POSTER: Efficient Ciphertext Policy Attribute Based Encryption Under Decisional Linear Assumption

Tran Viet Xuan Phuong
Centre for Computer and Information Security Research
School of Computer Science and Software Engineering
University of Wollongong
Wollongong, NSW, Australia
tvxp750@uowmail.edu.au

Guomin Yang
Centre for Computer and Information Security Research
School of Computer Science and Software Engineering
University of Wollongong
Wollongong, NSW, Australia
gyang@uow.edu.au

Willy Susilo
Centre for Computer and Information Security Research
School of Computer Science and Software Engineering
University of Wollongong
Wollongong, NSW, Australia
wsusilo@uow.edu.au

ABSTRACT

We propose a new Ciphertext Policy Attribute Based Encryption (CP-ABE) scheme where access structures are defined by AND-Gates with wildcards. One major difference between our scheme and the existing ones is that we can use a single element to represent one attribute, while the previous schemes require three different elements to represent the three possible values (namely positive, negative, and wildcard) of an attribute. Our proposed scheme also achieves both constant-size ciphertext and constant number of decryption operations, and is proven secure under the standard Decision Linear Assumption.

Categories and Subject Descriptors

E.3 [**Data Encryption**]: Public Key Cryptosystems

Keywords

Attribute Based Encryption, Viète's Formula

1. INTRODUCTION

Attribute-based encryption (ABE), which was introduced by Sahai and Waters [9] and extensively studied in recent years [6, 1, 11, 7], provides a fine-grained access control of encrypted data. In a Ciphertext Policy Attribute Based Encryption (CP-ABE) system, each user secret key is associated with a set of attributes, and every ciphertext is associated with an access policy. The ciphertext can be decrypted by a secret key if and only if the attributes associated with the secret key satisfies the access policy. A Key Policy ABE (KP-ABE) system can be defined in a similar way by swapping the positions of the attributes and the access policy. ABE differs from the conventional PKE and IBE schemes in the sense that it defines a one-to-many relationship between a ciphertext and the corresponding decryption keys, and hence can directly be used as a broadcast encryption scheme.

In this work, we explore new constructions of CP-ABE that use AND-gates with wildcard as the access structure. The existing schemes of this type [3, 8, 12] require three different elements to represent the three possible values – positive, negative, and wildcard – of an attribute. In this paper, we propose a novel construction which uses only one element to represent one attribute. The main idea behind our construction is to use the "positions" of the attributes to do the matching. We put the indices of all the positive, negative and wildcard attributes defined in an access structure into three sets. By using the Viète's formulas [10], the decryptor can remove all the wildcard positions, and the decryption will be successful if and only if the remaining attributes of the decryptor match those in the access structure. Also, our scheme achieves constant-size ciphertext and constant computation cost during decryption, which make it more efficient than the existing schemes. We prove the security of the proposed scheme under the standard Decision Linear (DLIN) assumption.

2. PRELIMINARIES

Bilinear Map on Prime Order Groups. Let $\mathbb{G}$ and $\mathbb{G}_T$ be two multiplicative cyclic groups of the same prime order p, and g a generator of $\mathbb{G}$. Let $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ be a bilinear map with the following properties:(1) *Bilinearity* : $e(u^a, v^b) = e(u^b, v^a) = e(u, v)^{ab}$ for all $u,v \in \mathbb{G}$ and $a,b \in \mathbb{Z}_p$. (2) *Non-degeneracy* : $e(g, g) \neq 1$.

DLIN Assumption. The Decisional Linear (DLIN) problem in $\mathbb{G}$ is defined as follows: given a tuple $(g, g^a, g^b, g^{ac}, g^d, T) \in \mathbb{G}^6$, decide whether $T = g^{b(c+d)}$ or T is random random element of $\mathbb{G}$. We say that the DLIN assumptions holds in $\mathbb{G}$ if for any probabilistic polynomial-time algorithm A $\Pr[A(g, g^a, g^b, g^{ac}, g^d, T = g^{b(c+d)}) = 1] - \Pr[A(g, g^a, g^b, g^{ac}, g^d, T = g^r) = 1]| \leq \epsilon(k)$, where $a, b, c, d, r \in_R \mathbb{Z}_p$ and $\epsilon(k)$ is negligible in the security parameter k.

