# CP-ABE With Constant-Size Keys for Lightweight Devices

Fuchun Guo, Yi Mu, *Senior Member, IEEE*, Willy Susilo, *Senior Member, IEEE*, Duncan S. Wong, and Vijay Varadharajan, *Senior Member, IEEE*

***Abstract*— Lightweight devices, such as radio frequency identification tags, have a limited storage capacity, which has become a bottleneck for many applications, especially for security applications. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising cryptographic tool, where the encryptor can decide the access structure that will be used to protect the sensitive data. However, current CP-ABE schemes suffer from the issue of having long decryption keys, in which the size is linear to and dependent on the number of attributes. This drawback prevents the use of lightweight devices in practice as a storage of the decryption keys of the CP-ABE for users. In this paper, we provide an affirmative answer to the above long standing issue, which will make the CP-ABE very practical. We propose a novel CP-ABE scheme with constant-size decryption keys independent of the number of attributes. We found that the size can be as small as 672 bits. In comparison with other schemes in the literature, the proposed scheme is the only CP-ABE with expressive access structures, which is suitable for CP-ABE key storage in lightweight devices.**

***Index Terms*— Attribute-based encryption, ciphertext policy, short decryption key.**

## I. Introduction

LIGHTWEIGHT devices (e.g. Radio Frequency Identification (RFID) tags) have been well known to have many useful applications. To name a few, this includes electronic passports, ID cards and secret data storage, such as cryptographic key storage. As shown in Fig. 1, the authority generates decryption keys of users and stores them in an RFID tag embedded within a user's ID card. The user can extract the key from his/her ID card for a security use.

Lightweight devices usually have limited memory capacity. For example, a passive RFID tag only offers a storage of few kilo bits [1]. This has become a major challenge to applications such as key storage. Many encryption systems can offer short decryption keys. For example, identity-based broadcast encryption [2], identity-based encryption with traitor tracing [3], multi-identity single-key decryption [4]–[6]. Unfortunately, there is no any efficient attribute-based encryption scheme in the literature, which offers short decryption keys.

Attribute-based encryption (ABE) is an extension of identity-based encryption [7] which allows users to encrypt and decrypt messages based on attributes and access structures. Ciphertext-policy attribute-based encryption (CP-ABE) is a type of ABE schemes where the decryption key is associated with a user's attribute set. The encryptor defines the access structure to protect sensitive data such that only users whose attributes satisfy the access structure can decrypt the messages. Due to this nice property, CP-ABE has attracted a lot of attention (e.g. [8]–[10]) in applications such as access control.

Many CP-ABE schemes (e.g. [11]–[19]) have been proposed for various purposes such as short ciphertext and full security proofs. However, we found no CP-ABE scheme with expressive access structures in the literature addressing the size issue of decryption keys, which seems to be a drawback due to resource consumption. All existing CP-ABE schemes suffer from the issue of long decryption keys, in which the length is dependent on the number of attributes. This issue becomes more obvious, when CP-ABE decryption keys are applied to storage-constrained devices. Because of the popularity of lightweight devices and useful applications of CP-ABE, in this work, we propose a provably secure CP-ABE scheme that offers short decryption keys, which are applicable for key storage in lightweight devices.

### A. Our Contributions

We propose a ciphertext-policy attribute-based encryption in which the access structures are AND gates [13], [16]. A decryption key associated with an attribute set $\mathbb{A}$ can decrypt ciphertxts with the access structure $\mathbb{P}$ when $\mathbb{P} \subseteq \mathbb{A}$. Mostly important, the decryption key is constant-size and independent of the number of attributes. More precisely, the decryption key is composed of two group elements only and the size can be 672 bits at most under 80-bit security requirement. The proposed CP-ABE scheme is provably secure in the selective security model.

A detailed comparison of ABE is given in Table I. The comparison shows that our scheme is the only expressive

Manuscript received May 11, 2013; revised January 13, 2014 and February 23, 2014; accepted February 23, 2014. Date of publication March 5, 2014; date of current version April 2, 2014. The work of F. Guo, Y. Mu, W. Susilo, and V. Varadharajan was supported in part by ARC Discovery under Grant DP110101951. The work of W. Susilo was also supported by ARC Future Fellowship under Grant FT0991397. The work of D. S. Wong was supported by a grant from the RGC of the HKSAR, China, under Project CityU 123913. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. C.-C. Jay Kuo.

F. Guo, Y. Mu, and W. Susilo are with the School of Computer Science and Software Engineering, University of Wollongong, Wollongong, NSW 2500, Australia (e-mail: fuchun@uow.edu.au; ymu@uow.edu.au; wsusilo@uow.edu.au).

D. S. Wong is with the Department of Computer Science, City University of Hong Kong, Hong Kong (e-mail: duncan@cityu.edu.hk).

V. Varadharajan is with the Department of Computing, Macquarie University, North Ryde, NSW 2109, Australia (e-mail: vijay.varadharajan@mq.edu.au).

Digital Object Identifier 10.1109/TIFS.2014.2309858

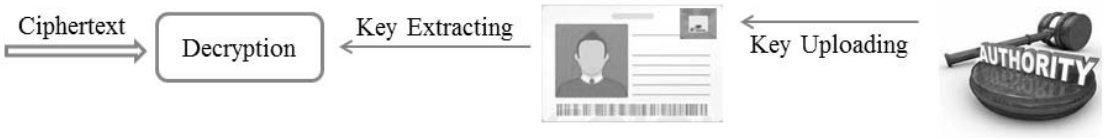


Fig. 1. A security use of decryption with decryption keys stored in RFID tags embedded within ID cards.

TABLE I
COMPARISON OF ATTRIBUTE-BASED ENCRYPTION SCHEMES

| Schemes | KP/CP-ABE | Access Structure | Security Model | Length of Decryption Key | Length of Ciphertext |
|---|---|---|---|---|---|
| SW[20] | KP-ABE | Threshold | Selective Security | $n\mathbb{G}$ | $n\mathbb{G}+\mathbb{G}_T$ |
| GPSW[11] | KP-ABE | Tree | Selective Security | $\|\mathbb{A}\|\mathbb{G}$ | $\|\mathbb{P}\|\mathbb{G}+\mathbb{G}_T$ |
| OSW[21] | KP-ABE | Tree | Selective Security | $2\|\mathbb{A}\|\mathbb{G}$ | $(\|\mathbb{P}\|+1)\mathbb{G}+\mathbb{G}_T$ |
| BSW[12] | CP-ABE | Tree | Selective Security | $(2\|\mathbb{A}\|+1)\mathbb{G}$ | $(2\|\mathbb{P}\|+1)\mathbb{G}+\mathbb{G}_T$ |
| HLR[17] | CP-ABE | Threshold | Selective Security | $(n+\|\mathbb{A}\|)\mathbb{G}$ | $2\mathbb{G}+\mathbb{G}_T$ |
| CCLZFLW[22] | KP/CP-ABE | Threshold | Full Security | $O(n^2)$ | $O(1)$ |
| EMONS[15] | CP-ABE | $(n,n)$-Threshold | Selective Security | $2\mathbb{G}$ | $2\mathbb{G}+\mathbb{G}_T$ |
| LOSTW [18] | CP-ABE | LSSS | Full Security | $(\|\mathbb{A}\|+2)\mathbb{G}_c$ | $(2\|\mathbb{P}\|+1)\mathbb{G}_c+\mathbb{G}_{T_c}$ |
| Waters[14] | CP-ABE | LSSS | Selective Security | $(\|\mathbb{A}\|+2)\mathbb{G}$ | $(2\|\mathbb{P}+1\|)\mathbb{G}+\mathbb{G}_T$ |
| ALP[23] | KP-ABE | LSSS | Selective Security | $3\|\mathbb{A}\|\mathbb{G}$ | $2\mathbb{G}+\mathbb{G}_T$ |
| LW[19] | CP-ABE | LSSS | Full Security | $(\|\mathbb{A}\|+3)\mathbb{G}_c$ | $(2\|\mathbb{P}\|+2)\mathbb{G}_c+\mathbb{G}_{T_c}$ |
| CN[13] | CP-ABE | AND gates | Selective Security | $(2\|\mathbb{A}\|+1)\mathbb{G}$ | $(\|\mathbb{P}\|+1)\mathbb{G}+\mathbb{G}_T$ |
| ZH[16] | CP-ABE | AND gates | Selective Security | $(\|\mathbb{A}\|+1)\mathbb{G}$ | $2\mathbb{G}+\mathbb{G}_T$ |
| Our Scheme | CP-ABE | AND gates | Selective Security | $2\mathbb{G}$ | $(n-\|\mathbb{P}\|+2)\mathbb{G}+\mathbb{G}_T$ |

CP-ABE with constant-size decryption keys. Since the key size is constant and small, our CP-ABE scheme allows all applications with key storage in lightweight devices.

