An Efficient CP-ABE with Constant Size Secret Keys using ECC for Lightweight Devices

Vanga Odelu [1], Ashok Kumar Das [2], and Adrijit Goswami [3]

[1] Department of Mathematics
Indian Institute of Technology, Kharagpur 721 302, India
E-mail: odelu.phd@maths.iitkgp.ernet.in, odelu.vanga@gmail.com

[2] Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad 500 032, India
E-mail: iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in

[3] Department of Mathematics
Indian Institute of Technology, Kharagpur 721 302, India
E-mail: goswami@maths.iitkgp.ernet.in, goswami@iitkgp.ac.in

Abstract

The energy cost of asymmetric cryptography is a vital component of modern secure communications, which inhibits its wide spread adoption within the ultra-low energy regimes such as Implantable Medical Devices (IMDs) and Radio Frequency Identification (RFID) tags. The ciphertext-policy attribute-based encryption (CP-ABE) is a promising cryptographic tool, where an encryptor can decide the access policy that who can decrypt the data. Thus, the 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 the 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 the cost efficient solutions for the encryption and decryption using ECC, called the CP-ABE-CSSK scheme. In the proposed CP-ABE-CSSK, the size of secret key is as small as 320 bits. In addition, ECC is efficient and more suitable for the lightweight devices as compared to the bilinear pairing based cryptosystem. Thus, the proposed CP-ABE-CSSK scheme provides the low computation and storage overheads with an expressive AND-gate access structure as compared to the related existing schemes in the literature. As a result, our scheme is very suitable for CP-ABE key storage and computation cost in the ultra-low energy devices.

Keywords: Attribute-based encryption, ciphertext-policy, constant-size secret key, elliptic curve cryptography, implantable medical devices, RFID tag, security.

1 Introduction

Implantable medical devices (IMDs) monitor and treat the physiological conditions within the body. These devices, including implantable cardiac defibrillators (ICDs) and drug delivery systems, etc., can help managing of a broad range of ailments, such as diabetes, cardiac arrhythmia, and Parkinson's disease. IMDs pervasiveness continues to swell, with upward of 25 million US citizens currently reliant on them for life-critical functions. The IMD should make its presence and type known to the authorized entities. A caregiver frequently needs to aware of an IMD's presence. For example, an ICD should be deactivated before surgery. For this reason, the FDA recently considers attaching remotely readable RFID tags to the implanted devices. Moreover, devices must report the measured data to the healthcare professionals or certain physiological values to the patients. An entity is authorized for a set of tasks on the basis of its role, such as physician or ambulance computer. The device manufacturer might also have special role-based access to the device. In the recent years, the newer IMDs are enhanced with wireless communications which will expend more energy than their passive predecessors. Since the devices are lightweight battery-limited and attached remotely with the readable RFID tags to implanted devices, the IMDs must ensure that the minimum power consumption and data storage overheads to maximize the lifetime of the device [19, 28, 3, 25].

In 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. As a result, CP-ABE is extremely suitable for medical health environment because it enables data owners to make and enforce access policies themselves [4, 29, 1]. Since the devices are lightweight and battery-limited, CP-ABE should ensure that it must offer the low storage overhead and cost effective mechanism for encryption and decryptions. Unfortunately, in the literature, most of the existing CP-ABE schemes so far use the bilinear maps and also produce the large size secret keys and ciphertexts, which are almost linear to the associated attributes, and the encryption and decryption require the group exponentiations, which are at least linear to the number of attributes involved in the access policy [18, 34, 8].