The Viète's formulas [10]. Consider two vectors $\overrightarrow{v} = (v_1, v_2, \ldots, v_L)$ and $\overrightarrow{z} = (z_1, z_2, \ldots, z_L)$ where v contains both alphabets and wildcards and z only contains alphabets. Let $J = \{j_1, \ldots, j_n\} \subset \{1, \ldots, L\}$ denote the wildcard positions. Then the statement $(v_i = z_i \vee v_i = * \text{ for } i = 1 \ldots L)$ can be expressed by

$$\sum_{i=1, i \notin J}^{L} v_i \prod_{j \in J} (i - j) = \sum_{i=1}^{L} z_i \prod_{j \in J} (i - j). \quad (1)$$

CCS'14, November 3–7, 2014, Scottsdale, Arizona, USA.
ACM 978-1-4503-2957-6/14/11.
http://dx.doi.org/10.1145/2660267.2662358 .

Expand $\prod_{j\in J}(i-j)=\sum_{k=0}^{n}\lambda_k i^k$, where λ_k are the coefficients dependent on J, then (1) becomes:

$$\sum_{i=1,i\notin J}^{L} v_i \prod_{j\in J}(i-j)=\sum_{k=0}^{n}\lambda_k\sum_{i=1}^{L} z_i i^k \tag{2}$$

To hide the computations, we choose random group element H_i and put v_i, z_i as the exponents of group elements: $H_i^{v_i}, H_i^{z_i}$. Then (2) becomes:

$$\prod_{i=1,i\notin J}^{L} H_i^{v_i\prod_{j\in J}(i-j)}=\prod_{k=0}^{n}(\prod_{i=1}^{L} H_i^{z_i i^k})^{\lambda_k} \tag{3}$$

Using Viète's formulas we can construct the coefficient λ_k in (2) by:

$$\lambda_{n-k}=(-1)^k\sum_{1\le i_1<i_2<\ldots<i_k\le n} j_{i_1}j_{i_2}\ldots j_{i_k},\ 0\le k\le n. \tag{4}$$

where $n=|J|$. For example, if we have $J=\{j_1,j_2,j_3\}$, the polynomial is $(x-j_1)(x-j_2)(x-j_3)$, then $\lambda_3=1,\lambda_2=-(j_1+j_2+j_3),\lambda_1=(j_1j_2+j_1j_3+j_2j_3),\lambda_0=-j_1j_2j_3$.

Access Structure. Let $U=\{Att_1,Att_2,...,Att_L\}$ be the universe of attributes in the system. Each attribute Att_i has two possible values: positive and negative. Let $W=\{Att_1,Att_2,...,Att_L\}$ be an AND-gates access policy with wildcards. A wildcard '*' means "don't care" (i.e., both positive and negative attributes are accepted). We use the notation $S\models W$ to denote that the attribute list S of a user satisfies W.

For example, suppose $U=\{Att_1=\text{CS},Att_2=\text{EE},Att_3=\text{Faculty},Att_4=\text{Student}\}$. Alice is a student in the CS department; Bob is a faculty in the EE department; Carol is a faculty holding a joint position in the EE and CS department. Their attribute lists are illustrated in Table 1. The access structure W_1 can be satisfied by all the CS students, while W_2 can be satisfied by all CS people.

Table 1: List of attributes and policies

Attributes	Att_1	Att_2	Att_3	Att_4
Description	CS	EE	Faculty	Student
Alice	+	−	−	+
Bob	−	+	+	−
Carol	+	+	+	−
W_1	+	−	−	+
W_2	+	−	*	*

3. CONSTANT-SIZE CP-ABE

In this section, we present our CP-ABE scheme based on the AND-gates with wildcards access structure. We represent each attribute in the universe by an element A_i. Given an access structure W, we first define three sets J, V, and Z where J contains the positions of all the wildcard positions, and V and Z contain the positions of all the positive and negative attributes, respectively. The set J is attached to the ciphertext and sent to the decryptor.