### *B. Related Work*

Attribute-based encryption (ABE) was first introduced by Sahai and Waters in [20]. There are two variants of ABE: Key-Policy ABE and Ciphertext-Policy ABE [11].

- KP-ABE: In a KP-ABE scheme, the ciphertext encrypting a message is associated with a set of attributes. A decryption key issued by an authority is associated with an access structure. The ciphertext can be decrypted with the decryption key if and only if the attribute set of ciphertext satisfies the access structure of decryption key.
- CP-ABE: In a CP-ABE scheme, on the contrary, the ciphertext encrypts a message with an access structure while a decryption key is associated with a set of attributes. The decryption condition is similar: if and only if the attribute set fulfils the access structure.

Many KP-ABE schemes [11], [20]–[23] and CP-ABE schemes [11]–[19] have been proposed in the literature. In comparison with KP-ABE, CP-ABE is more appropriate in access control applications since it enables message encryptor to choose the access structure to decide who can access the message.

The notion of CP-ABE was first proposed by Goyal *et al.* in [11] but they did not offer any construction [12]. Soon after that, Bethencourt, Sahai and Waters [12] proposed the first CP-ABE construction. Then, Cheung and Newport [13] proposed another CP-ABE in which the access structures are AND gates.

CP-ABE towards constant-size ciphertexts have been proposed. Herranz *et al.* [17] and Chen *et al.* [22] proposed CP-ABE schemes with constant-size ciphertexts under the threshold access structure. Zhou and Huang [16] proposed a CP-ABE scheme with constant-size ciphertexts under AND gates access structure. CP-ABE schemes with constant-size ciphertexts are also studied in [24] and [25].

Most of CP-ABE schemes in the literature have linear-size decryption keys. The only proposed scheme with constant-size key is proposed in [15]. However, the access structure is $(n, n)$-threshold, where the required attributes in the access structure and the user's attributes must be the same. This access structure does not fulfil the motivation of ABE for fuzzy decryption. In Section IV, we show there exists a simple construction of CP-ABE under this particular access structure.

Most of proposed CP-ABE schemes are provably secure in the selective security model. Lewko *et al.* [18] proposed the first fully secure CP-ABE using composite-order pairing. Okamoto and Takashima [26] proposed a fully secure and unbounded CP-ABE scheme, where the setup phase does not need to fix the maximum number of attributes. Lewko and Waters [19] developed a new methodology for utilizing the prior techniques to prove full security of CP-ABE. Chen *et al.* [22] proposed a fully secure CP-ABE with constant-size ciphertexts.

CP-ABE schemes fall into different types of access structures. They are including AND gates access structure [13], and threshold access structure [17], [22] for short ciphertexts. For general access structure, there are CP-ABE schemes based on monotone tree access structure [12], [27] that support AND, OR, and threshold, and based on LSSS [14], [18], [19] in which any monotonic boolean formula can be converted into an LSSS representation. Okamoto and Takashima [26] proposed fully secure CP-ABE schemes under non-monotone access structure based on span program. Sahai and Waters [28] proposed the first ABE schemes for general circuit.

Other ABE schemes are proposed for different purposes. Chase [29] gave a construction of multi-authority attribute-based encryption. Nishide *et al.* [30] proposed ABE schemes with partially hidden access structures. Hohenberger and Waters [31] gave a construction of ABE scheme with fast decryption. Hinek *et al.* considered the problem of key cloning for attribute-based encryption in [32]. Liu *et al.* proposed white-box traceable CP-ABE with monotone access structure in [33].

## II. Preliminaries and Definitions

In this section, we give all preliminaries and definitions associated with ciphertext-policy attribute-based encryption.

### A. Attribute Definition and Access Structure

We denote by $A$ an attribute. Let $\{A_1, A_2, \ldots, A_n\}$ be the set of all attributes. For convenience, we denote by subscript $i$ the attribute $A_i$.

Let $\mathbb{A}$ be an attribute set of a user. We define $\mathbb{A} \subset \{A_1, A_2, \ldots, A_n\}$. In this paper, we represent the attribute set $\mathbb{A}$ with an $n$-bit string $a_1 a_2 \cdots a_n$ defined as follows.

$$\begin{cases} a_i = 1: & A_i \in \mathbb{A} \\ a_i = 0: & A_i \notin \mathbb{A} \end{cases}$$

For example, let $n = 4$. The 4-bit string $\mathbb{A} = 1011$ means the attribute set consists of the attributes $\{A_1, A_3, A_4\}$. We use $|\mathbb{A}|$ to denote the number of attributes in $\mathbb{A}$.

We consider the AND gate access structure represented by attributes from $\{A_1, A_2, \ldots, A_n\}$. We utilize $\mathbb{P}$ to define an access structure specified with attributes. In this paper, we also represent the $\mathbb{P}$ with an $n$-bit string $b_1 b_2 \cdots b_n$ defined as follows.

$$\begin{cases} b_i = 1: & A_i \in \mathbb{P} \\ b_i = 0: & A_i \notin \mathbb{P} \end{cases}$$

For example, let $n = 4$. The 4-bit string $\mathbb{P} = 1001$ means the access structure $\mathbb{P}$ requires $\{A_1, A_4\}$ attributes. We use $|\mathbb{P}|$ to denote the number of attributes in $\mathbb{P}$.

In the rest of this paper, the attribute set $\mathbb{A}$ and the access structure $\mathbb{P}$ will be represented with an $n$-bit string.

*Definition 1:* An attribute set $\mathbb{A} = a_1 a_2 \cdots a_n$ fulfils the access structure $\mathbb{P} = b_1 b_2 \cdots b_n$ if for all $i = 1$ to $n$, we have $a_i \geq b_i$. We write $\mathbb{P} \subseteq \mathbb{A}$ for the shorthand of $\mathbb{A}$ fulfilling $\mathbb{P}$.

The above definition is based on the representation of bit strings, and useful in our scheme description. To easily understand the definition, we can view $\mathbb{A}$ and $\mathbb{P}$ as a set of attributes. We have $\mathbb{A}$ fulfilling $\mathbb{P}$ if $\mathbb{P}$ is a subset of $\mathbb{A}$.

### B. Definitions

A ciphertext-policy attribute-based encryption scheme is composed of four algorithms: Setup, Encrypt, KeyGen, and Decrypt.