The bilinear map looses the high efficiency over 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 to the bilinear maps [32, 5, 22]. Therefore, designing an expressive access structure CP-ABE using ECC is an emerging research problem in this area. Due to 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 with the constant size secret keys, 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 [32, 10, 17] have been proposed with constant size secret keys and ciphertexts. Attribute-based encryption (ABE) is an extension of identity-based encryption. The first ABE scheme was introduced by Sahai and Waters [27], and it has two variants: Key-Policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE, the ciphertext is associated with an attribute set and the secret key is associated with an access policy. The ciphertext can be decrypted with the secret key if and only if the attribute set of ciphertext satisfies the access policy of secret key. On the contrary, in CP-ABE, the ciphertext is associated with an access policy and the secret key is associated with an attribute set. The ciphertext can be decrypted with the secret key if and only if the attributes of the secret key satisfies the ciphertext access policy.

After the introduction of Sahai-Waters's seminal work [27], several KP-ABE schemes [27, 16, 26, 2] and CP-ABE schemes [21, 7, 23, 30, 24] are presented in the literature. Since CP-ABE enables the data encryptor to choose the access policy to decide who can access the data, it is more appropriate in the access control applications as compared to the KP-ABE schemes [18]. Recently, several CP-ABE schemes have been proposed with the constant size ciphertexts [13, 33, 31, 11] and constant size secret keys [18, 13] with an expressive access structure based on the bilinear maps. Unfortunately, except EMNOS scheme [13], no CP-ABE scheme is found in the literature which can offer both the ciphertexts and secret keys of constant size. EMNOS scheme [13] offers only (n, n)-threshold and it is not hard to design such scheme [18]. GSWV scheme [18] offers constant size secret keys with an expressive AND-gate access structure. However, both EMNOS [13] and GSWV [18] schemes use the bilinear maps. Since the bilinear maps looses the high efficiency over ECC, both EMNOS [13] and GSWV [18] schemes are not well suitable for the ultra-low energy devices [32, 5, 22]. In Table 1, we have compared the different attribute-based encryption schemes with various access structures presented so far in the literature. Compared to the other related existing schemes in the literature, only our scheme provides the constant size secret keys which offers cost efficient solution for encryption and decryption with an expressive AND-gate access structure.

Table 1: Comparison of attribute-based encryption schemes

Scheme	KP/CP-ABE	Access structure	Security model	LSK	LCT
SW [27]	KP-ABE	Threshold	Selective security	nG	$nG + G_t$
GPSW [16]	KP-ABE	Tree	Selective security	$\|\mathbb{A}\|G$	$\|\mathbb{P}\|G + G_t$
OSW [26]	KP-ABE	Tree	Selective security	$2\|\mathbb{A}\|G$	$(\|\mathbb{P}\| + 1)G + G_t$
HLR [21]	CP-ABE	Threshold	Selective security	$(n + \|\mathbb{A}\|)G$	$2G + G_t$
CCLZFLW [7]	KP/CP-ABE	Threshold	Full security	$\mathcal{O}(n^2)$	$\mathcal{O}(1)$
EMNOS [13]	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 [30]	CP-ABE	LSSS	Selective security	$(\|\mathbb{A}\| + 2)G$	$(2\|\mathbb{P}\| + 1)G + G_t$
ALP [2]	KP-ABE	LSSS	Selective security	$3\|\mathbb{A}\|G$	$2G + G_t$
LW [24]	CP-ABE	LSSS	Full security	$(\|\mathbb{A}\| + 3)G_c$	$(2\|\mathbb{P}\| + 2)G_c + G_{t_c}$
DJ [11]	CP-ABE	AND gate-MV	Full security	$(n_{\mathbb{A}}\|\mathbb{A}\| + 2)G_c$	$2G_c + G_{t_c}$
ZZCLL [31]	CP-ABE	AND gate-MVW	Selective security	$(n + 1)G$	$2G + G_t$
CN [9]	CP-ABE	AND gates	Selective security	$(2\|\mathbb{A}\| + 1)G$	$(\|\mathbb{P}\| + 1)G + G_t$
ZH [33]	CP-ABE	AND gates	Selective security	$(\|\mathbb{A}\| + 1)G$	$2G + G_t$
GSWV [18]	CP-ABE	AND gates	Selective security	$2G$	$(n - \|\mathbb{P}\| + 2)G + G_t + L$
Ours	CP-ABE	AND gates	Selective security	$2 \times O(P)$	$(n - \|\mathbb{P}\| + 3)\mathbb{G} + L$

Note: 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; 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 which is assumed to be 160-bit integer in Z_p; $n_{\mathbb{A}}$: average number of values assigned to each attribute in attribute set $\mathbb{A}$.