Setup(1^k): Let N_1,N_2,N_3 be three upper bounds defined as $N_1\le L$: the maximum number of wildcard in an access structure; $N_2\le L$: the maximum number of positive attribute in an attribute set S; $N_3\le L$: the maximum number of negative attribute in an attribute set S. The setup algorithm first generates bilinear groups $\mathbb{G},\mathbb{G}_T$ with order p, and selects two random generators $V_0,V_1,g\in\mathbb{G}$. Then randomly choose $\alpha,\beta_1,\beta_2,a_1,\ldots,a_L\in_R\mathbb{Z}_p$, and set $\Omega_1=e(g,V_0)^{\alpha\beta_1}e(g,V_1)^{\alpha\beta_1},\Omega_2=e(g,V_0)^{\alpha\beta_2}e(g,V_1)^{\alpha\beta_2}$. Let $A_i=g^{a_i}$ for $1=1,\ldots,L$.

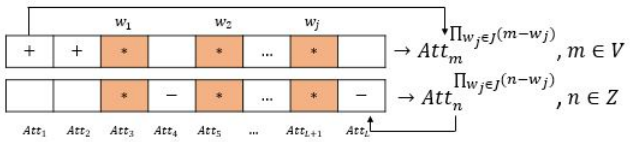

Figure 1: Encryption Process

The Public key and Master Secret Key are defined as: $PK=(e,g,\Omega_1,\Omega_2,g^{\alpha},V_0,V_1,A_1,\ldots,A_L)$, $MSK=(\alpha,\beta_1,\beta_2,a_1,\ldots,a_L)$.

Encrypt(W,M,PK): Suppose that the access structure W contains: $n_1\le N_1$ wildcards which occur at positions $J=\{w_1,\ldots,w_{n_1}\}$; $n_2\le N_2$ positive attributes which occur at positions $V=\{v_1,\ldots,v_{n_2}\}$; $n_3\le N_3$ negative attributes which occur at positions $Z=\{z_1,\ldots,z_{n_3}\}$. Based on (4), compute for the wildcard positions $\{w_j\}$ $(j=0,1,2,\cdots,n_1)$ $\{\lambda_{w_j}\}$ and set $t_w=\sum_{j=0}^{n_1}\lambda_{w_j}$. The encryption algorithm then chooses $r_1,r_2\in_R\mathbb{Z}_p$, and creates the ciphertext as:

$C_0=M\Omega_1^{r_1}\Omega_2^{r_2}, C_1=g^{\frac{\alpha r_1}{t_w}}, C_2=g^{\frac{r_2}{t_w}}$,

$C_3=(V_0\prod_{i\in V}(A_i^{\frac{\prod_{j=0}^{n_1}(i-w_j)}{t_w}})^{r_1+r_2}, C_4=(V_1\prod_{i\in Z}(A_i^{\frac{\prod_{j=0}^{n_1}(i-w_j)}{t_w}})^{r_1+r_2}$,

The ciphertext is set as $CT=(C_0,C_1,C_2,C_3,J=\{w_1,w_2,\ldots,w_{n_1}\})$.

KeyGen(MSK,S): Suppose that a user joins the system with the attribute list S, which contains: $n_2'\le N_2$ positive attributes which occur at positions $V'=\{v_1',\ldots,v_{n_2'}'\}$; $n_3'\le N_3$ negative attributes which occur at positions $Z'=\{z_1',\ldots,z_{n_3'}'\}$. By means of the Viète's formulas, for all the positive positions $\{v_k'\}$ $(k=0,1,2,\cdots,n_2')$, calculate $\{\lambda_{v_k'}\}$ and set $t_v'=\sum_{k=0}^{n_2}\lambda_{v_k'}$; and for all the negative positions $\{z_\tau'\}$ $(\tau=0,1,2,\cdots,n_3')$, calculate $\{\lambda_{z_\tau'}\}$ and set $t_z'=\sum_{\tau=0}^{n_3'}\lambda_{z_\tau'}$. The algorithm then chooses $s\in_R\mathbb{Z}_p$ and computes $s_1=\beta_1+s, s_2=\beta_2+s$ and creates the secret key as:

