SECURITY AND COMMUNICATION NETWORKS
*Security Comm. Networks* (2016)
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1587

RESEARCH ARTICLE

# Design of a new CP-ABE with constant-size secret keys for lightweight devices using elliptic curve cryptography

Vanga Odelu[1]* and Ashok Kumar Das[2]

[1] Department of Mathematics, Indian Institute of Technology, Kharagpur 721 302, India
[2] Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India

## ABSTRACT

The energy cost of public-key cryptography is a vital component of modern secure communications. It inhibits the widespread adoption within the ultra-low energy regimes (for example, implantable medical devices and Radio Frequency Identification tags). In the ciphertext-policy attribute-based encryption (CP-ABE), an encryptor can decide the access policy that who can decrypt the data. Thus, data will be protected from the unauthorized users. However, most of the existing CP-ABE schemes require huge storage and computational overheads. Moreover, CP-ABE schemes based on bilinear map loose high efficiency over the elliptic curve cryptography because of the requirement of the security parameters of larger size. These drawbacks prevent the use of ultra-low energy devices in practice. In this paper, we aim to propose a novel expressive AND gate access structured CP-ABE scheme with constant-size secret keys (CSSK) with cost-efficient solutions for encryption and decryption using elliptic curve cryptography, called the CP-ABE-CSSK scheme. In the proposed CP-ABE-CSSK, the size of the secret key is as small as 320 bits. In addition, elliptic curve cryptography is efficient and more suitable for lightweight devices as compared with bilinear pairing-based cryptosystem. Thus, the proposed CP-ABE-CSSK scheme provides low computation and storage overheads with an expressive AND gate access structure as compared with related existing schemes. Consequently, our scheme becomes very practical for CP-ABE key storage and computation cost for ultra-low energy devices. Copyright © 2016 John Wiley & Sons, Ltd.

**KEYWORDS**
attribute-based encryption; ciphertext-policy; constant-size secret key; elliptic curve cryptography; security
***Correspondence**
Vanga Odelu, Department of Mathematics, Indian Institute of Technology, Kharagpur 721 302, India.
E-mail: odelu.vanga@gmail.com

## 1. INTRODUCTION

Implantable medical devices (IMDs) are used to monitor and treat physiological conditions within the body of a patient. These devices, including implantable cardiac defibrillators and drug delivery systems, are useful in managing a variety of ailments, such as diabetes, cardiac arrhythmia, Parkinson's disease, and so on. IMDs pervasiveness continues to swell, with upwards of 25 million US citizens currently reliant on them for life-critical functions. The IMD needs to make its presence and type known to authorized entities, where a caregiver frequently needs to aware of an IMD's presence. For example, we need to deactivate an implantable cardiac defibrillator before a surgery happens. Thus, the Food and Drug Administration recently considers attaching remotely readable Radio Frequency Identification tags to implanted devices. In addition, devices then report measured information to healthcare professionals or certain physiological values to patients. An entity is authorized based on a set of tasks on its role, such as a physician or ambulance computer. The device manufacturer needs to have a special role-based access to the device as well. In recent years, the IMDs are enhanced with wireless communications, which can further expend more energy than their passive predecessors. Because devices are lightweight battery-limited in nature and they are also attached remotely with readable Radio Frequency Identification tags to implanted devices, IMDs must consume minimum power and data storage overhead to maximize the lifetime of these devices [1–4].

With the help of ciphertext-policy attribute-based encryption (CP-ABE), data are encrypted with an access policy, and each user associated with a set of attributes is able to decrypt a ciphertext if and only if his/her

attributes fulfill the ciphertext access policy. CP-ABE is then extremely appropriate for the medical health environment as it enables data owners to make and enforce access policies themselves [5–7]. The devices are lightweight and battery-limited in nature. CP-ABE should ensure to offer the low storage overhead and cost-effective solution for encryption and decryptions for such devices. Unfortunately, most of the existing CP-ABE schemes proposed in the literature use the bilinear maps and also produce the large-size secret keys and ciphertexts, which are almost linear to associated attributes. And the encryption and decryption require the group exponentiations, which are at least linear to the number of attributes involved in access policy [8–10].

The bilinear map looses the high efficiency over elliptic curve cryptography (ECC) because of the requirement of the security parameters of larger size. ECC is thus more suitable for the ultra-low energy devices as compared with the bilinear maps [11–13]. Therefore, designing an expressive access structure CP-ABE using ECC is an emerging research problem in this area.

Generally, access structures can be represented by the Boolean circuits [14]. A Boolean circuit comprises a number of input wires (which are not gate output wires), a number of output wires (which are not gate input wires), and a number of OR gate, AND gate as well as NOT gate. The OR gate and AND gate consists of two input wires. On the other hand, the NOT gate consists of one input wire. However, all of them can have more than one output wire. In this paper, we make use of access structures, which are based on AND gates.

Because of the greater demand for lightweight devices, in this paper, we aim to propose a new provably secure AND gate access structured CP-ABE scheme using ECC. The proposed scheme offers the constant-size secret keys (CSSK) and cost-efficient mechanisms for both encryption and decryption. To the best of our knowledge, this is the first attempt to design such a provably secure AND gate access structure CP-ABE scheme using ECC.

### 1.1. Related work

In the literature, several identity-based encryption schemes [11,15,16] are presented with CSSK and ciphertexts. Attribute-based encryption (ABE) is an extended version of identity-based encryption. Sahai and Waters [17] introduced the first ever ABE scheme. An ABE scheme comprises two variants: key-policy ABE (KP-ABE) and CP-ABE. With the help of KP-ABE, the ciphertext is associated with an attribute set and the secret key corresponding to an access policy. Decryption of the ciphertext with the secret key is possible if and only if the attribute set of ciphertext satisfies the access policy of that secret key. On the other hand, with the help of CP-ABE, the ciphertext is associated with an access policy, and the secret key is associated with an attribute set. In this case, the ciphertext can be decrypted with the secret key if and only if the attributes of secret key fulfills the ciphertext access policy.

After the introduction of the seminal work of Sahai–Waters [17], several KP-ABE schemes [17–20] and CP-ABE schemes [21–25] are presented in the literature. Note that CP-ABE enables the data encryptor to choose the access policy in order to decide who can access the data. It is then more appropriate in access control applications while comparing with KP-ABE schemes [8]. Recently, several CP-ABE schemes are presented with the constant-size ciphertexts [26–29] and CSSK [8,26] with an expressive access structure based on bilinear maps. Unfortunately, except the EMNOS scheme [26], no other CP-ABE scheme can offer both ciphertexts and secret keys of constant size. The EMNOS scheme [26] offers only $(n, n)$-threshold, and it is not also hard to design such a scheme [8]. The GSWV scheme [8] offers CSSK with an expressive AND gate access structure. Both EMNOS [26] and GSWV [8] schemes apply the bilinear maps. Because the bilinear maps looses the high efficiency over ECC, both EMNOS and GSWV schemes are not well suitable for the ultra-low energy devices [11–13]. In Table I, we have provided comparison among different attribute-based encryption schemes with various access structures presented so far in the literature up to date. When compared with other related existing schemes, it is observed that only our scheme provides the CSSK, and it also offers cost efficient solution for encryption and decryption with an expressive AND gate access structure.

### 1.2. Our contributions

We list our contributions subsequently:

- We present a new CP-ABE using ECC, which offers CSSK with an expressive AND gate access structure (called CP-ABE-CSSK). Constructing a provable secure CP-ABE scheme using ECC is an open problem in the literature. To the best of our knowledge, it is the first attempt to devise such a provably secure AND gate access structured CP-ABE scheme using ECC. Decryption of ciphertexts corresponding to access policy $\mathbb{P}$ with the help of a secret key associated with an attribute set $\mathbb{A}$ is possible if and only if $\mathbb{P} \subseteq \mathbb{A}$.
- Under the selective security model, it is shown that CP-ABE-CSSK provides provably security.
- CP-ABE-CSSK provides the CSSK with expressive access structure.
- Because ECC is highly efficient as compared with the bilinear maps, CP-ABE-CSSK is very suitable for IMDs as compared with existing schemes.