1.2 Our contributions

The contributions of this paper are listed below:

- We propose a new CP-ABE using ECC, which offers constant-size secret keys with an expressive AND gate access structure. 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. A secret key associated with an attribute set $\mathbb{A}$ is used to decrypt ciphertexts with the access policy $\mathbb{P}$ if and only if $\mathbb{P} \subseteq \mathbb{A}$.

- It is shown that our CP-ABE-CSSK scheme is provably secure under the selective security model.

- Our CP-ABE-CSSK scheme provides the constant-size secret keys with expressive access structure.

- Since ECC is highly efficient as compared to the bilinear maps, our proposed CP-ABE-CSSK scheme is very suitable for implantable medical devices (IMDs) as compared to other related existing schemes in the literature.

1.3 Organization of the paper

The rest of the paper is sketched as follows. In Section 2, we discuss the related mathematical preliminaries and definitions in order to describe and analyze our CP-ABE-CSSK scheme. In Section 3, we propose a new ECC-based provably secure AND-gate access structured CP-ABE scheme, called CP-ABE-CSSK, which offers constant size secret keys with efficient encryption and decryption mechanisms. We provide the rigorous security analysis of our CP-ABE-CSSK scheme in Section 4. In Section 5, we compare the performance of the proposed CP-ABE-CSSK scheme with related existing schemes in the literature. Finally, the concluding remarks along with some open problems are provided in Section 6.

2 Mathematical preliminaries and definitions

In this section, we discuss the following mathematical preliminaries and definitions associated with the ciphertext-policy attribute-based encryption, which are useful in this paper.

2.1 Attribute and access structure

The attribute and access policy are defined as provided in [18]. Let the attribute universe $\mathbb{U} = \{A_1, A_2, \cdots, A_n\}$ be the set of n attributes $A_1, A_2, \cdots, A_n$. An attribute set of a user is denoted by $\mathbb{A} \subseteq \mathbb{U}$ and presented with an n-bit string $a_1 a_2 \cdots a_n$ 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 $b_1 b_2 \cdots b_n$, 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, we consider the AND gate access control structure represented by the attributes from $\mathbb{U}$. Assume that $\mathbb{A} = a_1 a_2 \cdots a_n$ is an attribute set and $\mathbb{P} = b_1 b_2 \cdots b_n$ the access policy. Then $\mathbb{P} \subseteq \mathbb{A}$ if and only if $a_i \geq b_i$, for all $i = 1, 2, \cdots, n$. We call that the attribute set $\mathbb{A}$ fulfills the access policy $\mathbb{P}$ if and only if $\mathbb{P} \subseteq \mathbb{A}$. Hereafter, we represent the attribute set $\mathbb{A}$ and access policy $\mathbb{P}$ with n-bit strings as defined above.

2.2 Computational hard problems

In this section, we consider the following computational hard problems [6]. We use the notations listed in Table 2 throughout the paper.