$$\begin{aligned}
L_1 &= g^{\frac{\alpha s}{t_v'}}, L_2=g^{\frac{\alpha s}{t_z'}},\\
K_1 &= \{K_{1,0},K_{1,1},\ldots,K_{1,N_1}\}\\
&= \{V_0^{s_1}\prod_{i\in V'}g^{sa_i},V_0^{s_1}\prod_{i\in V'}g^{sa_ii},\ldots,V_0^{s_1}\prod_{i\in V'}g^{sa_ii^{N_1}}\},\\
K_1' &= \{K_{1,0}',K_{1,1}',\ldots,K_{1,N_1}'\}\\
&= \{V_0^{\alpha s_2}\prod_{i\in V'}g^{s\alpha a_i},V_0^{\alpha s_2}\prod_{i\in V'}g^{s\alpha a_ii},\ldots,V_0^{\alpha s_2}\prod_{i\in V'}g^{s\alpha a_ii^{N_1}}\}.
\end{aligned}$$

$$\begin{aligned}
K_2 &= \{K_{2,0},K_{2,1},\ldots,K_{2,N_1}\}\\
&= \{V_1^{s_1}\prod_{i\in Z'}g^{sa_i},V_1^{s_1}\prod_{i\in Z'}g^{sa_ii},\ldots,V_1^{s_1}\prod_{i\in Z'}g^{sa_ii^{N_1}}\},\\
K_2' &= \{K_{2,0}',K_{2,1}',\ldots,K_{2,N_1}'\}\\
&= \{V_1^{\alpha s_2}\prod_{i\in Z'}g^{s\alpha a_i},V_1^{\alpha s_2}\prod_{i\in Z'}g^{s\alpha a_ii},\ldots,V_1^{\alpha s_2}\prod_{i\in Z'}g^{s\alpha a_ii^{N_1}}\}.
\end{aligned}$$

The user secret key is set as $SK=(L_1,L_2,K_1,K_1',K_2,K_2')$.

Decrypt(CT,SK): The algorithm first identifies the wildcard positions in $J=\{w_1,\ldots,w_{n_1}\}$ and computes $\{\lambda_{w_j}\}$. Then we have:

$$\begin{aligned}
&\frac{e(L_1,C_3)^{t_v'}\cdot e(L_2,C_4)^{t_z'}}{e(\prod_{j=0}^{n_1}K_{1,j}^{\lambda_{w_j}},C_1)\cdot e(\prod_{j=0}^{n_1}(K_{1,j}')^{\lambda_{w_j}},C_2)\cdot e(\prod_{j=0}^{n_1}K_{2,j}^{\lambda_{w_j}},C_1)\cdot e(\prod_{j=0}^{n_1}(K_{2,j}')^{\lambda_{w_j}},C_2)}\\
&= e(g,V_0)^{-\alpha\beta_1r_1}e(g,V_0)^{-\alpha\beta_2r_2}e(g,V_1)^{-\alpha\beta_1r_1}e(g,V_1)^{-\alpha\beta_2r_2}\\
&= \Omega_1^{-r_1}\Omega_2^{-r_2}
\end{aligned}$$

and M can be recovered by $\Omega_1^{-r_1}\Omega_2^{-r_2} \cdot C_0$.

4. SECURITY ANALYSIS

The selective security of the proposed scheme can be proved under the DLIN assumption. Let $\mathcal{B}$ denote an algorithm that is given $(g, g^a, g^b, g^{ac}, g^d, T) \in \mathbb{G}^6$ as input. $\mathcal{B}$'s goal is to decide $T = g^{b(c+d)}$ or $T = g^r$.