### 1.3. Paper structure

In Section 2, related mathematical preliminaries and definitions are discussed to describe and analyze our CP-ABE-CSSK scheme. In Section 3, we present a new ECC-based provably secure AND gate access structured CP-ABE scheme (CP-ABE-CSSK). We present the rigorous security analysis of CP-ABE-CSSK in Section 4.


DOI: 10.1002/sec

**Table I.** Comparison of various ABE schemes.

| Scheme | KP/CP-ABE | Access structure | Security model | LSK | LCT |
|---|---|---|---|---|---|
| SW [17] | KP-ABE | Threshold | Selective security | $nG$ | $nG + G_t$ |
| GPSW [18] | KP-ABE | Tree | Selective security | $\|\mathbb{A}\|G$ | $\|\mathbb{P}\|G + G_t$ |
| OSW [19] | KP-ABE | Tree | Selective security | $2\|\mathbb{A}\|G$ | $(\|\mathbb{P}\| + 1)G + G_t$ |
| BSW [20] | CP-ABE | Tree | Selective security | $(2\|\mathbb{A}\| + 1)G$ | $(2\|\mathbb{P}\| + 1)G + G_t$ |
| HLR [21] | CP-ABE | Threshold | Selective security | $(n + \|\mathbb{A}\|)G$ | $2G + G_t$ |
| CCLZFLW [22] | KP/CP-ABE | Threshold | Full security | $\mathcal{O}(n^2)$ | $\mathcal{O}(1)$ |
| EMNOS [26] | CP-ABE | $(n, n)$-Threshold | Selective security | $2G$ | $2G + G_t$ |
| LOSTW [23] | CP-ABE | LSSS | Full security | $(\|\mathbb{A}\| + 2)G_c$ | $(2\|\mathbb{P}\| + 1)G_c + G_{t_c}$ |
| Waters [24] | CP-ABE | LSSS | Selective security | $(\|\mathbb{A}\| + 2)G$ | $(2\|\mathbb{P}\| + 1)G + G_t$ |
| ALP [20] | KP-ABE | LSSS | Selective security | $3\|\mathbb{A}\|G$ | $2G + G_t$ |
| LW [25] | CP-ABE | LSSS | Full security | $(\|\mathbb{A}\| + 3)G_c$ | $(2\|\mathbb{P}\| + 2)G_c + G_{t_c}$ |
| DJ [29] | CP-ABE | AND gate-MV | Full security | $(n_{\mathbb{A}}\|\mathbb{A}\| + 2)G_c$ | $2G_c + G_{t_c}$ |
| ZZCLL [28] | CP-ABE | AND gate-MVW | Selective security | $(n + 1)G$ | $2G + G_t$ |
| CN [30] | CP-ABE | AND gates | Selective security | $(2\|\mathbb{A}\| + 1)G$ | $(\|\mathbb{P}\| + 1)G + G_t$ |
| ZH [27] | CP-ABE | AND gates | Selective security | $(\|\mathbb{A}\| + 1)G$ | $2G + G_t$ |
| GSWV [8] | CP-ABE | AND gates | Selective security | $2G$ | $(n - \|\mathbb{P}\| + 2)G + G_t + L$ |
| Ours | CP-ABE | AND gates | Selective security | $2 \times O(P)$ | $(n - \|\mathbb{P}\| + 3)\mathbb{G} + L$ |

CP-ABE, ciphertext-policy attribute-based encryption; KP-ABE, key-policy attribute-based encryption; LSSS, linear secret-sharing scheme; MV, multivalued; MVW, multivalued with wildcards; LSK, length of user secret key; LCT, length of ciphertext; $L$, length of plaintext $M$; $n$, number of attributes; $G$ and $G_t$, prime order pairing groups; $G_c$ and $G_{t_c}$, composite order pairing groups; $\mathbb{G}$, elliptic curve group defined over finite field $Z_p$; $O(P)$, the order of the base point that is assumed to be 160-bit integer in $Z_p$; $n_{\mathbb{A}}$, average number of values assigned to each attribute in attribute set $\mathbb{A}$.

Section 5 shows the performance of CP-ABE-CSSK with related existing schemes is compared. Finally, the concluding remarks along with some open problems are discussed in Section 6.

## 2. MATHEMATICAL TOOLS

### 2.1. Attribute and access structure

The attribute and access policy are defined as provided in [8]. Let the attribute universe $\mathbb{U} = \{A_1, A_2, \ldots, A_n\}$ be the set of $n$ attributes $A_1, A_2, \ldots, A_n$. An attribute set of a user is denoted by $\mathbb{A} \subseteq \mathbb{U}$ and presented with an $n$-bit string $a_1 a_2 \ldots a_n$ defined as follows: $a_i = 1$, if $A_i \in \mathbb{A}$ and $a_i = 0$, if $A_i \notin \mathbb{A}$. For example, if $n = 4$ and $\mathbb{A} = \{A_1, A_2, A_4\}$, the 4-bit string $\mathbb{A}$ becomes 1101. We define an access policy by $\mathbb{P}$ specified with attributes in $\mathbb{U}$ and represent with an $n$-bit string $b_1 b_2 \ldots b_n$, where $b_i = 1$, if $A_i \in \mathbb{P}$ and $b_i = 0$, if $A_i \notin \mathbb{P}$. For example, if $n = 4$ and $\mathbb{P} = 1010$ means that the access policy $\mathbb{P}$ requires the set of the attributes $\{A_1, A_3\}$.

In this paper, the AND gate access control structure represented by the attributes from $\mathbb{U}$ is considered. If $\mathbb{A} = a_1 a_2 \ldots a_n$ is an attribute set and $\mathbb{P} = b_1 b_2 \ldots b_n$ is the access policy, $\mathbb{P} \subseteq \mathbb{A}$ if and only if $a_i \geqslant b_i$, $\forall i = 1, 2, \ldots, n$. $\mathbb{A}$ fulfills $\mathbb{P}$ if and only if $\mathbb{P} \subseteq \mathbb{A}$. Hereafter, we represent $\mathbb{A}$ and $\mathbb{P}$ with $n$-bit strings.

### 2.2. Computational hard problems

The following computational hard problems [31] in the setting of the ECC are provided. The notations listed in Table II are applied throughout the paper.

#### 2.2.1. q-Generalized Diffie–Hellman assumption.

Given $a_1 P, a_2 P \ldots, a_q P$ in $\mathbb{G}$ and all subset products $\left(\prod_{i \in S} a_i\right) P \in \mathbb{G}$ for any strict subset $S \subset \{1, \ldots, q\}$, it is hard to compute $(a_1 \ldots a_q)P \in \mathbb{G}$, where $P$ is a base point in the elliptic curve $E_p(a, b)$; $a_1, a_2, \ldots, a_q \in Z_p^*$ and $Z_p^* = \{1, 2, \ldots, p-1\}$. The number of subset products (elliptic curve scalar point multiplications) is exponential in $q$. Because of this reason, all these subset products are accessed through an oracle. For a vector $\mathbf{a} = (a_1, \ldots, a_q) \in (Z_p)^q$, $\mathcal{O}_{P,\mathbf{a}}$ is defined as an oracle that responds with $\mathcal{O}_{P,\mathbf{a}}(S) = \left(\prod_{i \in S} a_i\right) \in \mathbb{G}$ for any strict subset $S \subset \{1, \cdots, q\}$.

**Definition 1** (q-Generalized Diffie–Hellman (q-GDH) assumption [31]). *The $(t, q, \epsilon)$-GDH assumption is satisfied in $\mathbb{G}$, if for all $t$-time algorithms $\mathcal{A}$, the advantage is $Adv^{GDH}_{\mathcal{A},q} = Pr\left[\mathcal{A}^{\mathcal{O}_{P,\mathbf{a}}} = (a_1 \ldots a_q)P\right] < \epsilon$, where $\mathbf{a} = (a_1, \ldots, a_q) \leftarrow (Z_p)^q$ and for any sufficiently small $\epsilon > 0$.*

#### 2.2.2. q-Diffie–Hellman Inversion problem.

Given a $(q+1)$-tuple $(P, xP, x^2P, \ldots, x^qP) \in \mathbb{G}^{q+1}$, to compute $(1/x)P \in \mathbb{G}$ where $x \in Z_p^*$.