- **Setup:** Taking as input a security parameter $\lambda$ and a universe of attributes $\{A_1, A_2, \ldots, A_n\}$, the setup algorithm outputs public parameters $MPK$ and a master secret key $MSK$.
- **Encrypt:** Taking as input an access structure $\mathbb{P}$, public parameters $MPK$ and a message $M$, the encryption algorithm $\mathsf{Enc}[\mathbb{P}, M]$ outputs a ciphertext $C$.
- **KeyGen:** Taking as input an attribute set $\mathbb{A}$, public parameters $MPK$ and the master secret key $MSK$, the key generation algorithm outputs the decryption key of $\mathbb{A}$, which is denoted by $sk_{\mathbb{A}}$.
- **Decrypt:** Taking as input a ciphertext $C$ generated with access policy $\mathbb{P}$, public parameters $MPK$ and the decryption key $sk_{\mathbb{A}}$ corresponding to the attribute set $\mathbb{A}$, the decryption algorithm $\mathsf{Dec}[C, \mathbb{P}, sk_{\mathbb{A}}, \mathbb{A}]$ outputs the message $M$ or outputs $\perp$.

The correctness of CP-ABE must satisfy that for any $(MPK, MSK)$, ciphertext $\mathsf{Enc}[\mathbb{P}, M]$ and $sk_{\mathbb{A}}$, if $\mathbb{P} \subseteq \mathbb{A}$, the decryption algorithm always outputs the corrected message $M$. Otherwise, the message in $\mathsf{Enc}[\mathbb{P}, M]$ cannot be decrypted using $sk_{\mathbb{A}}$.

### C. Security Model

Let $\mathcal{A}$ be the adversary who tries to attack an encrypted message without a decryption key whose attributes satisfy the message's access policy. The game between an adversary and a challenger is described as follows.

- Initiation: The adversary outputs the $n$-bit string of access policy $\mathbb{P}^*$ that it wants to attack.
- Setup: The challenger generates a key pair $(MPK, MSK)$ with a security parameter $\lambda$, and sends $MPK$ to the adversary.
- Query: The adversary can make the following queries to the challenger.
  - the decryption key $sk_{\mathbb{A}_i}$ of any attribute set $\mathbb{A}_i$.
  - the decryption query on ciphertext $\mathsf{Enc}[\mathbb{P}_i, M_i]$.
- Challenge: In this phase, the adversary outputs $(M_0, M_1)$ for challenge. It requires the adversary did not query a decryption key on an attribute set $\mathbb{A}$ satisfying $\mathbb{P}^* \subseteq \mathbb{A}$. The challenger responds by picking a random $c^* \in \{0, 1\}$ and computing the ciphertext $\mathsf{Enc}[\mathbb{P}^*, M_{c^*}]$ for challenge to the adversary.
- Query: The adversary can continue decryption key queries and decryption queries except with a decryption key query on any $\mathbb{A}$ satisfying $\mathbb{P}^* \subseteq \mathbb{A}$ and the decryption query on $\mathsf{Enc}[\mathbb{P}^*, M_{c^*}]$.
- The adversary outputs a guess $c_g^*$ of $c^*$ and wins the game if $c_g^* = c^*$.

In the above game, we let $\epsilon = \Pr[c_g^* = c^*] - \frac{1}{2}$ be the advantage of adversary.

*Definition 2:* The CP-ABE scheme is $(t, q_e, q_c, \epsilon)$ selectively secure against chosen-ciphertext attack if for all $t$-polynomial time adversaries who make $q_e$ decryption key queries at most and $q_c$ decryption queries at most, we have $\epsilon$ is a negligible function of $\lambda$.

### D. Cryptographic Background

Let $\mathbb{BG} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, p, e)$ be the bilinear pairing group. More precisely, $\mathbb{G}_1, \mathbb{G}_2$ are the elliptic group, and $\mathbb{G}_T$ is the multiplicative group. The three groups are of the

same order $p$. $g_1$ is a generator of $\mathbb{G}_1$ and $g_2$ is a generator of $\mathbb{G}_2$. $e$ is the bilinear map capturing the three properties:

- For all $g \in \mathbb{G}_1, h \in \mathbb{G}_2$ and $a, b \in \mathbb{Z}_p$, we have
$$e(g^a, h^b) = e(g, h)^{ab}.$$
- If $g$ is a generator of $\mathbb{G}_1$ and $h$ is a generator of $\mathbb{G}_2$, we have $e(g, h)$ is a generator of $\mathbb{G}_T$.
- There exists an efficient algorithm to compute $e(g, h)$ for all $g \in \mathbb{G}_1, h \in \mathbb{G}_2$.

## III. Our CP-ABE With Constant-Size Keys

In this section, we give the construction of CP-ABE with constant-size keys. The decryption key of an attribute set $\mathbb{A}$ is composed of one group element from $\mathbb{G}_1$ and another group element from $\mathbb{G}_2$, which is independent of the number of attributes in $\mathbb{A}$.

### A. Proposed Scheme

*1) Setup:* Taking as input a security parameter $\lambda$ and a universe of attributes $\{A_1, A_2, \ldots, A_n\}$ and supposing the attribute $A_i$ is mapped to the index $i$ for all $i = 1, 2, \ldots, n$, the setup algorithm works as follows.

- Choose a pairing group $\mathbb{BG} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, e)$ and its two random generators $g \in \mathbb{G}_1$ and $h \in \mathbb{G}_2$. Compute $e(g, h)$.
- Pick a random $\alpha \in \mathbb{Z}_p$ and compute $v_i, h_i$ as follows.
$$v_i = g^{\alpha^i} \text{ for all } i = 1, 2, \ldots, n,$$
$$h_i = h^{\alpha^i} \text{ for all } i = 1, 2, \ldots, n.$$
- Select four collision-resistant hash functions:
$$H_1, H_4 : \{0,1\}^* \to \mathbb{Z}_p^*$$
$$H_2 : \{0,1\}^* \to \{0,1\}^{l_\sigma}$$
$$H_3 : \{0,1\}^* \to \{0,1\}^{l_m}$$
Here, $l_\sigma$ denotes the length of a random string under the security parameter and $l_m$ denotes the length of message (data).

The parameters $(MPK, MSK)$ are set as

$$MPK = \big(v_i, h, h_i, e(g,h), \mathbb{BG}, H_1, H_2, H_3, H_4\big),$$
$$MSK = (\alpha, g).$$

*2) Encrypt:* Our encryption is based the Fujisaki-Okamoto approach for the security against chosen-ciphertext adversary [34]:

$$\mathsf{E}\big(\sigma, H_4(\mathbb{P}, M, \sigma)\big), H_3(\sigma) \oplus M,$$

where $\mathsf{E}\big(\sigma, H_4(\mathbb{P}, M, \sigma)\big)$ denotes an attribute-based encryption on $\sigma$ using the hashing output $r = H_4(\mathbb{P}, M, \sigma)$ as the random number. More precisely, $\sigma$ is encrypted with $e(g, h)^r$, denoted by $C_3$ in our ciphertext. The ciphertext also consists of other components $(C_1, C_{2,1}, C_{2,2}, \ldots, C_{2,n-|\mathbb{P}|+1})$ for decryptors with a valid decryption key to compute $e(g, h)^r$. The encryption algorithm formally defines as follows.

Taking as input a message $M$, $MPK$ and an access policy $\mathbb{P}$ ($|\mathbb{P}| \neq 0$), the encryption algorithm works as follows.

- Pick a random $\sigma \in \{0,1\}^{l_\sigma}$ and compute
$$r = H_4(\mathbb{P}, M, \sigma).$$
- Let $\mathbb{P} = b_1 b_2 \cdots b_n$ be the policy string. Compute $f(x, \mathbb{P})$ as
$$f(x, \mathbb{P}) = \prod_{i=1}^{n} \big(x + H_1(i)\big)^{1-b_i},$$
where $f(x, \mathbb{P})$ is an $(n-1)$-degree at most polynomial function in $\mathbb{Z}_p[x]$. Let $f_i$ be the coefficient of $x^i$.
- Compute $C_1$ as
$$C_1 = \Big(h^{f(\alpha, \mathbb{P})}\Big)^r = \Big(h^{f_0} \prod_{i=1}^{n-1} h_i^{f_i}\Big)^r.$$
- Compute $C_{2,i}$ for all $i = 1, 2, \ldots, n - |\mathbb{P}| + 1$ as
$$C_{2,i} = v_i^r.$$
- Compute $e(g, h)^r$ and $(C_3, C_4)$ as
$$C_3 = H_2\big(e(g,h)^r\big) \oplus \sigma$$
$$C_4 = H_3(\sigma) \oplus M.$$
- Output the ciphertext on $M$ as
$$\Big(\mathbb{P},\ C_1, C_{2,1},\ C_{2,2}, \ldots, C_{2,n-|\mathbb{P}|+1},\ C_3,\ C_4\Big).$$

*3) KeyGen:* Taking as input an attribute set $\mathbb{A}$, $MPK$ and the master secret key $MSK$, the key generation algorithm works as follows.

