On Efficient Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption

[Extended Abstract] *

Zhibin Zhou
Arizona State University
zhibin.zhou@asu.edu

Dijiang Huang
Arizona State University
dijiang@asu.edu

ABSTRACT

Existing CP-ABE schemes incur very large ciphertext size, which increases linearly with respect to the number of attributes in the access policy. Large ciphertext prevents CP-ABE from being adopted in the communication constrained environments. In this paper, we proposed a new construction of CP-ABE, named Constant-size CP-ABE (denoted as CCP-ABE) that significantly reduces the ciphertext to a constant size for an AND gate access policy with any given number of attributes. Each ciphertext in CCP-ABE requires only 2 elements on a bilinear group.

Based on CCP-ABE, we further proposed an Attribute Based Broadcast Encryption (ABBE) scheme. Compared to existing Broadcast Encryption (BE) schemes, ABBE is more flexible because a broadcasted message can be encrypted by an expressive access policy, either with or without explicit specifying the receivers. Moreover, ABBE significantly reduces the storage and communication overhead to the order of $O(\log N)$, where N is the system size.

Categories and Subject Descriptors: E.3 [DATA ENCRYPTION]: Public key cryptosystems

General Terms: Security.

Keywords: Attribute-based Encryption, Broadcast Encryption.

1. INTRODUCTION

Research in Ciphtertext Policy Attribute-Based Encryption (CP-ABE) has been a very active area in recent years [1, 4, 3, 5]. Under the construction of CP-ABE, an attribute is a descriptive string assigned to (or associated with) an entity and each entity may be tagged with multiple attributes. Many entities may share common attributes, which allow message encryptors to specify a data access policy by composing multiple attributes through logical operators such as "AND", "OR", etc. To decrypt the message, the decryptor's attributes need to satisfy the access policy.

Apart from the promising features provided by CP-ABE solutions, there is a major problem of the existing CP-ABE schemes, which usually incur large, linearly increasing ciphertext. In the CP-ABE schemes reported in [1, 3, 5], the size of a ciphertext increases linearly with respect to the number of included attributes. For example, the message size in BSW CP-ABE [1] starts at about 630 bytes, and each additional attribute adds about 250-300 bytes.

In this paper, we propose a novel CP-ABE construction, named *Constant-size Ciphertext Policy Attribute Based Encryption* (CCP-ABE), which incurs constant-size of ciphertext, regardless of the number of attributes in a logical AND data access policy with wildcards. Besides the encrypted message and encoded access policy, each ciphertext only requires 2 bilinear group elements, which are bounded by 300 bytes in total.

Based on presented CCP-ABE, we further provide a new construction named as *Attribute Based Broadcast Encryption* (ABBE) that supports efficient Broadcast Encryption (BE). In existing BE schemes, e.g., [2], a broadcaster encrypts a message for an specified set of receivers who are listening on a broadcast channel. Each receiver in the specified set can decrypt the message while all other receivers that are not in the specified set cannot decrypt even though they collude together. However, in a system with large number of users, identifying every decryptor may be impractical. For example, to broadcast a message to all Computer Science students, the encryptor needs to query a central directory to get the contact information from every CS student in the roaster, in which the operation could be very expensive and time consuming. Using ABBE, an encryptor has the flexibility to encrypt the broadcasted data using CCP-ABE, either with or without the information of each intended receiver. ABBE also significantly reduces the storage overhead compared to many existing BE schemes. For example, in BGW scheme [2], the public key size is $O(N)$ or $O(N^{1/2})$, where N is the number of users in the system. ABBE addresses this key storage overhead problem by optimizing the organization of attribute hierarchy to minimize the storage requirement for each user to $O(\log N + m)$, where m is a constant number and $m \ll N$.