**Definition 2** (q-Diffie–Hellman Inversion (q-DHI) assumption [31]). *$\mathbb{G}$ satisfies the $(t, q, \epsilon)$-DHI assumption, if for all $t$-time algorithms $\mathcal{A}$, the advantage becomes $Adv^{DHI}_{\mathcal{A},q} = Pr[\mathcal{A}(P, xP, x^2P, \cdots, x^qP) = (1/x)P] < \epsilon$ for any sufficiently small $\epsilon > 0$, where the probability is considered over the random choices of $x$ in $Z_p^*$ and random bits of $\mathcal{A}$.*

**Table II.** List of notations.

| Symbol | Meaning |
|---|---|
| $\alpha, k_1, k_2$ | The system private keys |
| $p$ | A sufficiently large prime number |
| $E_p(a,b)$ | An elliptic curve $y^2 = x^3 + ax + b \pmod p$ defined over the finite field $Z_p$; $Z_p = \{0, 1, \cdots, p-1\}$ |
| $P$ | A base point in $E_p(a,b)$ whose order is a 160-bit number in $Z_p$ |
| $xP$ | $P + P + \cdots + P$ ($x$ times), scalar multiplication, $P \in E_p(a,b)$ |
| $P + Q$ | Elliptic curve point addition of $P$ and $Q \in E_p(a,b)$ |
| $\mathbb{G}$ | Elliptic curve group $\{p, E_p(a,b), P\}$ generated by $P$ |
| $W^q$ | Cartesian product of the set $W$ $q$ times, that is, $W^q = W \times W \times \cdots \times W$ ($q$ times) |
| $H_1, H_2, H_3, H_4$ | Four one-way collision-resistance hash functions |
| $KDF$ | Key derivation function |
| $\mathbb{U}$ | Attribute universe $\{A_1, A_2, \cdots, A_n\}$ with $n$ attributes $A_1, A_2, \cdots, A_n$ |
| $\mathbb{A}$ | Set of user attributes, $\mathbb{A} \subseteq \mathbb{U}$ |
| $\mathbb{P}$ | Access policy, $\mathbb{P} \subseteq \mathbb{U}$ |
| $\lvert\mathbb{X}\rvert$ | Number of attributes in attribute set $\mathbb{X}$ |

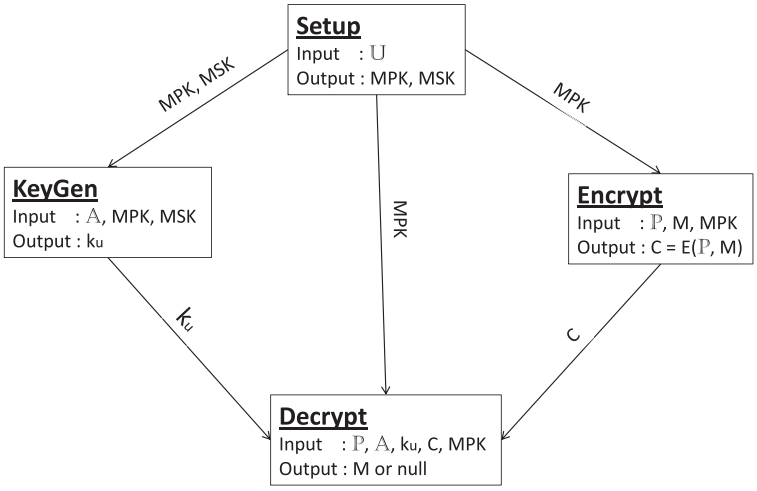


**Figure 1.** Steps involved in various phases of a generic ciphertext-policy attribute-based encryption scheme.

## 2.3. Definition of ciphertext-policy attribute-based encryption scheme

Ciphertext-policy attribute-based encryption scheme has the following algorithms [8]:

- **Setup:** This algorithm is provided with a security parameter $\rho$ and the universe of attributes $\mathbb{U} = \{A_1, A_2, \ldots, A_n\}$ as inputs, and it produces a master public key *MPK* and its corresponding master secret key *MSK*.
- **Encrypt:** It takes an access policy $\mathbb{P}$, the master public key *MPK* and a plaintext $M$ as inputs. The encryption algorithm $E[\mathbb{P}, M]$ then outputs a ciphertext $C$.
- **KeyGen:** The inputs of this algorithm are an attribute set $\mathbb{A}$, *MPK*, and *MSK*. The key generation algorithm then produces a user secret key (decryption key) $k_u$ corresponding to $\mathbb{A}$.
- **Decrypt:** It takes a ciphertext $C$ produced with an access policy $\mathbb{P}$, public key *MPK*, and secret key $k_u$ corresponding to attribute set $\mathbb{A}$ as inputs, and outputs the original plaintext $M$ or outputs null ($\perp$) using decryption algorithm $D[C, \mathbb{P}, k_u, \mathbb{A}]$. Note that if $\mathbb{P} \subseteq \mathbb{A}$, $D[C, \mathbb{P}, k_u, \mathbb{A}]$ always outputs the original $M$.

As a summary, a CP-ABE scheme must satisfy the following property. For any pair $(MPK, MSK)$, $E[\mathbb{P}, M]$, and $k_u$, if $\mathbb{P} \subseteq \mathbb{A}$, $D[C, \mathbb{P}, k_u, \mathbb{A}]$ will produce the correct $M$. Otherwise, plaintext in $E[\mathbb{P}, M]$ cannot be decrypted using $k_u$. All these aforementioned algorithms are summarized as a generic system model in Figure 1.

## 2.4. Selective game for ciphertext-policy attribute-based encryption scheme

To prove the security under chosen ciphertext attack, the *selective game* for a CP-ABE scheme is considered [8,26].


DOI: 10.1002/sec

The sole purpose of a CP-ABE game is to capture the indistinguishability of messages and collision-resistance of user secret keys. To capture collision resistance, an adversary $\mathcal{A}$ can issue multiple secret key queries after the challenge phase. The game between $\mathcal{A}$ and a challenger $\mathcal{B}$ proceeds as follows:

- **Initialization:** $\mathcal{A}$ outputs the challenge as an $n$-bit access policy $\mathbb{P}'$ and sends it to $\mathcal{B}$.
- **Setup:** $\mathcal{B}$ runs *Setup* and *KeyGen* algorithms with security parameter $\rho$ for generating the key pair $(MSK, MPK)$. After that $\mathcal{B}$ supplies $MPK$ to $\mathcal{A}$.
- **Query:** $\mathcal{A}$ makes the following queries to $\mathcal{B}$:
  - $\mathcal{A}$ queries for secret key $k_{u^i}$ of any attribute set $\mathbb{A}^i$, which does not fulfill the access policy $\mathbb{P}'$. $\mathcal{B}$ answers with a secret key $k_{u^i}$ for these attributes.
  - A decryption query on ciphertext $E[\mathbb{P}^i, M^i]$.
- **Challenge:** $\mathcal{A}$ outputs $(M_0, M_1)$ for the challenge. $\mathcal{A}$ does not need to query for a secret key on $\mathbb{A}$ with $\mathbb{P}' \subseteq \mathbb{A}$. $\mathcal{B}$ replies by selecting a random bit $c' \in \{0,1\}$ and then calculating ciphertext $E[\mathbb{P}', M_{c'}]$ for challenge to $\mathcal{A}$.
- **Query:** $\mathcal{A}$ can carry on with secret key and decryption queries except with a secret key query on any $\mathbb{A}$ satisfying $\mathbb{P}'$ and decryption query on $E[\mathbb{P}', M_{c'}]$.
- **Guess:** $\mathcal{A}$ outputs a guess $c'_g$ of $c'$, and wins the game if $c'_g = c'$.

In this game, the advantage $\epsilon$ of $\mathcal{A}$ is defined by $\epsilon = Pr\left[c'_g = c'\right] - \frac{1}{2}$.

