returns either 0 or 1 given a set of attributes S. If S satisfies Ω, it will return 1. Otherwise, it will return 0. Actually, arbitrary boolean functions, threshold trees can be an access policy. In this paper, we mainly consider AND gate.

2.2.1 Security Model

The selective security model against chosen plaintext attacks for CP-ABE can be defined via the following IND-sCP-CPA game. In this game, a challenge access policy Ω is supposed to be chosen before **Setup** and the adversary is allowed to query keys for any attribute set S that is not satisfied by Ω.
1). The adversary $\mathscr{A}$ chooses a challenge access policy Ω and gives it to the challenger $\mathscr{C}$.
2). $\mathscr{C}$ runs the algorithm **Setup** to generates public parameter PP and master secret key MK. Then it gives PP to $\mathscr{A}$.
3). $\mathscr{A}$ adaptively queries keys for any attribute set S that is not satisfied by Ω. $\mathscr{C}$ runs **KeyGen**(PP, MK, S) and returns SK_S to the adversary.
4). At some point, $\mathscr{A}$ outputs two equal length messages M_0 and M_1. The challenger randomly chooses a bit $b \in \{0,1\}$ and computes **Encrypt**(PP, M_b, Ω). It then sends CT_Ω to the adversary $\mathscr{A}$.

5). $\mathscr{A}$ can additionally make key queries for attribute sets not satisfying Ω and $\mathscr{C}$ responds the same as above.
6). $\mathscr{A}$ outputs a guess bit $b' \in \{0,1\}$ and wins the game if $b' = b$.

The advantage of an adversary in the above game is defined as follows:

$$Adv_{\mathscr{A}}^{\mathrm{IND-sCP-CPA}}(k) = |Pr[b' = b] - \frac{1}{2}|$$

Definition 1. A CP-ABE scheme is said to be IND-sCP-CPA secure if no probabilistic polynomial-time adversary can have non-negligible advantage in the above game.

3 Our Scheme

In this paper, the access policy we mainly consider is AND gate $\bigwedge_{A_i \in U} A_i$. Actually, if denoting $\neg A_i$ as an individual attribute in the system, NOT gate is supported as well. Here, we just omit this part for simplicity.

Setup(k, n): Takes as input the security parameter k and the maximum number of attributes n in the system, the algorithm first runs $\mathscr{G}(1^k)$ and generates bilinear maps (p, G, G_T, g, e). Then it randomly chooses two polynomials $p_1(x)$, $p_2(x)$ in Z_p with order $n-1$, and sets $R_i = g^{-p_1(r_i)}$, $U_i = e(g^{p_2(r_i)}, g)$ where $r_i \in Z_p$ are randomly chosen for $i = 1, \ldots, n$.

The public parameter is

$$PP = \{g, < r_i, R_i, U_i >_{i=1,\ldots,n}\}$$

The private key is

$$MK = \{p_1(x), p_2(x)\}.$$

KeyGen(PP, MK, S): Takes an attribute set S as input, the algorithm randomly chooses $V \in G$, and computes $\sigma_j = g^{p_2(j)} V^{p_1(j)}$ for $j \in S$.

The secret key for the user is $SK_S = \{V, \{\sigma_j\}_{j \in S}\}$.

Encrypt(PP, M, Ω): The encryption algorithm encrypts a message $M \in G_T$ under the AND policy $W = \bigwedge_{j \in \Omega} j$. It chooses random element $t \in Z_p$, then computes $C_0 = M \cdot (\prod_{j \in \Omega} U_j)^t, C_1 = (\prod_{j \in \Omega} R_j)^t, C_2 = g^t$. Where $U_j = e(g,g)^{p_2(j)}$ and $R_j = g^{-p_1(j)}$ for $j \in \Omega$ can be interpolation calculated using the public parameter.

The ciphertext for message M is $CT_\Omega = \{\Omega, C_0, C_1, C_2\}$.

Decrypt(PP, SK_S, CT_Ω): The decryption algorithm first checks whether $\Omega \subseteq S$. If not, return $\perp$. Otherwise, computes $\sigma = \prod\limits_{j\in\Omega} \sigma_j$ and outputs $M = \frac{C_0}{e(V,C_1)\cdot e(\sigma,C_2)}$ as the plaintext.

Theorem 1. *Suppose the decisional n-BDHE assumption holds in G. Then no polynomial time adversary can win the IND-sCP-CPA game defined in section 2.2 with non-negligible probability.*

Proof. Our proof of the security is almost the same with that of [2] except some little difference in secret key generation.

Suppose there exists a simulator $\mathscr{S}$ with n-BDHE inputs $(g, g^s, \overrightarrow{y}_{g,\alpha,n}, T)$, then $\mathscr{S}$ can simulate the IND-sCP-CPA game via following steps:

Initiation. The adversary $\mathscr{A}$ sends $\mathscr{S}$ a challenge access policy $\mathbb{W} = \bigwedge\limits_{i\in\Omega} i$.