2. BACKGROUND AND MODELS

Bilinear Pairing is a bilinear map function $e : \mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1$, where $\mathbb{G}_0$ and $\mathbb{G}_1$ are two multiplicative cyclic groups with large prime order p. The Discrete Logarithm Problem (DLP) on both $\mathbb{G}_0$ and $\mathbb{G}_1$ is hard. One of the pairing properties is *Bilinearity*: $e(P^a, Q^b) = e(P, Q)^{ab}$, $\forall P, Q \in \mathbb{G}_0, \forall a, b \in \mathbb{Z}_p^*$.

Decisional K-BDHE The decisional K-BDHE assumption is said to be hold in $\mathbb{G}_0$ if there is no probabilistic polynomial time adversary who is able to distinguish the following 2

*A full version of this paper is available at http://eprint.iacr.org/2010/395

CCS'10, October 4–8, 2010, Chicago, Illinois, USA.
ACM 978-1-4503-0244-9/10/10.

tuples:

$$< h, g, Y_{g,\alpha,K}, e(g,h)^{\alpha^{(K+1)}} >, < h, g, Y_{g,\alpha,K}, e(g,h)^{R} >$$

with non-negligible advantage, where $\alpha, R \in \mathbb{Z}_p$ and $g, h \in \mathbb{G}_0$ are chosen independently and uniformly at random and

$$Y_{g,\alpha,K} = \{g^{\alpha}, g^{(\alpha^2)}, \cdots, g^{\alpha^K}, g^{\alpha^{K+2}}, \cdots, g^{\alpha^{2K}}\}.$$

Let $U = \{A_1, A_2, \cdots, A_k\}$ be the *Universe* of attributes in the system. Each A_i has three values: $\{A_i^+, A_i^-, A_i^*\}$. When a user u joins the system, u is tagged with an attribute list defined as follows:

DEFINITION 1. *A user's attribute list is defined as* $L = \{A_1^{+/-}, A_2^{+/-}, \ldots, A_k^{+/-}\}$, *where* $A_i^{+/-} \in \{A_i^+, A_i^-\}$ *and* k *is the number of attributes in the universe.* $L = L^+ \cup L^-$. $L^+ = \{A_i^+ | \forall i \in \{1 \cdots k\}\}$ *and* $L^- = \{A_i^- | \forall i \in \{1 \cdots k\}\}$. *Also, we have* $L^+ \bigcap L^- = \emptyset$. □

Intuitively, A_i^+ denotes the user has A_i; A_i^- denotes the user does not have A_i or A_i is not a proper attribute of this user. For example, suppose $U = \{A_1 = \text{CS}, A_2 = \text{EE}, A_3 = \text{Faculty}, A_4 = \text{Student}\}$. Alice is a student in CS department; Bob is a faculty in EE department; Carol is a faculty holding a joint position in EE and CS department. Their attribute lists are illustrated in the following table:

Attributes	A_1	A_2	A_3	A_4
Description	CS	EE	Faculty	Student
Alice	A_1^+	A_2^-	A_3^-	A_4^+
Bob	A_1^-	A_2^+	A_3^+	A_4^-
Carol	A_1^+	A_2^+	A_3^+	A_4^-

DEFINITION 2. *Let* $W = \{A_1, A_2, \cdots, A_k\}$ *be an AND-gate access policy, where* $A_i \in \{A_i^+, A_i^-, A_i^*\}$. *We use the notation* $L \models W$ *to denote that the attribute list* L *of a user satisfies* W, *as:*

$$L \models W \Longleftrightarrow W \subset L \bigcup \{A_1^*, A_2^*, \cdots A_k^*, \}.$$

□

3. CONSTANT CP-ABE

Setup(k): Assuming there are k attributes $\{A_1, A_2, \cdots, A_k\}$ in the system, we have $K = 3k$ attributes values since each attribute A_i has 3 values: $\{A_i^+, A_i^-, A_i^*\}$. For ease of presentation, we map $\{A_1^+, A_2^+, \cdots, A_k^+\}$ to $\{1, \cdots, k\}$, $\{A_1^-, A_2^-, \cdots, A_k^-\}$ to $\{k+1, \cdots, 2k\}$ and $\{A_1^*, A_2^*, \cdots, A_k^*\}$ to $\{2k+1, \cdots, 3k\}$.