2.2.1 q-Generalized Diffie-Hellman (q-GDH) assumption

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

Definition 1 (q-GDH assumption [6]). *We say that $\mathbb{G}$ satisfies the (t, q, ϵ)-GDH assumption if for all t-time algorithms $\mathcal{A}$, we have the advantage $Adv^{GDH}_{\mathcal{A},q} = Pr[\mathcal{A}^{\mathcal{O}_{P,\boldsymbol{a}}} = (a_1 \cdots a_q)P] < \epsilon$, where $\boldsymbol{a} = (a_1, \cdots, a_q) \leftarrow$ $(Z_p)^q$ and for any sufficiently small $\epsilon > 0$.*

Table 2: Notations used in this paper

Symbol	Description
α, 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, $P, Q \in E_p(a,b)$
$\mathbb{G}$	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 $\mathbb{X}$

2.2.2 q-Diffie-Hellman Inversion (q-DHI) problem

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

Definition 2 (q-DHI assumption [6])**.** *We say that $\mathbb{G}$ satisfies the (t, q, ϵ)-DHI assumption if for all t-time algorithms $\mathcal{A}$, we have the advantage $Adv_{\mathcal{A},q}^{DHI} = Pr[\mathcal{A}(P, xP, x^2P, \cdots, x^qP) = (1/x)P] < \epsilon$ for any sufficiently small $\epsilon > 0$, where the probability is over the random choice of x in Z_p^* and the random bits of $\mathcal{A}$.*

2.3 Definition of CP-ABE scheme

CP-ABE encryption scheme is composed of the following four algorithms, namely, Setup, Encrypt, KeyGen, and Decrypt [18]:

- **Setup:** This algorithm takes a security parameter ρ and the universe of attributes $\mathbb{U} = \{A_1, A_2, \cdots, A_n\}$ as inputs, and 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 $\mathbb{A}$, the master public key MPK and the master secret key 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 $\mathbb{P}$, the public key MPK and the secret key k_u corresponding to the attribute set $\mathbb{A}$ as inputs, and outputs the original plaintext M or outputs null $(\perp)$ using the decryption algorithm $D[C, \mathbb{P}, k_u, \mathbb{A}]$.

A CP-ABE scheme must satisfy the following property. For any pair (MPK, MSK), a ciphertext $E[\mathbb{P}, M]$ and the secret key k_u, if $\mathbb{P} \subseteq \mathbb{A}$, the decryption algorithm always outputs the original plaintext M. Otherwise, the plaintext in $E[\mathbb{P}, M]$ cannot be decrypted using the key k_u.

2.4 Selective game for CP-ABE scheme

In order to prove the security under chosen ciphertext attack, we use the *selective game* for a CP-ABE scheme as defined in [18, 13]. The CP-ABE game captures the indistinguishability of messages and the collision-resistance of user secret keys, namely, the attackers cannot generate a new secret key by combining their secret keys. To capture the collision-resistance, the multiple secret key queries can be issued by an adversary $\mathcal{A}$ after the challenge phase. The game between the adversary $\mathcal{A}$ and a challenger $\mathcal{B}$ is as follows.

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

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

Definition 3. *CP-ABE scheme is said to be (t, q_s, q_d, ϵ)-selectively secure against a chosen-ciphertext attack, if for all t-polynomial time adversaries who make the q_s secret key queries at most and q_d decryption queries at most, where ϵ is a negligible function of ρ.*

3 The proposed CP-ABE-CSSK scheme

In this section, we propose a new CP-ABE scheme with constant size secret keys. We call this scheme as CP-ABE-CSSK using ECC. We also use the notations listed in Table 2 for describing our scheme. The CP-ABE-CSSK scheme consists of the following four phases, namely the Setup phase, Encrypt phase, KeyGen phase and Decrypt phase.

3.1 Setup phase

In this phase, the setup algorithm takes the security parameter ρ and the universe of attributes $\mathbb{U} = \{A_1, A_2, \cdots, A_n\}$ 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 α, 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:

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

where l_σ is the length of a random string under the security parameter, l_m the length of plaintext message M, $\{0,1\}^*$ a binary string of 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

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

3.2 Encrypt phase

The encryption is based on the approach presented in [18, 15] for providing the security against chosen-ciphertext attack:

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

where $E(\sigma_m, H_1(\mathbb{P}, M, \sigma_m)$ represents an attribute-based encryption on σ_m using the hash output $r_m = H_1(\mathbb{P}, M, \sigma_m)$ as the random number. More precisely, σ_m is encrypted with $k_m = KDF(r_m P)$ and M is encrypted with σ_m, and these are denoted by C_{σ_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 $i = 1, 2, \cdots, n$.