In the selective game, the simulator $\mathcal{B}$ first receives from the adversary a challenge access structure $W^* = [W_1^*, \ldots, W_L^*]$ which contains n_1 wildcards which occur at positions $J = \{w_1, \ldots, w_{n_1}\}$, n_2 positive attributes which occur at positions $V = \{v_1, \ldots, v_{n_2}\}$, n_3 negative attributes which occur at positions $Z = \{z_1, \ldots, z_{n_3}\}$. Then $\mathcal{B}$ chooses an upper bound $n_1 \leq N_1 \leq L$ for the number of wildcard in an access structure, and then selects $\sigma_1, \sigma_2, \sigma_3 \in_R \mathbb{Z}_p$. $\mathcal{B}$ also selects $\gamma_0, \gamma_1, \{a_i'\}_{1 \leq i \leq L} \in_R \mathbb{Z}_p$, and computes by means of the Viète's formulas $\{\lambda_{w_j}\}_{w_j \in J}$ and sets $t_w = \sum_{j=0}^{n_1} \lambda_{w_j}$. $\mathcal{B}$ then sets

$$V_0 = (g^b)^{\gamma_0} g^{-\sum_{att_i \in W_i^*, i \in V} \frac{a_i' \prod_{j=1}^{n_1}(i-w_j)}{t_w}}$$

$$V_1 = (g^b)^{\gamma_1} g^{-\sum_{att_i \in W_i^*, i \in Z} \frac{a_i' \prod_{j=1}^{n_1}(i-w_j)}{t_w}}$$

$$A_i = g^{a_i} = \begin{cases} g^{a_i'} & att_i = W_i^* \\ g^{\frac{a_i'}{\sum_{att_m \in W_i^*} a_m' \prod_{j=1}^{n_1}(m-w_j)}} & att_i \neq W_i^* \end{cases}$$

$\Omega_1 = e(g^a, V_0)^{\sigma_1 - \sigma_2} e(g^a, V_1)^{\sigma_1 - \sigma_2}$
$\Omega_2 = e(g^{\sigma_3}(g^a)^{-\sigma_2}, V_0) e(g^{\sigma_3}(g^a)^{-\sigma_2}, V_1)$. The public key is $PK = (e, g, \Omega_1, \Omega_2, g^a, V_0, V_1, A_1, \ldots, A_L)$, and the corresponding master secret key is $MSK = (\alpha = a, \beta_1 = \sigma_1 - \sigma_2, \beta_2 = \frac{\sigma_3}{a} - \sigma_2, a_1, \ldots, a_L)$.

Given two messages M_0 and M_1 chosen by the adversary, $\mathcal{B}$ flips a coin ν and generates the challenge ciphertext as:

$$C_0 = M_\nu e(g^{ac}, g^b)^{\sigma_1 \gamma_0} \cdot e(g^{ac}, g)^{(\sigma_1 - \sigma_2) \sum_{att_i \in W_i^*, i \in V} \frac{a_i' \prod_{j=1}^{n_1}(i-w_j)}{t_w}} \cdot$$
$$e(g^a, g^d)^{\sigma_2 \sum_{att_i \in W_i^*, i \in V} \frac{a_i' \prod_{j=1}^{n_1}(i-w_j)}{t_w}} \cdot e(g^b, g^d)^{\sigma_3 \gamma_0} \cdot$$
$$e(g^{ac}, g^b)^{\sigma_1 \gamma_1} \cdot e(g^{ac}, g)^{(\sigma_1 - \sigma_2) \sum_{att_i \in W_i^*, i \in Z} \frac{a_i' \prod_{j=1}^{n_1}(i-w_j)}{t_w}} \cdot$$
$$e(g^a, g^d)^{\sigma_2 \sum_{att_i \in W_i^*, i \in Z} \frac{a_i' \prod_{j=1}^{n_1}(i-w_j)}{t_w}} \cdot e(g^b, g^d)^{\sigma_3 \gamma_1} \cdot$$
$$e(g^d, g)^{\sigma_3 \sum_{att_i \in W_i^*, i \in V} \frac{a_i' \prod_{j=1}^{n_1}(i-w_j)}{t_w}} \cdot e(g^a, T)^{\sigma_2 \gamma_0} \cdot$$
$$e(g^d, g)^{\sigma_3 \sum_{att_i \in W_i^*, i \in Z} \frac{a_i' \prod_{j=1}^{n_1}(i-w_j)}{t_w}} \cdot e(g^a, T)^{\sigma_2 \gamma_1},$$

