Received January 16, 2017, accepted February 6, 2017, date of publication February 16, 2017, date of current version March 28, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2669940

Expressive CP-ABE Scheme for Mobile Devices in IoT Satisfying Constant-Size Keys and Ciphertexts

VANGA ODELU[1], ASHOK KUMAR DAS[2], MUHAMMAD KHURRAM KHAN[3], (Senior Member, IEEE), KIM-KWANG RAYMOND CHOO[4], (Senior Member, IEEE), AND MINHO JO[5], (Senior Member, IEEE)

[1]Department of Computer Convergence Software, Indian Institute of Information Technology, Sricity 517 588, India
[2]Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India
[3]Center of Excellence in Information Assurance, King Saud University, Riyadh 12372, Saudi Arabia
[4]Department of Information Systems and Cyber Security, The University of Texas at San Antonio, TX 78249, USA
[5]Department of Computer Convergence Software, Korea University, Sejong Metropolitan city 30019, South Korea

Corresponding author: M. Jo (minhojo@korea.ac.kr)

This research was supported in part by the Korea-China Joint Research Center Program through National Research Foundation (NRF), South Korea, under Grant 2016K1A3A1A20006024 and in part by Deanship of Scientific Research at King Saud University under Grant PRG-1436-16.

ABSTRACT Designing lightweight security protocols for cloud-based Internet-of-Things (IoT) applications for battery-limited mobile devices, such as smart phones and laptops, is a topic of recent focus. Ciphertext-policy attribute-based encryption (CP-ABE) is a viable solution, particularly for cloud deployment, as an encryptor can "write" the access policy so that only authorized users can decrypt and have access to the data. However, most existing CP-ABE schemes are based on the costly bilinear maps, and require long decryption keys, ciphertexts and incur significant computation costs in the encryption and decryption (e.g. costs is at least linear to the number of attributes involved in the access policy). These design drawbacks prevent the deployment of CP-ABE schemes on battery-limited mobile devices. In this paper, we propose a new RSA-based CP-ABE scheme with constant size secret keys and ciphertexts (CSKC) and has $\mathcal{O}(1)$ time-complexity for each decryption and encryption. Our scheme is then shown to be secure against a chosen-ciphertext adversary, as well as been an efficient solution with the expressive AND gate access structures (in comparison to other related existing schemes). Thus, the proposed scheme is suitable for deployment on battery-limited mobile devices.

INDEX TERMS Mobile devices, cloud computing, ciphertext-policy attribute-based encryption, constant-size secret key, constant-size ciphertext, RSA-based cryptography.

I. INTRODUCTION

With the popularity and availability of battery-limited mobile devices (e.g. Android and iOS devices), there is an increasing demand to design efficient and secure lightweight applications for such devices [1]–[3]. In a ciphertext-policy attribute-based encryption (CP-ABE), data are encrypted based on the access policy and each user associated with a set of attributes is able to decrypt a ciphertext, if and only, if the user's attributes fulfill the ciphertext access policy. Thus, CP-ABE is extremely suitable for cloud computing environment because it enables data owners to make and enforce access policies themselves [4]–[8], [49]. Since most mobile devices are battery-limited, key design criteria in a CP-ABE scheme should include constant size secret key and constant size ciphertext, as well as a cost efficient mechanism for encryption and decryption.

In the literature, several identity-based encryption schemes [9]–[11] with constant size secret keys and ciphertexts have been proposed. Attribute-based encryption (ABE), an extension of identity-based encryption, scheme was first introduced by Sahai-Waters [12] and has two variants, namely: Key-Policy ABE (KP-ABE) [12]–[15] and ciphertext-policy ABE (CP-ABE) [16]–[20]. In KP-ABE, ciphertext is associated with the 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. As CP-ABE enables the data encryptor to choose

TABLE 1. Attribute-based encryption schemes: A comparative summary.