**Definition 3.** *CP-ABE scheme is $(t, q_s, q_d, \epsilon)$-selectively secure against chosen-ciphertext attack (CCA), if for all t-polynomial time adversaries the $q_s$ secret key queries at most and $q_d$ decryption queries at most are made, where $\epsilon$ is a negligible function of $\rho$.*

# 3. THE PROPOSED CP-ABE-CSSK SCHEME

We propose a new CP-ABE scheme with CSSK using ECC, called CP-ABE-CSSK. The notations given in Table II are utilized for describing CP-ABE-CSSK. The CP-ABE-CSSK scheme has following four algorithms, namely, Setup, Encrypt, KeyGen, and Decrypt.

## 3.1. Setup

The setup algorithm takes the security parameter $\rho$ and the universe of attributes $\mathbb{U} = \{A_1, A_2, \ldots, A_n\}$ as inputs. This algorithm consists of the following steps:

S1. Choose an elliptic curve group $\mathbb{G} = \{p, E_p(a,b), P\}$, where $P$ is a base point on the elliptic curve $E_p(a,b)$ defined over the finite field $Z_p$.

S2. Pick three random private keys $\alpha$, $k_1$, and $k_2$ in $Z_p$. Then, compute

$$P_i = \alpha^i P, \tag{1}$$

$$U_i = k_1 \alpha^i P, \tag{2}$$

$$V_i = k_2 \alpha^i P, \tag{3}$$

for all $i = 0, 1, \cdots, n$.

S3. Choose four one-way collision-resistance hash functions $H_1$, $H_2$, $H_3$, and $H_4$, which are defined as follows:

$$\begin{aligned} H_1, H_4 &: \{0,1\}^* \rightarrow Z_p^*, \\ H_2 &: \{0,1\}^* \rightarrow \{0,1\}^{l_\sigma}, \\ H_3 &: \{0,1\}^* \rightarrow \{0,1\}^{l_m}, \end{aligned}$$

where $l_\sigma$ is the length of a sufficiently large random string, $l_m$ the length of plaintext message $M$, $\{0,1\}^*$ a binary string of an arbitrary length and $\{0,1\}^l$ a binary string of length $l$.

S4. Finally, output the master secret key $MSK$ and master public key $MPK$ as

$$\begin{aligned} MSK &= \{\alpha, k_1, k_2\}, \\ MPK &= \{\mathbb{G}, P_i, V_i, U_i, H_1, H_2, H_3, H_4\}, \\ & i = 0, 1, \cdots, n. \end{aligned}$$

## 3.2. Encrypt

The encryption is based on the approach presented in [8,32] for providing the security against CCA:

$$E\left(\sigma_m, H_1(\mathbb{P}, M, \sigma_m)\right), H_3(\sigma_m) \oplus M,$$

where $E(\sigma_m, H_1(\mathbb{P}, M, \sigma_m)$ represents an attribute-based encryption on $\sigma_m$ using the random hash output $r_m = H_1(\mathbb{P}, M, \sigma_m)$. In particular, $\sigma_m$ is encrypted with $k_m = KDF(r_m P)$ and $M$ is encrypted with $\sigma_m$, and these are denoted by $C_{\sigma_m}$ and $C_m$, respectively, which are included in the ciphertext $C$. The other components of the ciphertext $C$ are $P_{m,i}$, $K_{1m}$, and $K_{2m}$, where $i = 1, 2, \ldots, n$.

The encryption algorithm takes an access policy $\mathbb{P} \subseteq \mathbb{U}$ where $|\mathbb{P}| \neq 0$, the master public key $MPK$ and a plaintext message $M$ as inputs, and outputs the ciphertext $C = \{\mathbb{P}, P_{m,i}, K_{1m}, K_{2m}, C_{\sigma_m}, C_m\}$ using the following steps:

E1. Pick a random number $\sigma_m \in \{0,1\}^{l_\sigma}$, and compute $r_m = H_1(\mathbb{P}, M, \sigma_m)$ and $k_m = KDF(r_m P)$.

E2. Let $\mathbb{P} = b_1 b_2 \cdots b_n$ be the access policy string. Compute the corresponding $(n-1)$-degree at most polynomial function $f(x, \mathbb{P})$ in $Z_p[x]$ as

$$f(x,\mathbb{P}) = \prod_{i=1}^{n} (x + H_4(i))^{1-b_i}. \quad (4)$$

Let $f_i$ denote the coefficient of $x^i$ in the polynomial $f(x,\mathbb{P})$.

E3. Compute the ciphertext's parameters as follows:

$$P_{m,i} = r_m P_i, i = 1, \cdots, n - |\mathbb{P}|, \quad (5)$$

$$K_{1m} = r_m \sum_{i=0}^{n} f_i U_i = r_m k_1 f(\alpha,\mathbb{P})P, \quad (6)$$

$$K_{2m} = r_m \sum_{i=0}^{n} f_i V_i = r_m k_2 f(\alpha,\mathbb{P})P, \quad (7)$$

$$C_{\sigma_m} = H_2(k_m) \oplus \sigma_m, \quad (8)$$

$$C_m = H_3(\sigma_m) \oplus M. \quad (9)$$

E4. Finally, output the ciphertext $C$ as $C = \{\mathbb{P}, P_{m,i}, K_{1m}, K_{2m}, C_{\sigma_m}, C_m\}$.

### 3.3. KeyGen

The key generation algorithm takes a user attribute set $\mathbb{A}$, master public key *MPK* and master secret key *MSK* as inputs, and then generates the user secret key $k_u$ using the following steps:

K1. Let $\mathbb{A} = a_1 a_2 \cdots a_n$ be the user attribute string. Compute

$$f(\alpha,\mathbb{A}) = \prod_{i=1}^{n} (\alpha + H_4(i))^{1-a_i}, \quad (10)$$

where $f(x,\mathbb{A})$ is a polynomial function in $Z_p[x]$ whose degree is at most $n$.

K2. Pick two random numbers $r_u$ and $t_u$. Compute $s_u$ such that the condition $\frac{1}{f(\alpha,\mathbb{A})} = k_1 s_u + k_2 r_u \pmod p$ holds. Thus,

$$s_u = \frac{1}{k_1}\left(\frac{1}{f(\alpha,\mathbb{A})} - k_2 r_u\right). \quad (11)$$

Also, compute

$$u_1 = r_u + k_1 t_u \pmod p,$$
$$u_2 = s_u - k_2 t_u \pmod p.$$

Finally, output the user secret key $k_u = (u_1, u_2)$.

**Proposition 1.** *Based on $f(x,\mathbb{P})$ and $f(x,\mathbb{A})$ defined in Equations (4) and (10), respectively, we have the following result:*

$$F(x,\mathbb{A},\mathbb{P}) = \frac{f(x,\mathbb{P})}{f(x,\mathbb{A})} = \prod_{i=1}^{n} (x + H_4(i))^{a_i - b_i}. \quad (12)$$

*It is easy to check that $\frac{f(x,\mathbb{P})}{f(x,\mathbb{A})}$ becomes a polynomial function in x if and only if $\mathbb{P} \subseteq \mathbb{A}$* [8].

The design of an encryption algorithm and construction of the secret key need to be in such a way that $\frac{f(x,\mathbb{P})}{f(x,\mathbb{A})}$ must be a polynomial for a successful decryption.

### 3.4. Decrypt

The decryption algorithm takes the secret key $k_u = (u_1, u_2)$ corresponding to the attribute set $\mathbb{A}$ and ciphertext $C = \{\mathbb{P}, P_{m,i}, K_{1m}, K_{2m}, C_{\sigma_m}, C_m\}$ corresponding to the access policy $\mathbb{P}$, and outputs the original plaintext message $M$ using the following steps:

D1. If $\mathbb{A} = a_1 a_2 \ldots a_n$ does not fulfill the access policy $\mathbb{P} = b_1 b_2 \ldots b_n$, then abort. Otherwise, execute the next step.