$$C_1 = (g^{ac})^{\frac{1}{t_w}}, C_2 = (g^d)^{\frac{1}{t_w}},$$

$$C_3 = (V_0 \prod_{i \in V} (A_i^{\frac{\prod_{j=0}^{n_1}(i-w_j)}{t_w}})^{r_1 + r_2} = T^{\gamma_0},$$

$$C_4 = (V_1 \prod_{i \in Z} (A_i^{\frac{\prod_{j=0}^{n_1}(i-w_j)}{t_w}})^{r_1 + r_2} = T^{\gamma_1}.$$

If $Z = g^{b(c+d)}$, the challenge ciphertext is simulated perfectly; otherwise, if Z is a random group element, then the message M_ν is completely hidden from the adversary.

5. COMPARISON

In Table 2, we give a detailed comparison among the existing CP-ABE schemes based on the AND-Gate access structure where **p** denotes the pairing operation, **e** denotes the exponentiation operation, and t is the number of attributes involved in the access structure.

Table 2: Comparison among CP-ABE

Scheme	Ciphertext Length	Dec Cost	Wildcard	Assumption
CN[3]	$\lvert\mathbb{G}_T\rvert + (t+1)\lvert\mathbb{G}\rvert$	$(t+1)\mathbf{p}$	√	DBDH
NYO[8]	$\lvert\mathbb{G}_T\rvert + (2t+1)\lvert\mathbb{G}\rvert$	$(2t+1)\mathbf{p}$	√	DBDH + DLIN
Emura et al.[4]	$\lvert\mathbb{G}_T\rvert + 2\lvert\mathbb{G}\rvert$	$2\mathbf{p}$	X	DBDH
ZH[12]	$\lvert\mathbb{G}_T\rvert + 2\lvert\mathbb{G}\rvert$	$2t\mathbf{p} + 1$	√	n-BDHE
CZF[2]	$\lvert\mathbb{G}_T\rvert + 2\lvert\mathbb{G}\rvert$	$2\mathbf{p}$	X	n-BDHE
DZCCZ12[5]	$\lvert\mathbb{G}_T\rvert + 2\lvert\mathbb{G}\rvert$	$2\mathbf{p}$	X	n-BDHE
Our Scheme	$\lvert\mathbb{G}_T\rvert + 4\lvert\mathbb{G}\rvert$	$6\mathbf{p}$	√	DLIN

6. REFERENCES

[1] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *IEEE S&P 2007*, pages 321 –334, 2007.

[2] C. Chen, Z. Zhang, and D. Feng. Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost. In *5th ProvSec*, pages 84–101, 2011.

[3] L. Cheung and C. Newport. Provably secure ciphertext policy abe. In *14th ACM CCS 2007*, pages 456–465.

[4] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. In *5th ISPEC*, pages 13–23, 2009.

[5] A. Ge, R. Zhang, C. Chen, C. Ma, and Z. Zhang. In *Information Security and Privacy*, pages 336–349, 2012.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *13th ACM CCS 2006*, pages 89–98, 2006.

[7] A. B. Lewko and B. Waters. New proof methods for attribute-based encryption: Achieving full security through selective techniques. In *CRYPTO*, pages 180–198, 2012.

[8] T. Nishide, K. Yoneyama, and K. Ohta. Attribute-based encryption with partially hidden encryptor-specified access structures. In *6th ACNS 2008*, pages 111–129.

[9] A. Sahai and B. Waters. Fuzzy identity-based encryption. In *EUROCRYPT 2005*, volume 3494, pages 457–473, 2005.

[10] S. Sedghi, P. Liesdonk, S. Nikova, P. Hartel, and W. Jonker. In *SCN 2010*, pages 138–153.

[11] B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *PKC 2011*, pages 53–70.

[12] Z. Zhou and D. Huang. On efficient ciphertext-policy attribute based encryption and broadcast encryption: extended abstract. In *17th ACM CCS 2010*, pages 753–755.