Let $\mathbb{G}_0$ be the bilinear group of prime order p. Trusted Authority (TA) first picks a random generator $g \in \mathbb{G}_0$ and a random $\alpha \in \mathbb{Z}_p$. It computes $g_i = g^{(\alpha^i)}$ for $i = 1, 2, \cdots, K, K+2, \cdots, 2K$ where $K = 3k$. Next, TA picks a random $\gamma \in \mathbb{Z}_p$ and sets $v = g^{\gamma} \in \mathbb{G}_0$. The public key is: $PK = (g, g_1, \ldots, g_K, g_{K+2}, \ldots, g_{2K}, v) \in \mathbb{G}_0^{2K+1}$.

The master key $MK = \{\gamma, \alpha\}$ is guarded by the TA.

Key Generation :Each user u is tagged with the attribute list $L_u = L_u^+ \cup L_u^-$ when joining the system. We have $L_u^+ \subset \{1, \cdots, k\}$, $L_u^- \subset \{k+1, \cdots, 2k\}$. We also have $L^* = \{2k+1, \cdots, 3k\}$. The TA first selects k random numbers $\{r_1, r_2, \cdots, r_k\}$ from $\mathbb{Z}_p$ and calculate $r = \sum_{i=1}^{k} r_i$.

The TA computes $D = g^{\gamma r} = v^r$. For every $i \in L_u^+$, TA calculates $D_i = g^{\gamma(\alpha^i + r_{i'})}$ where $i' = i$; for every $i \in L_u^-$, TA calculates $D_i = g^{\gamma(\alpha^i + r_{i'})}$ where $i' = i - k$; for every $i \in L^*$, TA calculates $F_i = g^{\gamma(\alpha^i + r_{i'})}$ where $i' = i - 2k$.

The private key for user u is computed as:

$$SK_u = (D,\ \{D_i | \forall i \in L_u^+\},\ \{D_i | \forall i \in L_u^-\},\ \{F_i | \forall i \in L^*\}).$$

Encryption: The encrypter picks a random t in $\mathbb{Z}_p$ and sets the one-time symmetric encryption key $Key = e(g_K, g_1)^{kt}$. Suppose AND-gate policy is W with k attributes. Each attribute is either positive/negative or wildcards.

The encryptor first encrypts the message using symmetric key Key as $\{M\}_{Key}$. The encryptor also sets $C_0 = g^t$. Then, it calculates $C_1 = (v \prod_{j \in W} g_{K+1-j})^t$. The ciphertext is:

$$\begin{aligned} CT &= (W, \{M\}_{Key}, g^t, (v \prod_{j \in W} g_{K+1-j})^t) \\ &= (W, \{M\}_{Key}, C_0, C_1). \end{aligned}$$

Decryption: The decryptor u needs to checks whether $L_u \models W$ when receiving the ciphertext. If not, u returns $\perp$.

Then for $\forall i \in W$, u calculates the following terms:

$$\begin{aligned} e(g_i, C_1) &= e(g^{\alpha^i}, g^{t(\gamma + \sum_{j \in W} \alpha^{K+1-j})}) \\ &= e(g,g)^{t\gamma\alpha^i + t\sum_{j \in W} \alpha^{K+1-j+i}}, \text{ and} \end{aligned}$$

$$\begin{aligned} & e(C_0, D_i \cdot \prod_{j \in W, j \neq i} g_{K+1-j+i}) \\ &= e(g^t, g^{\gamma(\alpha^i + r_{i'}) + \sum_{j \in W, j \neq i} \alpha^{K+1-j+i}}) \\ &= e(g,g)^{t\gamma(\alpha^i + r_{i'}) + t\sum_{j \in W, j \neq i} \alpha^{K+1-j+i}}. \end{aligned}$$