D2. Compute

$$U = u_2 K_{1m} = (s_u - k_2 t_u)(r_m k_1 f(\alpha,\mathbb{P}))P,$$
$$V = u_1 K_{2m} = (r_u + k_1 t_u)(r_m k_2 f(\alpha,\mathbb{P}))P,$$

$$\begin{aligned} U + V &= (s_u - k_2 t_u)(r_m k_1 f(\alpha,\mathbb{P}))P \\ &\quad + (r_u + k_1 t_u)(r_m k_2 f(\alpha,\mathbb{P}))P \\ &= ((s_u r_m k_1 f(\alpha,\mathbb{P}) \\ &\quad - k_2 t_u r_m k_1 f(\alpha,\mathbb{P})) \\ &\quad + (r_u r_m k_2 f(\alpha,\mathbb{P}) \\ &\quad + k_1 t_u r_m k_2 f(\alpha,\mathbb{P}))) P \\ &= (s_u r_m k_1 f(\alpha,\mathbb{P}) \\ &\quad + r_u r_m k_2 f(\alpha,\mathbb{P})) P \\ &= r_m (s_u k_1 + r_u k_2) f(\alpha,\mathbb{P}) P \\ &= r_m \frac{1}{f(\alpha,\mathbb{A})} f(\alpha,\mathbb{P}) P \\ &= r_m F(\alpha) P. \end{aligned}$$

D3. Compute $c_i = a_i - b_i$ for $i = 1, 2, \ldots, n$. Let $F(x,\mathbb{A},\mathbb{P})$ be the $(n - |\mathbb{P}|)$-degree at most polynomial function in $Z_p[x]$ defined as

$$F(x) = F(x,\mathbb{A},\mathbb{P}) = \prod_{i=1}^{n-|\mathbb{P}|} (x + H_4(i))^{c_i}, \quad (13)$$

and $F_i$ be the coefficient of $x^i$ in the polynomial $F(x)$. It is clear that $F_0 \neq 0$. After that, compute

$$
\begin{aligned}
W &= \sum_{i=1}^{n-|\mathbb{P}|} F_i P_{m,i} \\
&= r_m \left( \sum_{i=1}^{n-|\mathbb{P}|} F_i \alpha^i \right) P \\
&= r_m \left( \sum_{i=1}^{n-|\mathbb{P}|} F_i \alpha^i + F_0 - F_0 \right) P \\
&= r_m \left( F(\alpha) - F_0 \right) P \\
&= r_m F(\alpha) P - r_m F_0 P
\end{aligned}
$$

and the key $r_m P$ as $\frac{1}{F_0}((U+V)-W)$. Note that

$$
\begin{aligned}
r_m P &= \frac{1}{F_0}((U+V)-W) \\
&= \frac{1}{F_0}(r_m F(\alpha) P \\
&\quad -(r_m F(\alpha) P - r_m F_0 P)) \\
&= \frac{r_m F(\alpha) - r_m F(\alpha) + r_m F_0}{F_0} P \\
&= r_m P.
\end{aligned}
$$

D4. Compute $\sigma'_m = H_2(KDF(r_m P)) \oplus C_{\sigma_m}$, $M' = C_m \oplus H_3(\sigma'_m)$ and $r'_m = H_1\left(\mathbb{P}, M', \sigma'_m\right)$. Then, verify whether the condition $r_m P = r'_m P$ holds or not. If it holds, treat $M'$ the original plaintext $M$. Otherwise, output null ($\perp$).

**Remark 1.** If $\mathbb{A} = \mathbb{P}$, $F(x) = 1$, which is a constant polynomial. This implies that $\frac{f(\alpha,\mathbb{P})}{f(\alpha,\mathbb{A})} = F(\alpha) = 1$. Hence, $U + V = r_m P$, and in this case, we need to execute Step $D4$ directly by skipping Step $D3$.

## 4. SECURITY ANALYSIS

In this section, we analyze the security of our proposed CP-ABE-CSSK scheme for different possible known attacks. The main goal of selective security for a CP-ABE scheme is to capture the indistinguishability of messages and the collision resistance of secret keys, that is, the attackers cannot generate a new user secret key by combining their secret keys [30,33]. In this paper, we follow the group generic model to prove that our scheme is secure against possible known attacks. Furthermore, we prove that our scheme is provably secure against CCA under the selective security game.

**Proposition 2.** *Let $c_i = a_i y + b_i z$, for $i = 1, 2, \ldots, l$, be a system of $l$ linear equations in variables $y$ and $z$, where $a_i = a_j$ and $b_i = b_j$ if and only if $i = j$. We have then the following three cases* [34,35]*:*

- *If both $a_i$ and $b_i$ are known, the equations form a system of $l$ linear equations with two unknowns $y$ and $z$. The system is solvable for $y$ and $z$, and has a unique solution.*
- *If $a_i$ (or $b_i$) is unknown, the equations form a system of $l$ equations with $l+2$ unknowns $a_i$ (or $b_i$), $y$ and $z$. The system is solvable, however, it has infinitely many solutions.*
- *If both $a_i$ and $b_i$ are unknown, the equations form a system of $l$ equations with $2l+2$ unknowns $a_i$, $b_i$, $y$, and $z$. The system is also solvable, however, it has infinitely many solutions.*

**Theorem 1.** *CP-ABE-CSSK is secure against an adversary for deriving the system private key pair $(k_1, k_2)$ by collision attack.*

*Proof.* Assume that a group of users $u^i$, $i = 1, \ldots, l$, associated with the attribute set $\mathbb{A}^i$ collaborate among each other and try to derive the system private key pair $(k, x)$ using their valid secret keys $k_{u^i} = \left(u_1^i, u_2^i\right)$, where

$$u_1^i = s_{u^i} + k_1 . t_{u^i} \pmod{p}, \tag{14}$$

$$u_2^i = r_{u^i} - k_2 . t_{u^i} \pmod{p}. \tag{15}$$

From Step K2 of the *KeyGen* algorithm (Section 3.3), we have

$$\frac{1}{f(\alpha, \mathbb{A}^i)} = k_1 s_{u^i} + k_2 r_{u^i} \pmod{p}. \tag{16}$$

From Equation (16), it is clear that if $s_{u^i}$ and $r_{u^i}$ are known, it is solvable for $k_1$ and $k_2$, and has a unique solution. Thus, the solution produces the original values of $k_1$ and $k_2$. However, Equations (14) and (15) respectively form the system of $l$ linear equations with $2l+1$ unknowns. From Proposition 2, note that Equation (14) requires to randomly guess two unknowns $(s_{u^i}, t_{u^i})$ in order to solve $k_1$, and Equation (15) also requires to randomly guess two unknowns $(r_{u^i}, t_{u^i})$ to solve $k_2$. Hence, from the corrupted user secret keys $k_{u^i}$, $\forall i = 1, 2, \ldots, l$, the system's private key pair $(k_1, k_2)$ is unknown, and as a result, the random numbers $s_{u^i}$ and $r_{u^i}$ are also unknown to an adversary. □

**Theorem 2.** *CP-ABE-CSSK is secure against an adversary for deriving the valid user secret key $k_u = (u_1, u_2)$ corresponding to the attribute set $\mathbb{A}$.*

*Proof.* From Theorem 1, it follows that computing the system private key pair $(k_1, k_2)$ is computationally infeasible by an adversary $\mathcal{A}$. This implies that it is computationally infeasible for the adversary $\mathcal{A}$ to compute the valid pair $k_u = (u_1, u_2)$ corresponding to the attribute set $\mathbb{A}$. The adversary $\mathcal{A}$ can randomly choose $r_u$ and $t_u$, and compute $s_u$ such that it satisfies the condition $\frac{1}{f(\alpha,\mathbb{A})} = s_u k_1 + r_u k_2 \pmod{p}$. However, to compute the value $s_u$, the adversary $\mathcal{A}$ requires the system private key pair $(k_1, k_2)$

and the value $f(\alpha, \mathbb{A})$. Thus, generating the valid user secret key $k_u$ is computationally infeasible problem by the adversary $\mathcal{A}$. □