Setup. The simulator randomly chooses $i^* \in \Omega$ and random elements $r_k, a_k \in Z_p$, $k = 1,\ldots,n$. Then it computes

$$(R_{i^*}, U_{i^*}) = (g^{r_{i^*}}(\prod_{k\in\Omega,k\neq i^*} g_{n+1-k}), e(g,g)^{a_{i^*}} e(g,g)^{\alpha^{n+1}})$$

For $i \in \Omega \setminus \{i^*\}$

$$(R_i, U_i) = (g^{r_i} g_{n+1-i}^{-1}, e(g,g)^{a_i})$$

Then $n - |\Omega|$ other random elements are chosen and for every element i in it, computes

$$(R_i, U_i) = (g^{r_i}, e(g,g)^{a_i})$$

Let U denotes all the attributes i mentioned above and sends $\mathscr{A}$ the public parameter $< i, R_i, U_i >_{i\in U} = < i, g^{-p_1(i)}, e(g^{p_2(i)}, g) >_{i\in U}$.

Key Queries. The adversary can query keys for attribute set $w(\Omega \subsetneq w)$. The simulator chooses $i' \in \Omega \setminus w$ and random $r \in Z_p$, computes $V = g_{i'} g^r$.

For attribute in U, just computes $\sigma_i = g^{p_2(i)} V^{p_1(i)}$.

For attribute not in U, the secret key can be computed utilizing interpolation calculation $\sigma_i = g^{\sum\limits_{j\in U} l_j(i) p_2(j)} V^{\sum\limits_{j\in U} l_j(i) p_1(j)} = \prod\limits_{j\in U} (g^{p_2(j)} V^{p_1(j)})^{l_j(i)} = \prod\limits_{j\in U} \sigma_j^{l_i(j)}$, where $l_j(i) = \prod\limits_{k\in U, k\neq j} \frac{i-k}{j-k}$.

Challenge. At some point, $\mathscr{A}$ outputs two equal length messages M_0 and M_1, the simulator chooses random bit $b \in \{0,1\}$ and computes

$$CT = (C_0 = M_b \cdot T e(g, g^s)^{a_\Omega}, C_1 = g^{s r_\Omega}, C_2 = g^s)$$

where $a_\Omega = \sum\limits_{i\in\Omega} a_i$, $r_\Omega = -\sum\limits_{i\in\Omega} r_i$.

Guess. Finally, if $\mathscr{A}$ guess $b' = b$, $\mathscr{S}$ outputs 0; otherwise, he outputs 1.

We can known if $T = e(g_{n+1}, g^s)$, CT is a valid encryption of message M_b; otherwise, it's a ciphertext for a random message. Thus, if the adversary wins the game with probability ε, then the simulator will attack the problem of n-BDHE with probability $1/2\varepsilon$.

4 Conclusion and Future Work

In this work, we construct a CP-ABE scheme with large attribute universe based on the results of [2]. The number of attributes in the proposed system is independent of the public parameter. That is to say, once any user gains a new attribute, he can add it to the system as long as his personal number of attributes less than the upper bound. It is crucial in cloud storage system for not necessary to fix how many attributes all together at the beginning, thus is more flexible. Though the added payment are just two interpolation operations for every encryption, our scheme only supports a restricted access policy, which is AND gate. How to achieve ABE with more expressive access policy with large attribute universe while maintaining constant-size ciphertext is what we will continue to investigate in the future.

Acknowledgements The authors would like to thank the anonymous referees for their helpful comments. This work is supported by the National Natural Science Foundation of China (Nos. 61309016, 61379150,61602512).

References

1. Sahai A. and Waters B.: Fuzzy identity based encryption. In: Proc. Advances in Cryptology-Eurocrypt, pp.457-473(2005)
2. Chen C., Zhang Z., and Feng D.: Efficient ciphertext-policy attribute-based encryption with constant-size ciphertext and constant computation-cost. In: Proc. ProveSec'11, pp.84-101(2011)
3. Goyal V., Pandey O., Sahai A. and Waters B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Proc. CCS'06, pp.89-98(2006)
4. Ostrovsky R., Sahai A. and Waters B.: Attribute-based encryption with nonmonotonic access structures. In: Proc. ACM Conference on Computer and Communication Security, pp.195-203(2007)
5. Bethencourt J., Sahai A. and Waters B.: Ciphertext-policy attribute-based encryption. In: Proc. IEEE Symposium on Security and Privacy, pp.321-334(2007)
6. Cheung L. and Newport C.: Provably secure ciphertext policy abe. In: Proc. ACM Conference on Computer and Communication Security, pp.456-465(2007)
7. Emura K., Miyaji A., Nomura A., et al.: A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. In: Proc. ISPEC'09, pp.13-23(2009)
8. Zhou Z., and Huang D.: On efficient ciphertext-policy attribute-based encryption and broadcast encryption. In: Proc. CCS'10, pp.753-755(2010)
9. Ge A., Zhang R., Chen C., Ma C.and Zhang,Z.: Threshold ciphertext-policy attribute-based encryption with constant-size ciphertexts. In: Proc. ACISP'12, pp.336-349(2012)

10. Chen C., Chen J., Lim H., et al.: Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures. In: Proc. CT-RSA'13, pp.50-67(2013)
11. Guo F., Mu Y., Susilo W., Wong D.and Varadharajan,V.: CP-ABE with constant-size keys for lightweight devices. In: IEEE Trans. Inf. Forensics Security, vol.9, no.5, pp.763-771(2014)