Scheme	KP/CP-ABE	Access structure	Security model	LSK	LCT
SW [12]	KP-ABE	Threshold	Selective security	nG	$nG + G_t$
GPSW [13]	KP-ABE	Tree	Selective security	$\|\mathbb{A}\|G$	$\|\mathbb{P}\|G + G_t$
OSW [14]	KP-ABE	Tree	Selective security	$2\|\mathbb{A}\|G$	$(\|\mathbb{P}\| + 1)G + G_t$
BSW [26]	CP-ABE	Tree	Selective security	$(2\|\mathbb{A}\| + 1)G$	$(2\|\mathbb{P}\| + 1)G + G_t$
HLR [16]	CP-ABE	Threshold	Selective security	$(n + \|\mathbb{A}\|)G$	$2G + G_t$
CCLZFLW [17]	KP/CP-ABE	Threshold	Full security	$\mathcal{O}(n^2)$	$\mathcal{O}(1)$
EMNOS [21]	CP-ABE	(n, n)-Threshold	Selective security	$2G$	$2G + G_t$
LOSTW [18]	CP-ABE	Linear secret-sharing scheme	Full security	$(\|\mathbb{A}\| + 2)G_c$	$(2\|\mathbb{P}\| + 1)G_c + G_{t_c}$
Waters [19]	CP-ABE	Linear secret-sharing scheme	Selective security	$(\|\mathbb{A}\| + 2)G$	$(2\|\mathbb{P}\| + 1)G + G_t$
ALP [15]	KP-ABE	Linear secret-sharing scheme	Selective security	$3\|\mathbb{A}\|G$	$2G + G_t$
LW [20]	CP-ABE	Linear secret-sharing scheme	Full security	$(\|\mathbb{A}\| + 3)G_c$	$(2\|\mathbb{P}\| + 2)G_c + G_{t_c}$
DJ [23]	CP-ABE	AND gate-Multivalued	Full security	$(n_{\mathbb{A}}\|\mathbb{A}\| + 2)G_c$	$2G_c + G_{t_c}$
ZZCLL [4]	CP-ABE	AND gate-Multivalued with wildcards	Selective security	$(n + 1)G$	$2G + G_t$
CN [27]	CP-ABE	AND gates	Selective security	$(2\|\mathbb{A}\| + 1)G$	$(\|\mathbb{P}\| + 1)G + G_t$
ZH [22]	CP-ABE	AND gates	Selective security	$(\|\mathbb{A}\| + 1)G$	$2G + G_t$
GSWV [24]	CP-ABE	AND gates	Selective security	$2G$	$(n - \|\mathbb{P}\| + 2)G + G_t + L$
Ours	CP-ABE	AND gates	Selective security	$2G$	$3G + L$

Note: LSK: length of user secret key; LCT: length of ciphertext; L: length of plaintext M; G and G_t: prime order pairing (note that in our scheme, the group G is multiplicative group Z_N, where $N = pq$); G_c and G_{t_c}: composite order pairing; $n_{\mathbb{A}}$: average number of values assigned to each attribute in attribute set $\mathbb{A}$.

the access policy and decide who can access the data, it is more suited for access control applications as compared to KP-ABE schemes.

Unsurprisingly, several CP-ABE schemes with constant size ciphertexts [4], [21]–[23] and constant size secret keys [21], [24] with an expressive access structure based on bilinear maps have been proposed in recent times. In these schemes, with the exception of the EMNOS scheme [21], only the ciphertexts or the secret keys are of constant size (but not both). The EMNOS scheme [21] offers only (n, n)-threshold and most existing schemes require significant computational complexity for encryption and decryption, which are at least linear to the number of attributes involved in the access policy. In addition, these schemes are based on bilinear maps, which is significantly more costly than schemes based on conventional cryptosystems [9], [25]. Thus, designing a cost efficient and expressive access structure CP-ABE with the constant size secret keys and ciphertexts (CSKC) using conventional public-key cryptosystems remains a research challenge. This is the gap that we seek to address.