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

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

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

E3. Compute the ciphertext's parameters as follows:

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

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

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

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

$$C_m = H_3(\sigma_m) \oplus M. \tag{9}$$

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 phase

In this phase, 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

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

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

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,

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

Also, compute

$$\begin{aligned} u_1 &= r_u + k_1 t_u \pmod p, \\ u_2 &= s_u - k_2 t_u \pmod p. \end{aligned}$$

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

Proposition 1. *According to the polynomial functions $f(x, \mathbb{P})$ and $f(x, \mathbb{A})$ defined in Equations (4) and (10), respectively, we have*

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

It is not hard to verify that $\frac{f(x,\mathbb{P})}{f(x,\mathbb{A})}$ is polynomial function in x if and only if $\mathbb{P} \subseteq \mathbb{A}$ [18].

We design the encryption algorithm and construct the secret key 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 phase

This phase describes our decryption algorithm. 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 $\mathbb{A} = a_1 a_2 \cdots a_n$ does not fulfill the access policy $\mathbb{P} = b_1 b_2 \cdots b_n$, then abort. Otherwise, execute the next step.

D2. Compute

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

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

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

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

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

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

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

$$\begin{aligned} r_mP &= \frac{1}{F_0}((U+V)-W) \\ &= \frac{1}{F_0}(r_mF(\alpha)P-(r_mF(\alpha)P-r_mF_0P)) \\ &= \frac{r_mF(\alpha)-r_mF(\alpha)+r_mF_0}{F_0}P \\ &= r_mP. \end{aligned}$$

D4. Compute $\sigma'_m = H_2(KDF(r_mP)) \oplus C_{\sigma_m}$, $M' = C_m \oplus H_3(\sigma'_m)$ and $r'_m = H_1(\mathbb{P}, M', \sigma'_m)$. Then, verify whether the condition $r_mP = r'_mP$ 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, $U + V = r_mP$, 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 [9, 14]. 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 chosen-ciphertext attack under the selective security game.

Proposition 2. *Let $c_i = a_iy + b_iz$, for $i = 1, 2, \cdots, l$, 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 [12, 20]:*

- *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. *Our scheme 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, $i = 1, \cdots, l$, 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 $k_{u^i} = (u^i_1, u^i_2)$, where

$$u^i_1 = s_{u^i} + k_1.t_{u^i} \pmod p, \tag{14}$$

$$u^i_2 = r_{u^i} - k_2.t_{u^i} \pmod p. \tag{15}$$

From Step K2 of the $KeyGen$ algorithm (Section IV-C), we have

$$\frac{1}{f(\alpha, \mathbb{A}^i)} = k_1s_{u^i} + k_2r_{u^i} \pmod p. \tag{16}$$

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 $k_{u^i}, \forall i = 1, 2, \cdots, l$, 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. *Our scheme 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:*

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

Since $\sum_{i=1}^{n-|\mathbb{P}|} P_{m,i} = r_m(f(\alpha, \mathbb{P}) - f_0)P$, it is hard to compute $r_m P$ using K_{1m} and K_{2m} due to 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, ϵ)-GDH assumption also holds in $\mathbb{G}$.*

Proof. Suppose $\mathcal{A}$ is an algorithm that has advantage ϵ in solving the q-GDH problem. We construct an algorithm $\mathcal{B}$ that solves $(q-1)$-DHI with the same advantage ϵ. We follow the same proof as presented in [6].