- Let $\mathbb{A} = a_1 a_2 \cdots a_n$ be the attribute string. Compute $f(\alpha, \mathbb{A})$ as
$$f(\alpha, \mathbb{A}) = \prod_{i=1}^{n} \Big(\alpha + H_1(i)\Big)^{1-a_i},$$
where $f(x, \mathbb{A})$ is an $n$-degree at most polynomial function in $\mathbb{Z}_p[x]$.
- Pick a random $s \in \mathbb{Z}_p$ and generate the decryption key for $\mathbb{A}$ as
$$sk_{\mathbb{A}} = \Big(g^{\frac{s}{f(\alpha, \mathbb{A})}},\ \ h^{\frac{s-1}{\alpha}}\Big).$$

According to the definition of polynomial functions $f(x, \mathbb{A})$ in the key generation and $f(x, \mathbb{P})$ in the encryption, we have

$$\frac{f(x, \mathbb{P})}{f(x, \mathbb{A})} = \prod_{i=1}^{n} \Big(x + H_1(i)\Big)^{a_i - b_i}.$$

If $\mathbb{P} \subseteq \mathbb{A}$, it is not hard to verify that $\frac{f(x,\mathbb{P})}{f(x,\mathbb{A})}$ is a polynomial function in $x$. Otherwise, it is not a polynomial. We design the encryption and decryption key in the way that $\frac{f(x,\mathbb{P})}{f(x,\mathbb{A})}$ must be a polynomial for a successful decryption.

*4) Decrypt:* The main task of decryption is to compute $e(g,h)^r$, which is used to compute $\sigma$ for extracting message $M$. The decryption algorithm is defined as follows.

- If $\mathbb{A} = a_1 a_2 \cdots a_n$ does not fulfil the policy $\mathbb{P}$, abort. Otherwise, compute $c_i$ for $i = 1, 2, \ldots, n$ as
$$c_i = a_i - b_i \in \{0, 1\}.$$
Let $F(x, \mathbb{A}, \mathbb{P})$ be the $(n-|\mathbb{P}|)$-degree at most polynomial function in $\mathbb{Z}_p[x]$ defined as
$$F(x) = F(x, \mathbb{A}, \mathbb{P}) = \prod_{i=1}^{n} \big(x + H_1(i)\big)^{c_i},$$
and $F_i \in \mathbb{Z}_p$ be the coefficient of $x^i$. We have $F_0 \neq 0$.
- Compute $(U, V, W)$ as
$$U = e\big(C_{2,1}, \prod_{i=1}^{n-|\mathbb{P}|} h_{i-1}^{F_i}\big) = e(g,h)^{rF(\alpha)-rF_0}$$
$$V = e\big(\prod_{i=1}^{n-|\mathbb{P}|+1} C_{2,i}^{F_{i-1}}, h^{\frac{s-1}{\alpha}}\big) = e(g,h)^{rsF(\alpha)-rF(\alpha)}$$
$$W = e\big(g^{\frac{s}{f(\alpha,\mathbb{A})}}, C_1\big) = e(g,h)^{rsF(\alpha)}.$$
- Compute
$$e(g,h)^r = \Big(\frac{W}{U \cdot V}\Big)^{\frac{1}{F_0}}.$$
- Compute the random number $\sigma$ by
$$\sigma = H_2\big(e(g,h)^r\big) \oplus C_3$$
and the message $M$ by
$$M = H_3(\sigma) \oplus C_4.$$
- Compute $r = H_4(\mathbb{P}, M, \sigma)$ and verify whether the ciphertext is encrypted with $r$. If it is false, output $\perp$; otherwise, output $M$ as the decryption of the ciphertext.

### *B. Correctness*

The correctness of our encryption and decryption is showed as follows.

$$f(x, \mathbb{P}) = \prod_{i=1}^{n} (x + H_1(i))^{1-b_i},$$
$$f(x, \mathbb{A}) = \prod_{i=1}^{n} (x + H_1(i))^{1-a_i},$$
$$\frac{f(x,\mathbb{P})}{f(x,\mathbb{A})} = \prod_{i=1}^{n} (x + H_1(i))^{(1-b_i)-(1-a_i)} = \prod_{i=1}^{n} (x + H_1(i))^{a_i-b_i} = \prod_{i=1}^{n} (x + H_1(i))^{c_i}.$$

Therefore, we have

$$F(x) = F(x, \mathbb{A}, \mathbb{P}) = \prod_{i=1}^{n} (x + H_1(i))^{c_i} = \frac{f(x,\mathbb{P})}{f(x,\mathbb{A})}.$$

and $F(x)$ is a polynomial function when $c_i \in \{0, 1\}$ holds for all $i = 1, 2, \ldots, n$. The equations of $(U, V, W)$ and $e(g,h)^r$ are correct because

$$\begin{aligned} U &= e\big(C_{2,1}, \prod_{i=1}^{n-|\mathbb{P}|} h_{i-1}^{F_i}\big) \\ &= e\big(g^{r\alpha}, \prod_{i=1}^{n-|\mathbb{P}|} h^{\alpha^{i-1}F_i}\big) \\ &= e(g,h)^{r\sum_{i=1}^{n-|\mathbb{P}|}\alpha^i F_i + rF_0 - rF_0} \\ &= e(g,h)^{rF(\alpha)-rF_0}, \\ V &= e\big(\prod_{i=1}^{n-|\mathbb{P}|+1} C_{2,i}^{F_{i-1}}, h^{\frac{s-1}{\alpha}}\big) \\ &= e\big(g^{r\alpha F(\alpha)}, h^{\frac{s-1}{\alpha}}\big) \\ &= e(g,h)^{rsF(\alpha)-rF(\alpha)}, \\ W &= e\big(g^{\frac{s}{f(\alpha,\mathbb{A})}}, C_1\big) \\ &= e\big(g^{\frac{s}{f(\alpha,\mathbb{A})}}, h^{rf(\alpha,\mathbb{P})}\big) \\ &= e(g,h)^{rsF(\alpha)}, \\ \Big(\frac{W}{UV}\Big)^{\frac{1}{F_0}} &= \Big(\frac{e(g,h)^{rsF(\alpha)}}{e(g,h)^{rF(\alpha)-rF_0} e(g,h)^{rsF(\alpha)-rF(\alpha)}}\Big)^{\frac{1}{F_0}} \\ &= \Big(e(g,h)^{rF_0}\Big)^{\frac{1}{F_0}} \\ &= e(g,h)^r. \end{aligned}$$

## IV. Efficiency

In this section, we compare our scheme to other proposed ABE schemes in the literature.

The decryption key of our scheme is composed of two group elements only, and is independent of the number of attributes. The ciphertext mainly has $n-|\mathbb{P}|+2$ group elements depending on the total attribute number and the number of attributes in access policy.