Then, we calculate

$$\begin{aligned} & e(g_i, C_1) / e(C_0, d_i \cdot \prod_{j \in S, j \neq i} g_{K+1-j+i}) \\ &= e(g,g)^{-t\gamma r_{i'} + t\alpha^{K+1}}. \end{aligned}$$

After we calculate all k terms, we make a production of all the quotient terms and get:

$$e(g,g)^{-t\gamma(r_1 + r_2 + \cdots + r_k) + kt\alpha^{k+1}} = e(g,g)^{-t\gamma r + kt\alpha^{K+1}}.$$

We calculate:

$$e(D, C_0) = e(g,g)^{t\gamma r}.$$

Then, we produce these two terms and get

$$Key = e(g,g)^{kt\alpha^{K+1}} = e(g_K, g_1)^{kt}$$

and decrypt the message.

4. ABBE

In ABBE with N users, each user is issued an n-bit binary ID $b_0 b_1 \cdots b_n$, where b_i represents the i'th bit in the user's binary ID, where $n = \log N$. Accordingly, we can define n bit-assignment attributes $\{B_1, B_2, \cdots, B_n\}$. Each user is assigned n bit-assignment attribute values according to his/her ID. If the $b_i = 1$, he/she is assigned the B_i^+, if the $b_i = 0$, he/she is assigned the B_i^-. For example, in a system with 8 possible users, each user is assigned 3 bit-assignment attributes to represent the bit values in their ID, as illustrated in Figure 1:

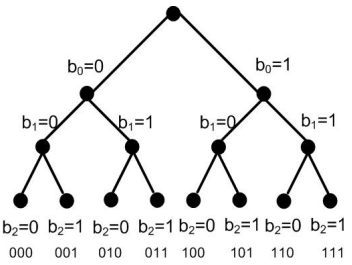

Figure 1: An illustration of bit-assignment attributes assignment for a 3-bit ID space.

With the $3n + 3m$ attribute values, the authority runs $\mathbf{Setup(n + m)}$ algorithm and generate public keys and private keys.

Here, we focus on how an encryptor can specify the list of receivers explicitly using n bit-assignment attributes. We first define some of the terms used in the following presentations:

- *Literal*: A variable or its complement, e.g., b_1, $\overline{b_1}$, etc.
- *Product Term*: Literals connected by AND, e.g., $\overline{b}_2 b_1 \overline{b}_0$.
- *Sum-of-Product Expression (SOPE)*: Product terms connected by OR, e.g., $\overline{b}_2 b_1 b_0 + b_2$.

Given the set of receivers S, the membership functions $f_S()$, which is in the form of SOPE, specifies the list of receivers:

$$f_S(b_1^u, b_2^u, \ldots, b_n^u) \quad = \quad \begin{cases} 0 & \text{iff } u \in S, \\ 1 & \text{iff } u \notin S. \end{cases}$$

For example, if the subgroup $S = \{000, 001, 011, 111\}$, then $f_S = \overline{b}_0\overline{b}_1\overline{b}_2 + \overline{b}_0\overline{b}_1 b_2 + \overline{b}_0 b_1 b_2 + b_0 b_1 b_2$.

Then, the broadcast encryptor runs the Quine-McCluskey algorithm [6] to reduce f_S to minimal SOPE f_S^{min}. The reduction can consider *do not care* values $*$ on those IDs that are not currently assigned to any receiver to further reduce number of product terms in the membership function. For example, if $S = \{000, 001, 011, 111\}$, $f_S^{min} = \overline{b}_0\overline{b}_1 + b_1 b_2$.