Algorithm $\mathcal{B}$ is given $Q, \alpha Q, \alpha^2 Q, \cdots, \alpha^{q-1} Q \in \mathbb{G}$ as inputs, and its goal is to compute $(1/\alpha)Q \in \mathbb{G}$. Let $R = \alpha^{q-1} Q$ and $y = 1/\alpha$. Then, the inputs of $\mathcal{B}$ can be re-written as $R, yR, y^2 R, \cdots, y^{q-1} R \in \mathbb{G}$ and $\mathcal{B}$'s goal is to output $y^q R = (1/\alpha)Q = T$.

Algorithm $\mathcal{B}$ first picks q random values $r_1, \cdots, r_q \in Z_p$. After that it runs the algorithm $\mathcal{A}$ and simulates the oracle $\mathcal{O}_{R,\mathbf{a}}$ for $\mathcal{A}$. The vector $\mathbf{a}$ that $\mathcal{B}$ will use is $\mathbf{a} = (y + r_1, \cdots, y + r_q)$. Note that $\mathcal{B}$ does not know the vector $\mathbf{a}$ explicitly since $\mathcal{B}$ does not have $y = 1/\alpha$. When $\mathcal{A}$ issues a query for $\mathcal{O}_{R,\mathbf{a}}(S)$ for some strict subset $S \subset \{1, \cdots, q\}$, the algorithm $\mathcal{B}$ responds as follows:

- Define the polynomial $f(x) = \prod_{i \in S}(x + r_i)$ and expand the terms to obtain $f(x) = \sum_{i=0}^{|S|} f_i x^i$.

- Compute $Y = \sum_{i=0}^{|S|}(f_i y^i R) = f(y)R$. Since $|S| < q$, all the values $y^i R$ in the sum are known to $\mathcal{B}$.

- By construction we know that $Y = \left(\prod_{i \in S}(y + r_i)\right)R$. Algorithm $\mathcal{B}$ 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 **a** $= (y+r_1, \cdots, y+r_q)$. Therefore, eventually, $\mathcal{A}$ will output $Z = \left(\prod_{i=1}^{q}(y + r_i)\right)R$. Define the polynomial $f(x) = \prod_{i=1}^{q}(x + r_i)$ and expand the terms to get $f(x) = x^q + \sum_{i=0}^{q-1} f_i x^i$. To conclude, $\mathcal{B}$ outputs $T = Z - \sum_{i=0}^{q-1} f_i y^i R = y^q R$. which is the required value. □

Remark 3. *From the above 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. *Our CP-ABE-CSSK scheme is (t, q_s, q_d, ϵ)-selectively secure if the q-GDH problem is (t', ϵ')-hard, where $t' = t + \mathcal{O}(q_s(t_{inv} + nt_{mul}) + q_{H_1} nt_{em})$, $\epsilon' = \epsilon - \frac{q_{H_2}}{p}$, $n = |\mathbb{U}|$, $q = n - |\mathbb{P}|$, and t_{inv}, t_{mul} and t_{em} denote the average time required for group inverse, multiplication and point multiplication operations, respectively, and q_{H_1}, q_{H_2} denote the number of queries made to the random oracles H_1 and H_2, respectively.*

5 Performance comparison with related existing schemes

In this section, we compare the performance of our CP-ABE-CSSK scheme with the related existing schemes.

From Table 1, we see that EMNOS scheme [13] 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). GSWV scheme [18] provides an efficient solution for only the shorter secret keys with an expressive AND gate access structure. Furthermore, in Table 1, we have compared the different attribute-based encryption schemes with various access structures. Our scheme is the first proposed CP-ABE scheme, which provides constant size secret keys with the expressive access structure without using bilinear maps. The size of the secret key k_u in our scheme is $|k_u| = 2 \times O(P) = 320$ bits as the 163-bit ECC provides the 80-bit security [22]. However, in GSWV scheme [18], 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 [18]. From Table 3, it is observed that our scheme reduces the number of group exponentiations required for encryption and decryption to the half as compared to GSWV scheme [18]. 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. As a result, our scheme is very suitable for practical applications as compared to the other related existing CP-ABE schemes in the literature.