Table I shows the comparison of recently proposed attribute-based encryption schemes in terms of policy type, access structure, security model, length of decryption key and length of ciphertext. We compare the efficiency of schemes under CPA (chosen plaintext attack) security only as previous schemes utilized different generalized security transformation from CPA to CCA. In this table, $|\mathbb{A}|$ denotes the number of attributes of a user and $|\mathbb{P}|$ denotes the number of attributes of access policy. We use $\mathbb{G}$ to denote the elliptic groups of $\mathbb{G}_1$ and $\mathbb{G}_2$ for prime-order bilinear pairing, and use $\mathbb{G}_c, \mathbb{G}_{T_c}$ to denote composite-order pairing. The comparison shows that only our scheme and the scheme proposed in [15] achieve constant-size decryption keys.

However, our scheme provides a more expressive access structure compared to [15]. Notice that [15] admits only $(n, n)$-threshold decryption policies [17]. In their scheme, a decryption key associated with attribute set $\mathbb{A}$ can only decrypt a ciphertext generated from an access policy $\mathbb{P}$ fulfilling $\mathbb{A} = \mathbb{P}$. While in our CP-ABE scheme, a decryption key associated with attribute set $\mathbb{A}$ can decrypt a ciphertext under any access policy $\mathbb{P}$ satisfying $\mathbb{P} \subseteq \mathbb{A}$.

We notice that it is not hard to construct CP-ABE with $\mathbb{A} = \mathbb{P}$ access structure, where the attribute set $\mathbb{A}$ of a decryption key must be equivalent to the access polity $\mathbb{P}$. We can merely use a traditional identity-based encryption scheme to achieve this CP-ABE by setting $\mathbb{A} = ID$ and $\mathbb{P} = ID'$ as unique identities. A message encrypted with $ID'$ is decrypted with the decryption key of $ID$ when $ID = ID'$. The only problem we need to address is how to map an attribute set $\mathbb{A}$ into a unique string $ID$. Let $\mathbb{A} = \{A_1, A_2, \ldots, A_n\}$ and $H$ be a collision-resistant hash function. We set $ID$ to be the output of $H(A_{i_1}, A_{i_2}, \ldots, A_{i_n})$ for $H(A_{i_1}) < H(A_{i_2}) < \cdots < H(A_{i_n})$. It is not hard to verify that such a modification from any IBE can be used to construct CP-ABE with $\mathbb{A} = \mathbb{P}$ access structure.

Our proposed CP-ABE scheme is feasible for key storage in lightweight devices with limited-memory storage, like passive tags in RFID system. Suppose an RFID tag should carry both possessed attributes $\mathbb{A}$ and the corresponding decryption key $sk_{\mathbb{A}}$. We can choose the pairing group $\mathbb{G}_1$ with 160 bits and $\mathbb{G}_2$ with 512 bits (under compression [35]) for 80-bit security so that $|sk_{\mathbb{A}}| = |\mathbb{G}_1| + |\mathbb{G}_2| = 672$ bits. Suppose the total attribute number is $n = 1000$, we have $|\mathbb{A}| = 1000$. We yield $|\mathbb{A} + sk_{\mathbb{A}}| = 1672$ bits. This is applicable for passive tags whose memory size has a few kilo bits only [1].

Our scheme is also comparable to other proposed ABE schemes (Table I) in terms of computational efficiency. Our decryption key generation for each attribute set only costs two point multiplications, which is independent of the number of attributes and is much more efficient than the others with linear size decryption keys. Since $f(x, \mathbb{P})$ is an $(n - |\mathbb{P}|)$-degree polynomial, our encryption therefore costs about $2(n - |\mathbb{P}|)$ point multiplications. We have $F(x, \mathbb{A}, \mathbb{P})$ is an $(|\mathbb{A}| - |\mathbb{P}|)$-degree polynomial, and hence our decryption mainly costs about $2(|\mathbb{A}| - |\mathbb{P}|)$ point multiplications and three pairing computations. Both encryption and decryption are still efficient in linear time. We note that the efficiency of encryption and decryption in other schemes are also with regards to the input attribute number or threshold number. Our scheme offers short decryption key and therefore it does not trade off the computational efficiency.

## V. Security

Before proving the security of our CP-ABE scheme, we define the adopted hard problem for security reduction. The hard problem we adopt is modified from the aMSE-DDH problem defined in [17].

Let the pairing group be $\mathbb{BG} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$. Let $f(x)$ and $g(x)$ be two co-prime polynomials in $\mathbb{Z}_p[x]$ with respective orders $q_1, q_2$. Let $g_0$ be a generator of $\mathbb{G}_1$ and $h_0$ be a generator of $\mathbb{G}_2$. Given

$$
\begin{array}{llllll}
g_0, & g_0^{\alpha}, & g_0^{\alpha^2}, & \ldots, & g_0^{\alpha^{q_1-1}} & \\
h_0, & h_0^{\alpha}, & h_0^{\alpha^2}, & \ldots, & h_0^{\alpha^n} & \\
g_0^{\omega}, & g_0^{\omega\alpha}, & g_0^{\omega\alpha^2}, & \ldots, & g_0^{\omega\alpha^{q_1}} & \\
h_0^{\omega}, & h_0^{\omega\alpha}, & h_0^{\omega\alpha^2}, & \ldots, & h_0^{\omega\alpha^n} & \\
g_0^{\alpha f(\alpha)}, & g_0^{\alpha^2 f(\alpha)}, & \ldots, & g_0^{\alpha^n f(\alpha)} & & \\
g_0^{\gamma\alpha f(\alpha)}, & g_0^{\gamma\alpha^2 f(\alpha)}, & \ldots, & g_0^{\gamma\alpha^n f(\alpha)}, & h_0^{\gamma g(\alpha)} &
\end{array}
$$

and $T \in \mathbb{G}_T$, the $(q_1, q_2, n)$-aMSE-DDH problem is deciding whether $T$ is equal to $e(g_0, h_0)^{\gamma f(\alpha)}$ or is a random group element in $\mathbb{G}_T$.

*Definition 3:* The $(q_1, q_2, n)$-aMSE-DDH problem is $(t, \epsilon)$-hard if for all $t$-polynomial time adversaries, the maximum advantage of solving this problem is $\epsilon$.

The intractability of the modified $(q_1, q_2, n)$-aMSE-DDH is covered by the analysis in [2]. Here, we give the intractability analysis based on the generic group model analysis in [2].

Given the challenge instance, one can compute

$$g_0^{A(\alpha)}, \quad g_0^{\alpha B(\alpha) f(\alpha)}, \quad h_0^{C(\alpha)}, \quad g_0^{\gamma\alpha D(\alpha) f(\alpha)},$$

where

$$
\begin{aligned}
&A(x) \text{ is any } (q_1 - 1)\text{-degree polynomial,}\\
&B(x) \text{ is any } (n - 1)\text{-degree polynomial,}\\
&C(x) \text{ is any } (n - 1)\text{-degree polynomial,}\\
&D(x) \text{ is any } (n - 1)\text{-degree polynomial.}
\end{aligned}
$$

With the additional element $h_0^{\gamma g(\alpha)}$, one can further compute

$$
\begin{aligned}
&e(g_0, h_0)^{\gamma A(\alpha) g(\alpha)},\\
&e(g_0, h_0)^{\gamma\alpha B(\alpha) f(\alpha) g(\alpha)},\\
&e(g_0, h_0)^{\gamma\alpha C(\alpha) D(\alpha) f(\alpha)},
\end{aligned}
$$

where all of them contain the unknown $\gamma$.