**Remark 2.** A ciphertext $C$ corresponding to the access policy $\mathbb{P}$ consists of the following parameters:

$$\begin{aligned} P_{m,i} &= r_m P_i, i = 1, \cdots, n - |\mathbb{P}|, \\ K_{1m} &= r_m k_1 f(\alpha, \mathbb{P}) P, \\ K_{2m} &= r_m k_2 f(\alpha, \mathbb{P}) P, \\ C_{\sigma_m} &= H_2(r_m P) \oplus \sigma_m, \\ C_m &= H_3(\sigma_m) \oplus M. \end{aligned}$$

Because $\sum_{i=1}^{n-|\mathbb{P}|} P_{m,i} = r_m(f(\alpha, \mathbb{P}) - f_0)P$, it is hard to compute $r_m P$ using $K_{1m}$ and $K_{2m}$ because of the difficulty of solving the elliptic curve discrete logarithm problem. Given $P_{m,i} = r_m P_i = r_m \alpha^i P$, $i = 1, 2, \cdots, q = n - |\mathbb{P}|$, this problem can be reduced to the $(q-1)$-DHI problem as follows. Let $Q = \alpha r_m P$. We then rewrite the parameters $P_{m,i} = r_m P_i = \alpha^i r_m P$ as $Q_i = P_{m,i} = \alpha^{i-1} Q$, $i = 1, 2, \cdots, q$. This implies that if an adversary $\mathcal{A}$ has the ability to solve the $(q-1)$-DHI problem, he/she can compute the key $r_m P = (1/\alpha)Q_1 = (1/\alpha)Q$, and then successfully decrypt the ciphertext $C$. In the following theorem, we prove that solving the $(q-1)$-DHI problem is as hard as the $q$-GDH problem.

**Theorem 3.** *If the $(t, q-1, \epsilon)$-DHI assumption holds in $\mathbb{G}$, the $(t, q, \epsilon)$-GDH assumption also holds in $\mathbb{G}$.*

*Proof.* Let $\mathcal{A}$ be an algorithm having advantage $\epsilon$ in solving the $q$-GDH problem. An algorithm $\mathcal{B}$ is constructed, which solves $(q-1)$-DHI with the same advantage $\epsilon$. We follow the same proof as presented in [31].

$\mathcal{B}$ is given the inputs: $Q, \alpha Q, \alpha^2 Q, \cdots, \alpha^{q-1} Q \in \mathbb{G}$ and its purpose is to calculate $(1/\alpha)Q \in \mathbb{G}$. If $R = \alpha^{q-1} Q$ and $y = 1/\alpha$, the inputs of $\mathcal{B}$ can be re-arranged as $R, yR, y^2 R, \cdots, y^{q-1} R \in \mathbb{G}$. $\mathcal{B}$'s goal is to produce $y^q R = (1/\alpha)Q = T$.

$\mathcal{B}$ first picks $q$ random values, say $r_1, \cdots, r_q \in Z_p$, and then simulates $\mathcal{A}$ and also simulates the oracle $\mathcal{O}_{R,\mathbf{a}}$ for $\mathcal{A}$. $\mathcal{B}$ will use the vector $\mathbf{a} = (y + r_1, \cdots, y + r_q)$. Note that $\mathcal{B}$ does not know $\mathbf{a}$ explicitly as $\mathcal{B}$ does not have $y = 1/\alpha$. $\mathcal{B}$ responds with following when $\mathcal{A}$ issues a query for $\mathcal{O}_{R,\mathbf{a}}(S)$ for some strict subset $S \subset \{1, \cdots, q\}$.

- Construct the polynomial $f(x) = \prod_{i \in S}(x + r_i)$ and expand its terms to obtain $f(x) = \sum_{i=0}^{|S|} f_i x^i$.
- Calculate $Y = \sum_{i=0}^{|S|} (f_i y^i R) = f(y)R$. Note that $|S| < q$. Therefore, all $y^i R$ in the sum are known to $\mathcal{B}$.
- By construction, we have $Y = \left(\prod_{i \in S}(y + r_i)\right) R$. $\mathcal{B}$ responds by setting $\mathcal{O}_{R,\mathbf{a}}(S) = Y$.

The responses to all the oracle queries of the adversary are consistent with the hidden vector $\mathbf{a} = (y + r_1, \cdots, y + r_q)$. $\mathcal{A}$ will then output $Z = \left(\prod_{i=1}^{q}(y + r_i)\right) R$. Furthermore, define the polynomial $f(x) = \prod_{i=1}^{q}(x + r_i)$ and expand the terms to obtain $f(x) = x^q + \sum_{i=0}^{q-1} f_i x^i$. As a summary, $\mathcal{B}$ outputs the required $T = Z - \sum_{i=0}^{q-1} f_i y^i R = y^q R$. □

**Remark 3.** From the preceding discussion, our scheme is collision resistance of secret keys. As a result, computing the key $k_m = r_m P$ from a ciphertext $C$ corresponding to the access policy $\mathbb{P}$ without a valid user secret key $k_u$ is as hard as the $q$-GDH problem. This implies that given $\{P_{m,1}, P_{m,2}, \cdots, P_{m,q}, K_{1m}, K_{2m}\}$, where $q = n - |\mathbb{P}|$, and $T \in \mathbb{G}$, the $q$-GDH problem reduces to the $(q-1)$-DHI problem, and then decides whether $T$ is equal to $r_m P$ or a random element in $\mathbb{G}$.

**Theorem 4.** *CP-ABE-CSSK is $(t, q_s, q_d, \epsilon)$-selectively secure if the $q$-GDH problem is $(t', \epsilon')$-hard, where $t' = t + \mathcal{O}(q_s(t_{inv} + nt_{mul}) + q_{H_1} n t_{em})$, $\epsilon' = \epsilon - \frac{q_{H_2}}{p}$, $n = |\mathbb{U}|$, $q = n - |\mathbb{P}|$, and $t_{inv}$, $t_{mul}$ and $t_{em}$ are the average time required for group inverse, multiplication and point multiplication operations, respectively, and $q_{H_1}$ and $q_{H_2}$ the number of queries made to the random oracles $H_1$ and $H_2$, respectively.*

*Proof.* Let $\mathcal{A}$ be an adversary, who can break the security of CP-ABE-CSSK with the advantage $(t, q_s, q_d, \epsilon)$. For completing the reduction, we construct an algorithm $\mathcal{B}$ with the advantage $\epsilon' = \epsilon - \frac{q_{H_2}}{p}$.

$\mathcal{B}$ is supplied the challenge as input, and its aim is to output $T = 1$ or 0. It interacts with $\mathcal{A}$ as follows.

**Initialization:** $\mathcal{A}$ outputs the access policy $\mathbb{P}'$, which needs to be challenged, where the total number of attributes is $n$.

**Setup:** $\mathcal{B}$ takes the attribute universe $\mathbb{U} = \{A_1, A_2, \cdots, A_n\}$ and the security parameter $\rho$ as input, and generates the master secret key $MSK = \{\alpha, k_1, k_2\}$ and master public key $MPK = \{\mathbb{G}, P_i, V_i, U_i, H_1, H_2, H_3, H_4\}$ according to *Setup* algorithm defined in our CP-ABE-CSSK. $\mathcal{B}$ then gives the public parameters to $\mathcal{A}$ except the four hash functions $H_1$, $H_2$, $H_3$, and $H_4$ set as random oracles.

**Hash Queries:** $\mathcal{A}$ can access $H_1$, $H_2$, $H_3$, and $H_4$ oracles. $\mathcal{B}$ maintains four lists $\mathcal{L}_{H_1}$, $\mathcal{L}_{H_2}$, $\mathcal{L}_{H_3}$, and $\mathcal{L}_{H_4}$ to record the queries and responses. Note that the same result will be returned by $\mathcal{B}$ in case the query was already responded and recorded in the list. $\mathcal{B}$ works for new queries as follows:

- $H_4$ oracle: Let the query to $H_4$ be $i \in [1, n]$. $\mathcal{B}$ responds $H_4(i)$ with a random number in $Z_p^*$.
- $H_2$ oracle: Let the query to $H_2$ be $k'_m = KDF(r'_m P)$. $\mathcal{B}$ responds $H_2(k'_m)$ with a random number $R_i \in \{0, 1\}^{l_{\sigma_m}}$.