Table 3: Comparison of computational complexity

Scheme	Encryption	Decryption
EMNOS [13]	$(n+1)T_G + 2T_{G_t}$	$2T_{G_t} + 2T_e$
GSWV [18]	$\big(2(n - \lvert\mathbb{P}\rvert) + 2\big)T_G$	$2(\lvert\mathbb{A}\rvert - \lvert\mathbb{P}\rvert)T_G + 1T_{G_t} + 3T_e$
Ours	$(n - \lvert\mathbb{P}\rvert + 2)T_{ecm\mathbb{G}}$	$(n - \lvert\mathbb{P}\rvert + 3)T_{ecm\mathbb{G}}$

Note: 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_{G_c}: time to execute an exponentiation in the composite group G_c; 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 $\mathbb{G}$; $n_{\mathbb{P}}$: average number of values assigned to each attribute in the access policy $\mathbb{P}$.

6 Conclusion

In this paper, we have proposed a novel ECC-based CP-ABE-CSSK scheme with the constant size secret keys 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, the proposed CP-ABE-CSSK offers the constant size secret keys, which is as small as 320-bits for the 80-bit security. The CP-ABE-CSSK also significantly reduces the encryption and decryption costs as compared to the related existing schemes in the literature. We have showed that our scheme is secure against possible known attacks, such as key recovery and collision attacks. In addition, we have shown that our scheme is secure under the chosen-ciphertext adversary. Thus, CP-ABE-CSSK offers constant size secret keys along with efficient solution for encryption and decryption under the chosen ciphertext adversary, which supports an expressive AND gate access structure.

References

[1] A. Abbas and S. U. Khan. A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. *IEEE Journal of Biomedical and Health Informatics*, 18(4):1431–1441, 2014.

[2] N. Attrapadung, B. Libert, and E. De Panafieu. Expressive key-policy attribute-based encryption with constant-size ciphertexts. In *14th International Conference on Practice and Theory in Public Key Cryptography (PKC 2011)*, pages 90–108. Springer, Taormina, Italy, 2011.

[3] L. Atzori, A. Iera, and G. Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.

[4] S. Avancha, A. Baxi, and D. Kotz. Privacy in mobile technology for personal healthcare. *ACM Computing Surveys*, 45(1):3, 2012.

[5] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott. Efficient algorithms for pairing-based cryptosystems. In *22nd International Conference on Cryptology (CRYPTO 2002)*, pages 354–369. Springer, Santa Barbara, USA, 2002.

[6] D. Boneh and X. Boyen. 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)*, pages 223–238, Interlaken, Switzerland, 2004. Springer.

[7] C. Chen, J. Chen, H. W. Lim, Z. Zhang, D. Feng, S. Ling, and H. Wang. 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)*, pages 50–67. Springer, San Francisco, CA, USA, 2013.

[8] C. Chen, Z. Zhang, and D. Feng. Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost. In *5th International Conference on Provable Security (ProvSec 2011)*, pages 84–101. Springer, Xi'an, China, 2011.

[9] L. Cheung and C. Newport. Provably secure ciphertext policy abe. In *Proceedings of the 14th ACM conference on Computer and Communications Security (CCS 2007)*, pages 456–465, Alexandria, Virginia, USA, 2007. ACM.

[10] C. Delerablée. Identity-based broadcast encryption with constant size ciphertexts and private keys. In *Proceedinds of 13th International Conference on the Theory and Applications of Crptology and Information Security (ASIACRYPT 2007)*, pages 200–215. Springer, Kuching, Malaysia, 2007.

[11] N. Doshi and D. C. Jinwala. Fully secure ciphertext policy attribute-based encryption with constant length ciphertext and faster decryption. *Security and Communication Networks*, 7(11):1988–2002, 2014.

[12] T. Elgamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469, 1985.

[13] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. In *5th International Conference on Information Security Practice and Experience (ISPEC 2009)*, pages 13–23. Springer, Xi'an, China, 2009.