If $e(g_0, h_0)^{\gamma f(\alpha)}$ can be computed from the above combinations, we should have

$$
\begin{aligned}
\gamma f(\alpha) = {} & \gamma A(\alpha) g(\alpha) + \gamma\alpha B(\alpha) f(\alpha) g(\alpha)\\
& + \gamma\alpha C(\alpha) D(\alpha) f(\alpha).
\end{aligned}
$$

That is, the polynomial $f(x)$ can be re-written into

$$
\begin{aligned}
f(x) &= A(x) g(x) + x B(x) f(x) g(x) + x C(x) D(x) f(x)\\
&= A(x) g(x) + f(x)\big(x B(x) g(x) + x C(x) D(x)\big)
\end{aligned}
$$

We deduce $f(x) | A(x)$ due to the co-prime of $f(x)$ and $g(x)$. Since the degree of $A(x)$ is less than $f(x)$, we have $A(x) \equiv 0$. Therefore, $f(x)$ can be further simplified as

$$f(x) = f(x)\big(x B(x) g(x) + x C(x) D(x)\big).$$

Obviously, from the above, we deduce

$$E(x) = x B(x) g(x) + x C(x) D(x) \equiv 1.$$

On the other hand, we have $E(0) = 0$ which contradicts $E(x) \equiv 1$. This contradiction indicates that $e(g_0, h_0)^{\gamma f(\alpha)}$ cannot be computed from the challenge instance.

*Theorem 1:* Our CP-ABE scheme is $(t, q_e, q_c, \epsilon)$ selectively secure if the $(q_1, q_2, n)$-aMSE-DDH problem is $(t', \epsilon')$-hard.

$$
\begin{aligned}
&t' = t + O(n q_e t_e + n q_{H_4} t_e),\ \epsilon' = \epsilon - \frac{q_{H_2}}{p},\\
&q_1 = |\mathbb{P}^*|,\ q_2 = n - |\mathbb{P}^*|,
\end{aligned}
$$

where $t_e$ denotes the average time of a point multiplication, $q_{H_2}, q_{H_4}$ denotes the number of queries to the random oracles $H_2$ and $H_4$, and $|\mathbb{P}^*|$ denotes the number of attributes in $\mathbb{P}^*$.

*Proof:* Suppose there exists an adversary who can break the security with advantage $(t, q_e, q_c, \epsilon)$. We construct an

algorithm $\mathcal{B}$ that solves the $(q_1, q_2, n)$-aMSE-DDH problem with advantage $(t', \epsilon')$ at least. The algorithm $\mathcal{B}$ is given the challenge input and the aim is to output $T = 1$ or 0. The algorithm $\mathcal{B}$ interacts with the adversary $\mathcal{A}$ as below.

**Initization:** The adversary outputs the access policy $\mathbb{P}^*$ to be challenged, where there are $n$ attributes in total. Let $\mathbb{P}^* = b_1 b_2 \cdots b_n$. $\mathcal{B}$ will set

$$f(x, \mathbb{P}^*) = \prod_{i=1}^{n} \big(x + H_i(i)\big)^{1-b_i} = g(x),$$
$$\prod_{i=1}^{n} \big(x + H_i(i)\big)^{b_i} = f(x),$$

where $g(x)$ is a $(n - |\mathbb{P}^*|)$-degree polynomial function, and therefore the degree of $f(x)$ is $|\mathbb{P}^*|$.

**Setup:** $\mathcal{B}$ sets the master secret key the same as $\alpha$ in the challenge instance. Then, the other components of public parameters are simulated as follows.

$$\begin{aligned} h &= h_0, \\ h_i &= h^{\alpha^i} = h_0^{\alpha^i}, \\ v_i &= g^{\alpha^i} = g_0^{\alpha^i f(\alpha)}, \\ e(g,h) &= e(g_0, h_0)^{f(\alpha)}. \end{aligned}$$

All $(v_i, h_i)$ directly come from the change instance. $e(g,h)$ is simulated from $g_0, g_0^{\alpha}, \ldots, g_0^{\alpha^{q_1-1}}$ and $h_0, h_0^{\alpha}, f(x)$. $\mathcal{B}$ computes and gives these parameters to the adversary excepting the four hash functions set as random oracles.

**Hash Queries:** The adversary can access the four random oracles $H_1, H_2, H_3, H_4$. $\mathcal{B}$ maintains four lists $\mathcal{L}_{H_1}, \mathcal{L}_{H_2}, \mathcal{L}_{H_3}, \mathcal{L}_{H_4}$ to record the query and response, respectively. If the query has been responded and recorded in the list, $\mathcal{B}$ responds with the same result. For new queries, $\mathcal{B}$ works as follows.

- $H_1$: Let the query to $H_1$ be $i$. If $i \notin [1, n]$, $\mathcal{B}$ responds $H_1(i)$ with a random number in $\mathbb{Z}_p$. Otherwise, for $i \in [1, n]$. Let $\mathbb{P}^* = b_1 b_2 \cdots b_n$. It follows into two cases:
  - $b_i = 0$, $\mathcal{B}$ responds $H_1(i)$ with a new root of $g(x)$.
  - Otherwise $b_i = 1$, $\mathcal{B}$ responds $H_1(i)$ with a new root of $f(x)$.
- $H_2$: Let the query to $H_2$ be $e(g,h)^{r_i'}$. $\mathcal{B}$ responds $H_2(e(g,h)^{r_i'})$ with a random $R_i \in \{0,1\}^{l_\sigma}$.
- $H_3$: Let the query to $H_3$ be $t_i$. $\mathcal{B}$ responds $H_3(t_i)$ with a random $Q_i \in \{0,1\}^{l_m}$.
- $H_4$: Let the query to $H_4$ be $(\mathbb{P}_i, M_i, t_i)$. $\mathcal{B}$ responds $H_4(\mathbb{P}_i, M_i, t_i)$ with a random $r_i \in \mathbb{Z}_p^*$.

**Query:**

For a decryption key query on $\mathbb{A}_i = a_1 a_2 \cdots a_n$, we can write $f(x, \mathbb{A}_i)$ into

$$\begin{aligned} f(x, \mathbb{A}_i) &= \sum_{i=1}^{n} \big(x + H_1(i)\big)^{1-a_i} \\ &= f_{f(x)}(x, \mathbb{A}_i) \cdot f_{g(x)}(x, \mathbb{A}_i), \end{aligned}$$

where all roots of $f_{f(x)}(x, \mathbb{A}_i)$ are from $f(x)$, and all roots of $f_{g(x)}(x, \mathbb{A}_i)$ are from $g(x)$. If $\mathbb{A}_i$ does not satisfy the access policy $\mathbb{P}^*$, we must have the degree of $f_{f(x)}(x, \mathbb{A}_i)$ is nonzero.

Let $f_{g(x)}(0, \mathbb{A}_i) = f_g(0)$. $\mathcal{B}$ randomly chooses $s_i \in \mathbb{Z}_p$ and sets

$$\begin{aligned} f^1_{\mathbb{A}_i}(x) &= \frac{f(x)}{f(x, \mathbb{A}_i)} \cdot f_{g(x)}(x, \mathbb{A}_i)\Big(s_i \omega x + \frac{1}{f_g(0)}\Big) \\ &= \frac{f(x)}{f_{f(x)}(x, \mathbb{A}_i)} \cdot \Big(s_i \omega x + \frac{1}{f_g(0)}\Big) \\ &= \frac{f(x)}{f_{f(x)}(x, \mathbb{A}_i)} \cdot s_i \omega x + \frac{f(x)}{f_{f(x)}(x, \mathbb{A}_i)} \cdot \frac{1}{f_g(0)}, \\ f^2_{\mathbb{A}_i}(x) &= \frac{f_{g(x)}(x, \mathbb{A}_i)(s_i \omega x + \frac{1}{f_g(0)}) - 1}{x} \\ &= s_i \omega f_{g(x)}(x, \mathbb{A}_i) + \frac{\frac{f_{g(x)}(x, \mathbb{A}_i)}{f_g(0)} - 1}{x}. \end{aligned}$$

We have

$$\frac{f(x)}{f_{f(x)}(x, \mathbb{A}_i)} \cdot s_i \omega x = \omega \cdot f^{1,1}_{\mathbb{A}_i}(x),$$

where $f^{1,1}_{\mathbb{A}_i}(x)$ is a $q_1$-degree at most polynomial function;

$$\frac{f(x)}{f_{f(x)}(x, \mathbb{A}_i)} \cdot \frac{1}{f_g(0)} = f^{1,2}_{\mathbb{A}_i}(x),$$

where $f^{1,2}_{\mathbb{A}_i}(x)$ is a $(q_1 - 1)$-degree at most polynomial function;

$$s_i \omega f_{g(x)}(x, \mathbb{A}_i) = \omega \cdot f^{2,1}_{\mathbb{A}_i}(x),$$

where $f^{2,1}_{\mathbb{A}_i}(x)$ is a $q_2$-degree at most polynomial function;

$$\frac{\frac{f_{g(x)}(x, \mathbb{A}_i)}{f_g(0)} - 1}{x} = 0 \text{ or } f^{2,2}_{\mathbb{A}_i}(x),$$

where $f^{2,2}_{\mathbb{A}_i}(x)$ is a $(q_2 - 1)$-degree at most polynomial function.