- $H_3$ oracle: Let the query to $H_3$ be $t_i$. $\mathcal{B}$ responds $H_3(t_i)$ with a random number $Q_i \in \{0,1\}^{l_m}$.
- $H_1$ oracle: Let the query to $H_1$ be $(\mathbb{P}_i, M_i, t_i)$. $\mathcal{B}$ responds $H_1(\mathbb{P}_i, M_i, t_i)$ with a random number $r_i \in Z_p^*$.

**Query:** For a secret key query on $\mathbb{A}_i = a_1 a_2 \cdots a_n$, $\mathcal{B}$ computes the secret key using the *KeyGen* algorithm and sends it to the adversary $\mathcal{A}$.

For any decryption query on $E[\mathbb{P}_i, M_i]$, if there exists $(\mathbb{P}_i, M_i, t_i, r_i, R_i, Q_i)$ in the query list such that the ciphertext is generated using $r_i$, the decryption query outputs $M_i$. Otherwise, it outputs null. Suppose no query will be aborted as all valid encryptions require the responses from hash oracles, and responses contain $r_i$ used in encryption.

**Challenge:** $\mathcal{A}$ produces two messages pair $(M_0, M_1)$ for the challenge where all the queried secret keys do not fulfill $\mathbb{P}'$. $\mathcal{B}$ randomly chooses $R' \in \{0,1\}^{l_{\sigma_m}}$ and $Q' \in \{0,1\}^{l_m}$, and derives the challenge ciphertext as

$$\begin{aligned} P'_{m,i} &= r'_m P_i, i = 1, \cdots, n - |\mathbb{P}|, \\ K'_{1m} &= r'_m k_1 f(\alpha, \mathbb{P}) P, \\ K'_{2m} &= r'_m k_2 f(\alpha, \mathbb{P}) P, \\ C_{\sigma_m} &= R', \\ C_m &= Q'. \end{aligned}$$

Under the random oracles, $\mathcal{A}$ must be able to calculate $T = r'_m P$ $(= (1/\alpha) P'_{m,1})$ and then query it to the $H_2$ oracle for decryption.

**Query:** The response of this phase remains unaltered as in the previous phase with exception that there will be no secret key query satisfying challenge policy and no decryption query on challenge ciphertext.

**Guess:** $\mathcal{A}$ obtains 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 $\mathbb{G}$.

In the guess phase, if $\mathcal{A}$ breaks encryption with an advantage $\epsilon$, $r'_m P$ presents in $\mathcal{L}_{H_2}$ with probability $\epsilon + 1/2$ at least. Note that the only error event is that $T$ is a random group element, but it is queried to $H_2$ oracle. This happens with probability $q_{H_2}/p$ at most.

Let $Pr[Abort]$ be the probability that $\mathcal{B}$ aborts. Then, $Pr[Abort] \leqslant q_{H_2}/p$. If $\mathcal{B}$ does not abort, $\mathcal{A}$'s view remains identical to its view in the real attack. Hence,

$$\begin{aligned} Adv^{GDH}_{\mathcal{B},q} &= \left| Pr\left[c'_g = c'\right] - Pr\left[c'_g \neq c'\right] \right| \\ &> \epsilon - q_{H_2}/p. \end{aligned}$$

Therefore, $\mathcal{B}$ distinguishes $T = 1$ or 0 having advantage $\epsilon - q_{H_2}/p$ at least.

Each key generation and decryption require $1t_{inv} + \mathcal{O}(n)t_{mul}$ and $\mathcal{O}(n)t_{em}$ operations, respectively. As a result, we have $t' = t + \mathcal{O}(q_s(t_{inv} + nt_{mul}) + q_{H_1} nt_{em})$ and hence, the theorem follows.

□

## 5. COMPARATIVE ANALYSIS

This section presents a comparative analysis among our scheme, and the other two most related existing schemes: EMNOS [26] and GSWV [8].

From Table I, we see that the EMNOS scheme [26] offers the constant-size ciphertexts and secret keys. However, it provides only $(n, n)$-threshold, and it is not hard to design such scheme (see Remark 1 in the Decrypt phase). The GSWV scheme [8] provides an efficient solution for only the shorter secret keys with an expressive AND gate access structure. Furthermore, in Table I, we have compared the different attribute-based encryption schemes with various access structures.

The following notations are used in order to evaluate the computational complexity comparison among various related protocols: $T_G$: time to execute an exponentiation in the group $G$; $T_{G_t}$: time to execute an exponentiation in the target group $G_t$; $T_e$: time for executing a bilinear map operation; $T_{ecm\mathbb{G}}$: time to execute a scalar point multiplication in the elliptic curve group $\mathbb{G}$.

Table III shows the computational cost comparison among our scheme and other schemes. More precisely, to analyze computation efficiency schematically, the rough estimations of various cryptographic operations on Pentium IV computer platform [36] are provided in Table IV. For this, we assume that $n = 1000$, $\mathbb{A} = 600$, and $\mathbb{P} = 500$. From Table III, it is observed that our scheme reduces the number of group exponentiations required for

**Table III.** Comparison of computational complexity.

| Scheme | Encryption | Decryption |
|---|---|---|
| EMNOS | $(n+1)T_G + 2T_{G_t}$ | $2T_{G_t} + 2T_e$ |
| | $\approx 1173.51$ *ms* | $\approx 8.66$ *ms* |
| GSWV | $(2(n - \lvert\mathbb{P}\rvert) + 2)\ T_G$ | $2(\lvert\mathbb{A}\rvert - \lvert\mathbb{P}\rvert)\ T_G$ |
| | | $+1T_{G_t} + 3T_e$ |
| | $\approx 1172.34$ *ms* | $\approx 244.65$ *ms* |
| Ours | $(n - \lvert\mathbb{P}\rvert + 2)\ T_{ecm\mathbb{G}}$ | $(n - \lvert\mathbb{P}\rvert + 3)\ T_{ecm\mathbb{G}}$ |
| | $\approx 276.10$ *ms* | $\approx 276.65$ *ms* |

**Table IV.** Execution timings of various cryptographic operations on Pentium IV computer platform. [36]

| $T_e$ | $T_m$ | $T_{ecm\mathbb{G}}$ |
|---|---|---|
| 3.16 ms | 1.17 ms | 0.55 ms |

Note: $T_G \approx T_{G_t} = T_m$ .

**Table V.** Comparison of secret key sizes.

| Scheme | Secret key size (in bits) |
|---|---|
| EMNOS [26] | 640 |
| GSWV [8] | 1344 |
| Ours | 320 |

encryption and decryption to the half as compared with GSWV scheme [8]. Moreover, our scheme uses only the conventional ECC to provide the cost-effective CP-ABE scheme for the lightweight devices. Thus, our scheme provides efficient solution for CP-ABE with expressive access structure for lightweight devices using ECC.

The lengths of ciphertexts produced by various ABE schemes are shown in Table I. From this table, we observe that our scheme and other existing EMNOS and GSWV schemes require $(n - |\mathbb{P}| + 3)\mathbb{G} + L$, $2G + G_t$ and $(n - |\mathbb{P}| + 2)G + G_t + L$ bits as the communication cost for sending a ciphertext to a recipient by a sender, respectively.

Our scheme is the first proposed CP-ABE scheme, which provides CSSK with the expressive access structure without using bilinear maps. Table V shows the comparison of secret key sizes among our scheme and other schemes [8,26]. The size of the secret key $k_u$ in our scheme is $|k_u| = 2 \times O(P) = 320$ bits as the 160-bit ECC roughly provides the 80-bit security [13]. In the EMNOS scheme [26], the secret key size is $|k_u| = 2|G| = 2 \times 320 (= 640$ bits ). However, in the GSWV scheme [8], the secret key size is $|k_u| = |G_1| + |G_2| = 2 \times 160 + 2 \times 512 = 1344$ bits for 80-bit security, where $G_1$ and $G_2$ are elliptic curve bilinear groups defined in GSWV scheme [8]. From this table, it is clear that our scheme needs significantly less secret key size as compared with that for other schemes [8,26].