Since f_S^{min} is in the form of SOPE, encryption is performed on each product term. That is, for each product term E in f_S^{min}, the encryptor specifies an AND-gate access policy W using the following rules:

1. For positive literal $b_i \in f_S^{min}$, set B_i^+ in the access policy W.
2. For negative literal $\overline{b}_i \in f_S^{min}$, set B_i^- in the access policy W.
3. Set B_i^* for the rest of bit-assignment attributes.

For each W, the encryptor uses $\mathbf{Encrypt(PK, W, M)}$ algorithm to encrypt the message. The total number of encrypted message equals to the number of product terms in f_S^{min}.

For example, if $S = \{000, 001, 011, 111\}$, $f_S^{min} = \overline{b}_0\overline{b}_1 + b_1 b_2$. We can find that f_S^{min} contains 2 product terms. the message M for S can be encrypted into 2 ciphertexts with 2 product terms respectively.

4.1 Information Theoretical Optimality

If we denote our optimal bit-assignment attributes assignment to be minimalist, which requires the least number of bit-assignment attributes to identity each user. We can refer BGW scheme in [2] as maximalist. In BGW scheme, for a system with N users, each user is mapped to a unique public key. Given all N public keys, the number of combinations is $2^N - 1$, which equals to the number of receiver subsets in the system. Thus, each encryptor needs maximal number of public keys to perform broadcast encryption.

To compare the minimalist and maximalist storage strategy, we can treat each attribute or public key as an binary variable $v \in \{1, 0\}$. We denote $p = P_{v=1}$ as the percentage of totals users who have this attributes or public key and $1 - p = P_{v=0}$ as the percentage of totals users who do not have this attributes or public key, given that $P_{(v=1)} + P_{(v=0)} = 1$.

Definition 3. *The entropy of an attribute or a public key is defined as:*

$$H(v) = p \log p^{-1} + (1 - p) \log(1 - p)^{-1}.$$

□

Based on the Definition 3 , we see the entropy of each attribute in minimalist strategy as $H_a(1/2) = 1$ since ,for each particular attribute, exact half of the users have it while the other half do not have it. On the other hand, the entropy of public key in maximalist strategy is $H_a(1/N) = (1/N)\log(N) + ((N-1)/N)\log(N/(N-1)) < 1$. Hence, we can conclude that minimalist strategy attains maximal binary entropy while the maximalist strategy attains minimal binary entropy.

5. CONCLUSION

In this paper, a Constant Ciphertext Policy Attribute Based Encryption (CCP-ABE) was proposed. Compared with existing CP-ABE constructions, CCP-ABE significantly reduces the ciphertext size from linear to constant and supports expressive access policies. Based on CCP-ABE, we further proposed an Attribute Based Broadcast Encryption (ABBE) scheme that attains information theoretical minimal storage overhead. Thus, a storage restricted user can easily pre-install all required key materials to perform encryption and decryption.

6. REFERENCES

[1] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *SP '07: Proceedings of the 2007 IEEE Symposium on Security and Privacy*, pages 321–334, Washington, DC, USA, 2007. IEEE Computer Society.

[2] D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In *Advances in Cryptology–CRYPTO 2005*, pages 258–275. Springer, 2005.

[3] D. Boneh and B. Waters. Conjunctive, subset, and range queries on encrypted data. In *TCC'07: Proceedings of the 4th conference on Theory of cryptography*, pages 535–554, Berlin, Heidelberg, 2007. Springer-Verlag.

[4] L. Cheung and C. Newport. Provably secure ciphertext policy abe. In *CCS '07: Proceedings of the 14th ACM conference on Computer and communications security*, pages 456–465, New York, NY, USA, 2007. ACM.

[5] J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In *EUROCRYPT'08: Proceedings of the theory and applications of cryptographic techniques 27th annual international conference on Advances in cryptology*, pages 146–162, Berlin, Heidelberg, 2008. Springer-Verlag.

[6] E.J. McCluskey. Minimization of Boolean functions. *Bell System Technical Journal*, 35(5):1417–1444, 1956.