$\mathcal{B}$ computes $sk_{\mathbb{A}_i}$ as

$$\begin{aligned} sk_{\mathbb{A}_i} &= (d_1, d_2) \\ &= \Big(g_0^{f^1_{\mathbb{A}_i}(\alpha)},\ h_0^{f^2_{\mathbb{A}_2}(\alpha)}\Big) \\ &= \Big(g_0^{\omega f^{1,1}_{\mathbb{A}_i}(\alpha) + f^{1,2}_{\mathbb{A}_i}(\alpha)},\ h_0^{\omega f^{2,1}_{\mathbb{A}_i}(\alpha) + f^{2,2}_{\mathbb{A}_i}(\alpha)}\Big), \end{aligned}$$

where $d_1, d_2$ are computed as follows.

$$\begin{aligned} g_0^{\omega f^{1,1}_{\mathbb{A}_i}(\alpha)} &\longleftarrow g_0^{\omega}, g_0^{\alpha\omega}, \ldots, g_0^{\alpha^{q_1}\omega}, f^{1,1}_{\mathbb{A}_i}(x). \\ g_0^{f^{1,2}_{\mathbb{A}_i}(\alpha)} &\longleftarrow g_0, g_0^{\alpha}, \ldots, g_0^{\alpha^{q_1-1}}, f^{1,2}_{\mathbb{A}_i}(x). \\ h_0^{\omega f^{2,1}_{\mathbb{A}_i}(\alpha)} &\longleftarrow h_0^{\omega}, h_0^{\alpha\omega}, \ldots, h_0^{\alpha^{q_2}\omega}, f^{2,1}_{\mathbb{A}_i}(x). \\ h_0^{f^{2,2}_{\mathbb{A}_i}(\alpha)} &\longleftarrow h_0, h_0^{\alpha}, \ldots, h_0^{\alpha^{q_2-1}}, f^{2,2}_{\mathbb{A}_i}(x). \end{aligned}$$

Let $s' = f_{g(\alpha)}(\alpha, \mathbb{A}_i)(s_i \omega \alpha + \frac{1}{f_g(0)})$, we have

$$\begin{aligned} g^{\frac{s'}{f(\alpha, \mathbb{A}_i)}} &= g_0^{f^1_{\mathbb{A}_i}(\alpha)}, \\ h^{\frac{s'-1}{\alpha}} &= h_0^{f^2_{\mathbb{A}_i}(\alpha)}, \end{aligned}$$

which is a valid decryption key on $\mathbb{A}_i$. $\mathcal{B}$ computes the decryption key and sends it to the adversary.

For any decryption query on $\mathsf{Enc}[\mathbb{P}_i, M_i]$, if there exist $(\mathbb{P}_i, M_i, t_i, r_i, R_i, Q_i)$ in the query lists such that the ciphertext is generated using $r_i$, $\mathcal{B}$ outputs $M_i$ as the decryption query. Otherwise, $\mathcal{B}$ outputs $\perp$. No query will be aborted since all valid encryptions need the response from hash oracles, and the response contains the random number $r_i$ used in encryption.

**Challenge:** The adversary outputs $(M_0, M_1)$ for challenge where all queried decryption keys do not fulfil the access policy $\mathbb{P}^*$. $\mathcal{B}$ randomly chooses $R^* \in \{0,1\}^{l_\sigma}$, $Q^* \in \{0,1\}^{l_m}$ and computes the challenge ciphertext as

$$\begin{aligned} C_1^* &= h_0^{\gamma g(\alpha)}, \\ C_{2,i}^* &= g_0^{\gamma \alpha^i f(\alpha)}, \\ C_3 &= R^*, \\ C_4 &= Q^*. \end{aligned}$$

Let the random number $r$ be $r = \gamma$, we have

$$\begin{aligned} C_1^* &= h_0^{\gamma g(\alpha)} = (h^{f(\alpha,\mathbb{P}^*)})^r, \\ C_{2,i}^* &= g_0^{\gamma \alpha^i f(\alpha)} = g^{\gamma \alpha^i} = v_i^r. \end{aligned}$$

$(C_1^*, C_{2,1}^*, \ldots, C_{2,n-|\mathbb{P}^*|+1}^*)$ is a valid encryption of policy $\mathbb{P}^*$ with random number $r$.

If $T = e(g_0, h_0)^{\gamma f(\alpha)}$, we have

$$e(g,h)^r = e(g_0^{f(\alpha)}, h_0)^\gamma = T.$$

Under random oracles, the adversary must be able to compute $e(g,h)^r$ and then query it to $H_2$ for decryption.

**Query:** The response of this phase is the same as the former phase with the restriction that no decryption key query fulfilling the challenge policy and no decryption query on the challenge ciphertext.

**Guess:** The adversary outputs a guess of $c_g^*$ and $\mathcal{B}$ outputs 1 if there exists a query on $T$ to the $H_2$ oracle; otherwise, $T$ is a random group element in $\mathbb{G}_T$.

In the guess phase, if the adversary can break the encryption with advantage $\epsilon$, $e(g,h)^r$ appears in the $\mathcal{L}_{H_2}$ list with probability $\epsilon + 1/2$ at least. The only error event is that $T$ is a random group element but it is queried to $H_2$ oracle. This occurs with probability $q_{H_2}/p$ at most. Therefore, $\mathcal{B}$ can distinguish $T = 1$ or $T = 0$ with advantage $\epsilon - q_{H_2}/p$ at least.

The simulation time is dominated by the decryption key generation and the decryption. Each key generation requires $O(n)$ point multiplications, and all decryption requires $O(q_{H_4} n)$ point multiplications, where $q_{H_4}$ denotes the query number of the $H_4$ oracle. We therefore obtain the Theorem 1 and prove the security of our proposed scheme. ■

## VI. Conclusion

Lightweight devices usually have a limited-memory storage, which could be too small to store the decryption keys of CP-ABE schemes, as the key size of existing CP-ABE schemes is linear to or dependent on the number of users' attributes. In this work, we proposed a provably secure CP-ABE scheme with AND gates access structure. Our CP-ABE scheme offers a constant-size decryption key whose length can be as small as 672 bits (80-bit security). The comparison showed that our scheme is the only expressive CP-ABE in which the decryption key can be stored in lightweight devices.

## Acknowledgment

We would like to thank the reviewers for their invaluable comments which have led to improvement of this work.