[14] K. Emura, A. Miyaji, K. Omote, and A. Nomura. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. *International Journal of Applied Cryptography*, 2(1):46–59, 2010.

[15] E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. *Journal of Cryptology*, 26(1):80–101, 2013.

[16] V. Goyal, O. Pandey, A. Sahai, and B. Waters. 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)*, pages 89–98, Alexandria, VA, USA, 2006. ACM.

[17] F. Guo, Y. Mu, and W. Susilo. Identity-based traitor tracing with short private key and short ciphertext. In *Welcome to the European Symposium on Research in Computer Security (ESORICS 2012)*, pages 609–626. Springer, Pisa, Italy, 2012.

[18] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan. CP-ABE With Constant-Size Keys for Lightweight Devices. *IEEE Transactions on Information Forensics and Security*, 9(5):763–771, 2014.

[19] D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu, and W. H. Maisel. Security and privacy for implantable medical devices. *IEEE Pervasive Computing*, 7(1):30–39, 2008.

[20] L. Harn and Y. Xu. Design of generalised elgamal type digital signature schemes based on discrete logarithm. *Electronics Letters*, 30(24):2025–2026, 1994.

[21] J. Herranz, F. Laguillaumie, and C. Ràfols. Constant size ciphertexts in threshold attribute-based encryption. In *13th International Conference on Practice and Theory in Public Key Cryptography (PKC 2010)*, pages 19–34. Springer, Paris, France, 2010.

[22] K. Lauter. The advantages of elliptic curve cryptography for wireless security. *IEEE Wireless communications*, 11(1):62–67, 2004.

[23] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters. 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)*, pages 62–91. Springer, French Riviera, 2010.

[24] A. Lewko and B. Waters. New proof methods for attribute-based encryption: Achieving full security through selective techniques. In *32nd International Conference on Cryptology (CRYPTO 2012)*, pages 180–198. Springer, Santa Barbara, USA, 2012.

[25] M. Li, W. Lou, and K. Ren. Data security and privacy in wireless body area networks. *IEEE Wireless Communications*, 17(1):51–58, 2010.

[26] R. Ostrovsky, A. Sahai, and B. Waters. Attribute-based encryption with non-monotonic access structures. In *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS 2007)*, pages 195–203, Alexandria, Virginia, USA, 2007. ACM.

[27] A. Sahai and B. Waters. Fuzzy identity-based encryption. In *25th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2005)*, pages 457–473. Springer, Aarhus, Denmark, 2005.

[28] A. D. Targhetta, D. E. Owen, and P. V. Gratz. The design space of ultra-low energy asymmetric cryptography. In *IEEE International on Symposium on Performance Analysis of Systems and Software (ISPASS 2014)*, pages 55–65. IEEE, 2014.

[29] Z. Wan, J. Liu, and R. H. Deng. Hasbe: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing. *IEEE Transactions on Information Forensics and Security*, 7(2):743–754, 2012.

[30] B. Waters. 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)*, pages 53–70. Springer, Taormina, Italy, 2011.

[31] Y. Zhang, D. Zheng, X. Chen, J. Li, and H. Li. Computationally Efficient Ciphertext-Policy Attribute-Based Encryption with Constant-Size Ciphertexts. In *8th International Conference on Provable Security (ProvSec 2014)*, pages 259–273. Springer, Hong Kong, 2014.

[32] M. Zheng, Y. Xiang, and H. Zhou. A strong provably secure ibe scheme without bilinear map. *Journal of Computer and System Sciences*, 81(1):125–131, 2015.

[33] Z. Zhou and D. Huang. 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)*, pages 753–755, Chicago, IL, USA, 2010. ACM.

[34] Z. Zhou, D. Huang, and Z. Wang. Efficient Privacy-Preserving Ciphertext-Policy Attribute Based-Encryption and Broadcast Encryption. *IEEE Transactions on Computers*, 64(1):126–138, 2015.