## 6. CONCLUSION

We have designed a new ECC-based CP-ABE-CSSK scheme with the CSSK with an expressive AND gate access structure without using bilinear maps. To the best of our knowledge, it is the first ECC-based CP-ABE scheme. In addition, CP-ABE-CSSK offers the CSSK, which is as small as 320 bits for the 80-bit security. CP-ABE-CSSK also significantly reduces the encryption and decryption costs as compared with related schemes. We have showed that CP-ABE-CSSK is secure against possible known attacks, such as key recovery and collision attacks. In addition, we have shown that CP-ABE-CSSK is provably secure under the chosen-ciphertext adversary. Thus, CP-ABE-CSSK offers CSSK along with efficient solution for encryption and decryption under the chosen ciphertext adversary, which supports an expressive AND gate access structure.

## Acknowledgements

The authors would like to acknowledge the helpful suggestions of the anonymous reviewers and the Editor. This work was partially supported by the Information Security Education & Awareness (ISEA) Phase II Project, Department of Electronics and Information Technology (DeitY), India.

## REFERENCES

1. Halperin D, Kohno T, Heydt-Benjamin TS, Fu K, Maisel WH. Security and privacy for implantable medical devices. *IEEE Pervasive Computing* 2008; **7**(1): 30–39.
2. Targhetta AD, Owen DE, Gratz PV. The design space of ultra-low energy asymmetric cryptography. *IEEE International on Symposium on Performance Analysis of Systems and Software (ISPASS 2014)*, 2014; 55–65.
3. Atzori L, Iera A, Morabito G. The internet of things: a survey. *Computer networks* 2010; **54**(15): 2787–2805.
4. Li M, Lou W, Ren K. Data security and privacy in wireless body area networks. *IEEE Wireless Communications* 2010; **17**(1): 51–58.
5. Avancha S, Baxi A, Kotz D. Privacy in mobile technology for personal healthcare. *ACM Computing Surveys* 2012; **45**(1): 3.
6. Wan Z, Liu J, Deng RH. Hasbe: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing. *IEEE Transactions on Information Forensics and Security* 2012; **7**(2): 743–754.
7. Abbas A, Khan SU. A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. *IEEE Journal of Biomedical and Health Informatics* 2014; **18**(4): 1431–1441.
8. Guo F, Mu Y, Susilo W, Wong DS, Varadharajan V. CP-ABE with constant-size keys for lightweight devices. *IEEE Transactions on Information Forensics and Security* 2014; **9**(5): 763–771.
9. Zhou Z, Huang D, Wang Z. Efficient privacy-preserving ciphertext-policy attribute-based encryption and broadcast encryption. *IEEE Transactions on Computers* 2015; **64**(1): 126–138.
10. Chen C, Zhang Z, Feng D. Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost. In *5th International Conference on Provable Security (ProvSec 2011)*. Springer: Xi'an China, 2011; 84–101.
11. Zheng M, Xiang Y, Zhou H. A strong provably secure IBE scheme without bilinear map. *Journal of Computer and System Sciences* 2015; **81**(1): 125–131.
12. Barreto P SLM, Kim HY, Lynn B, Scott M. Efficient algorithms for pairing-based cryptosystems. In *22nd International Conference on Cryptology (CRYPTO 2002)*. Springer: Santa Barbara, USA, 2002; 354–369.

13. Lauter K. The advantages of elliptic curve cryptography for wireless security. *IEEE Wireless communications* 2004; **11**(1): 62–67.
14. Ţiplea FL, Drăgan CC. First international conference on cryptography and information security in the balkans (balkancryptsec 2014), lecture notes in computer science. In *Key-Policy Attribute-Based Encryption for Boolean Circuits from Bilinear Maps*, Vol. 9024. Springer International Publishing: Istanbul, Turkey, 2015; 175–193.
15. Delerablée C. Identity-based broadcast encryption with constant size ciphertexts and private keys. In *Proceedinds of 13th International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT 2007)*. Springer: Kuching, Malaysia, 2007; 200–215.
16. Guo F, Mu Y, Susilo W. Identity-based traitor tracing with short private key and short ciphertext. In *Welcome to the European Symposium on Research in Computer Security (ESORICS 2012)*. Springer: Pisa, Italy, 2012; 609–626.
17. Sahai A, Waters B. Fuzzy identity-based encryption. In *25th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2005)*. Springer: Aarhus, Denmark, 2005; 457–473.
18. Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS 2006)*. ACM: Alexandria, VA, USA, 2006; 89–98.
19. Ostrovsky R, Sahai A, Waters B. Attribute-based encryption with non-monotonic access structures. In *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS 2007)*. ACM: Alexandria, Virginia, USA, 2007; 195–203.
20. Attrapadung N, Libert B, De Panafieu E. Expressive key-policy attribute-based encryption with constant-size ciphertexts. In *14th International Conference on Practice and Theory in Public Key Cryptography (PKC 2011)*. Springer: Taormina, Italy, 2011; 90–108.
21. Herranz J, Laguillaumie F, Ràfols C. Constant size ciphertexts in threshold attribute-based encryption. In *13th International Conference on Practice and Theory in Public Key Cryptography (PKC 2010)*. Springer: Paris, France, 2010; 19–34.
22. Chen C, Chen J, Lim HW, Zhang Z, Feng D, Ling S, Wang H. Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures. In *Proceedings of the Cryptographers' Track at the RSA Conference (CT-RSA 2013)*. Springer: San Francisco, CA, USA, 2013; 50–67.
23. Lewko A, Okamoto T, Sahai A, Takashima K, Waters B. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption. In *29th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2010)*. Springer: French Riviera, 2010; 62–91.
24. Waters B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. In *14th International Conference on Practice and Theory in Public Key Cryptography (PKC 2011)*. Springer: Taormina, Italy, 2011; 53–70.
25. Lewko A, Waters B. New proof methods for attribute-based encryption: achieving full security through selective techniques. In *32nd International Conference on Cryptology (CRYPTO 2012)*. Springer: Santa Barbara, USA, 2012; 180–198.
26. Emura K, Miyaji A, Nomura A, Omote K, Soshi M. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. In *5th International Conference on Information Security Practice and Experience (ISPEC 2009)*. Springer: Xi'an, China, 2009; 13–23.
27. Zhou Z, Huang D. On efficient ciphertext-policy attribute based encryption and broadcast encryption: extended abstract. In *Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS 2010)*. ACM: Chicago, IL, USA, 2010; 753–755.
28. Zhang Y, Zheng D, Chen X, Li J, Li H. Computationally efficient ciphertext-policy attribute-based encryption with constant-size ciphertexts. In *8th International Conference on Provable Security (ProvSec 2014)*. Springer: Hong Kong, 2014; 259–273.
29. Doshi N, Jinwala DC. Fully secure ciphertext policy attribute-based encryption with constant length ciphertext and faster decryption. *Security and Communication Networks* 2014; **7**(11): 1988–2002.
30. Cheung L, Newport C. Provably secure ciphertext policy abe. In *Proceedings of the 14th ACM conference on Computer and Communications Security (CCS 2007)*. ACM: Alexandria, Virginia, USA, 2007; 456–465.
31. Boneh D, Boyen X. Efficient selective-id secure identity-based encryption without random oracles. In *34th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2004)*. Springer: Interlaken, Switzerland, 2004; 223–238.
32. Fujisaki E, Okamoto T. Secure integration of asymmetric and symmetric encryption schemes. *Journal of Cryptology* 2013; **26**(1): 80–101.

33. Emura K, Miyaji A, Omote K, Nomura A. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. *International Journal of Applied Cryptography* 2010; **2**(1): 46–59.
34. Elgamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory* 1985; **31** (4): 469.
35. Harn L, Xu Y. Design of generalised elgamal type digital signature schemes based on discrete logarithm. *Electronics Letters* 1994; **30**(24): 2025–2026.
36. Scott M, Costigan N, Abdulwahab W. Implementing cryptographic pairings on smartcards. In *Workshop on Cryptographic Hardware and Embedded Systems (CHES 2006)*. Springer: Yokohama, Japan, 2006; 134–147.

 
DOI: 10.1002/sec