## References

[1] S. Vaudenay, "On privacy models for RFID," in *Proc. ASIACRYPT*, 2007, vol. 4833, pp. 68–87.
[2] C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys," in *Proc. ASIACRYPT*, 2007, vol. 4833, pp. 200–215.
[3] F. Guo, Y. Mu, and W. Susilo, "Identity-based traitor tracing with short private key and short ciphertext," in *Proc. ESORICS*, 2012, vol. 7459, pp. 609–626.
[4] F. Guo, Y. Mu, and Z. Chen, "Identity-based encryption: How to decrypt multiple ciphertexts using a single decryption key," in *Proc. Pairing*, 2007, vol. 4575, pp. 392–406.
[5] F. Guo, Y. Mu, Z. Chen, and L. Xu, "Multi-identity single-key decryption without random oracles," in *Proc. Inscrypt*, 2007, vol. 4990, pp. 384–398.
[6] H. Guo, C. Xu, Z. Li, Y. Yao, and Y. Mu, "Efficient and dynamic key management for multiple identities in identity-based systems," *Inf. Sci.*, vol. 221, pp. 579–590, Feb. 2013.
[7] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Proc. CRYPTO*, 2001, vol. 2139, pp. 213–229.
[8] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in *Proc. ACM Conf. Comput. Commun. Security*, 2010, pp. 735–737.
[9] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 7, pp. 1214–1221, Jul. 2011.
[10] Z. Wan, J. Liu, and R. H. Deng, "Hasbe: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 743–754, Apr. 2012.
[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conf. Comput. Commun. Security*, 2006, pp. 89–98.
[12] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Security Privacy*, May 2007, pp. 321–334.
[13] L. Cheung and C. C. Newport, "Provably secure ciphertext policy abe," in *Proc. ACM Conf. Comput. Commun. Security*, 2007, pp. 456–465.
[14] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Proc. Public Key Cryptograph.*, 2011, vol. 6571, pp. 53–70.
[15] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," in *Proc. ISPEC*, 2009, vol. 5451, pp. 13–23.
[16] Z. Zhou and D. Huang, "On efficient ciphertext-policy attribute based encryption and broadcast encryption: Extended abstract," in *Proc. ACM Conf. Comput. Commun. Security*, 2010, pp. 753–755.
[17] J. Herranz, F. Laguillaumie, and C. Ràfols, "Constant size ciphertexts in threshold attribute-based encryption," in *Proc. Public Key Cryptography*, 2010, vol. 6056, pp. 19–34.
[18] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Proc. EUROCRYPT*, 2010, vol. 6110, pp. 62–91.
[19] A. B. Lewko and B. Waters, "New proof methods for attribute-based encryption: Achieving full security through selective techniques," in *Proc. CRYPTO*, 2012, vol. 7417, pp. 180–198.
[20] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. EUROCRYPT*, 2005, vol. 3494, pp. 457–473.
[21] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proc. ACM Conf. Comput. Commun. Security*, 2007, pp. 195–203.
[22] C. Chen *et al.*, "Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures," in *Proc. CT-RSA*, 2013, vol. 7779, pp. 50–67.

[23] N. Attrapadung, B. Libert, and E. de Panafieu, "Expressive key-policy attribute-based encryption with constant-size ciphertexts," in *Proc. Public Key Cryptograph.*, 2011, vol. 6571, pp. 90–108.
[24] C. Chen, Z. Zhang, and D. Feng, "Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost," in *Proc. ProvSec*, 2011, vol. 6980, pp. 84–101.
[25] A. Ge, R. Zhang, C. Chen, C. Ma, and Z. Zhang, "Threshold ciphertext policy attribute-based encryption with constant size ciphertexts," in *Proc. ACISP*, 2012, vol. 7372, pp. 336–349.
[26] T. Okamoto and K. Takashima, "Fully secure unbounded inner-product and attribute-based encryption," in *Proc. ASIACRYPT*, 2012, vol. 7658, pp. 349–366.
[27] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in *Proc. 35th ICALP*, 2008, vol. 5126, pp. 579–591.
[28] A. Sahai and B. Waters, "Attribute-based encryption for circuits from multilinear maps," *CoRR*, vol. abs/1210.5287, 2012.
[29] M. Chase, "Multi-authority attribute based encryption," in *Proc. TCC*, 2007, vol. 4392, pp. 515–534.
[30] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in *Proc. ACNS*, 2008, vol. 5037, pp. 111–129.
[31] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in *Proc. Public Key Cryptograph.*, 2013, vol. 7778, pp. 162–179.
[32] M. J. Hinek, S. Jiang, R. Safavi-Naini, and S. F. Shahandashti, "Attribute-based encryption without key cloning," *IJACT*, vol. 2, no. 3, pp. 250–270, 2012.
[33] Z. Liu, Z. Cao, and D. Wong, "White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 76–88, Jan. 2013.
[34] E. Fujisaki and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes," in *Proc. CRYPTO*, 1999, vol. 1666, pp. 537–554.
[35] D. Freeman, M. Scott, and E. Teske, "A taxonomy of pairing-friendly elliptic curves," *J. Cryptol.*, vol. 23, no. 2, pp. 224–280, 2010.

**Fuchun Guo** received the B.S. and M.S. degrees from Fujian Normal University, China, and the Ph.D. degree from the University of Wollongong, Australia, in 2005, 2008, and 2013, respectively. He is currently an associate research fellow at the School of Computer Science and Software Engineering, University of Wollongong. His primary research interest is the public-key cryptography such as particular, protocols, encryption and signature schemes, and security proof.

**Yi Mu** (SM'03) received the Ph.D. degree from Australian National University in 1994. He is currently a Professor with the University of Wollongong. He was a Senior Lecturer with the Department of Computing, Macquarie University. He has been with the University of Wollongong since 2003. His current research interests include cryptography, network security, access control, and computer security. He was involved in the areas of quantum cryptography, quantum computers, atomic computations, and quantum optics. He is the Editor-in-Chief of the *International Journal of Applied Cryptography* and serves as an Associate Editor or Guest Editor for many international journals. He has served in program committees for a number of international security conferences, including the ACM Conference on Computer and Communications Security, the ACM Symposium on Information, Computer and Communications Security, the European Symposium on Research in Computer Security, the Australasian Conference on Information Security and Privacy, the Conference on Cryptology and Network Security, the European Public-Key Infrastructure, the International Conference on Information and Communication Systems, the International Conference on Information Security and Cryptology, the International Conference on Provable Security, and the International Conference on Information Security Practice and Experience. He is a member of the International Association for Cryptologic Research.

**Willy Susilo** (SM'01) received the Ph.D. degree in computer science from the University of Wollongong, Wollongong, Australia, where he is a Professor with the School of Computer Science and Software Engineering and the Director with the Centre for Computer and Information Security Research. He currently holds the prestigious ARC Future Fellow awarded by the Australian Research Council. His main research interests include cryptography and information security. His main contribution is in the area of digital signature schemes. He has served as a Program Committee Member in dozens of international conferences. He has authored numerous publications in the area of digital signature schemes and encryption schemes.

**Duncan S. Wong** received the B.Eng. degree from the University of Hong Kong, the M.Phil. degree from the Chinese University of Hong Kong, and the Ph.D. degree from Northeastern University, Boston, MA, USA, in 1994, 1998, and 2002, respectively. He is currently an Associate Professor with the Department of Computer Science, City University of Hong Kong. His primary research interests include cryptography, in particular, cryptographic protocols, encryption and signature schemes, and anonymous systems. He is also interested in other topics in information security, such as network security, wireless security database security, and security in cloud computing.

**Vijay Varadharajan** is a Microsoft Chair Professor of innovation in computing with Macquarie University. He is the Director of the Advanced Cyber Security Research Centre. He has been on the Editorial Board of several journals, including the IEEE TRANSACTIONS IN DEPENDABLE AND SECURE COMPUTING, the IEEE TRANSACTIONS IN CLOUD COMPUTING, the IEEE TRANSACTIONS IN INFORMATION FORENSICS AND SECURITY, and the *ACM Transactions in Information Systems Security*. He has authored more than 340 papers in international journals and conferences, coauthored and edited 10 books on security, networks, and distributed systems, and holds three patents. He is a fellow of the British Computer Society, IEE, U.K., the Institute of Mathematics and Applications, U.K., the Australian Institute of Engineers, and the Australian Computer Society. His current areas of research interest include secure distributed systems, trusted computing, Internet security, cloud computing, and mobile and wireless security.