In this paper, we propose a RSA-based AND-gate access structure CP-ABE scheme, which offers constant size secret keys and ciphertexts with efficient encryption and decryption mechanism. In our scheme, 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 $\mathbb{P} \subseteq \mathbb{A}$. Our scheme requires only $\mathcal{O}(1)$ time-complexity. It is clear from Table 1, only our scheme provides constant size secret keys and ciphertexts without using bilinear maps. We then demonstrate the security of the scheme under the selective security model. To the best of our knowledge, this is the first attempt to design such a provably secure RSA-based AND-gate access structure CP-ABE scheme. Due to the underlying RSA architecture, our scheme is suitable for practical deployments on battery-limited devices. Moreover, our scheme provides an efficient solution to the encryption and decryption, which requires only $\mathcal{O}(1)$ time-complexity (see Tables 3 and 6).

The rest of the paper is organized as follows. In Section II, we discuss the mathematical preliminaries and definitions required in the understanding of the proposed scheme. In Section III, we briefly discuss the key management in a defined access structure. In Sections IV and V, we present the proposed scheme and the security analysis, respectively. In Section VI, we evaluate the performance of our scheme with related schemes. Finally, the paper is concluded in Section VII.

II. MATHEMATICAL PRELIMINARIES AND DEFINITIONS

In this section, we discuss the mathematical preliminaries and definitions associated with ciphertext-policy attribute-based encryption.

A. ATTRIBUTE AND ACCESS STRUCTURE

We define the attribute and access policy as provided in [24]. Let the attribute universe $\mathbb{U} = \{A_1, A_2, \cdots, A_n\}$ be the set of n attributes $A_1, A_2, \cdots, A_n$. We denote an attribute set of a user by $\mathbb{A} \subseteq \mathbb{U}$, and an n-bit string $a_1a_2 \cdots a_n$ associated with $\mathbb{A}$ is 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 associated with $\mathbb{A}$ becomes 1101. In addition, we define an access policy by $\mathbb{P}$ specified with attributes in $\mathbb{U}$, and an n-bit string $b_1b_2 \cdots b_n$ associated with $\mathbb{P}$ is defined as follows: $b_i = 1$, if $A_i \in \mathbb{P}$ and $b_i = 0$, if $A_i \notin \mathbb{P}$. For example, for $n = 4$ the string 1010 associated with $\mathbb{P}$ means that $\mathbb{P}$ 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 $a_1a_2 \cdots a_n$ is an n-bit string associated with attribute set $\mathbb{A}$ and $b_1b_2 \cdots b_n$ an n-bit string associated with the access policy $\mathbb{P}$. 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 $\mathbb{P} \subseteq \mathbb{A}$.

B. COMPUTATIONALLY HARD PROBLEMS

In this section, we consider the following two computational problems.

1) INTEGER FACTORIZATION PROBLEM (IFP)

Let p and q be ρ-bit primes and $N = pq$. Assume that Gen_F be a polynomial-time algorithm which takes an input 1^ρ and outputs (N, p, q). The factoring assumption relative to Gen_F states that given N, it is computationally infeasible (hard) problem to derive p and q, except with negligible probability in ρ. The formal definition of this problem follows that of [28]: for a probabilistic polynomial-time (PPT) algorithm $\mathcal{A}$, the factoring advantage is defined by

$$Adv^{IFP}_{Gen_F,\mathcal{A}}(\rho) = Pr[(N, p, q) \leftarrow Gen_F(1^\rho) : \mathcal{A}(N) = \{p, q\}].$$

The factoring assumption (with respect to Gen_F) states that $Adv^{IFP}_{Gen_F,\mathcal{A}}(\rho)$ is negligible in ρ for every PPT $\mathcal{A}$. We say that $(t_{IFP}, \epsilon_{IFP})$-IFP assumption holds if $Adv^{IFP}_{Gen_F,\mathcal{A}}(\rho) \leq \epsilon_{IFP}(\rho)$, for any sufficiently small $\epsilon_{IFP}(\rho) > 0$, and its running time is at most t_{IFP}.

2) COMPUTATIONAL Diffie-Hellman PROBLEM (CDHP)

The problem of breaking the Diffie-Hellman scheme with a RSA modulus $N = pq$ and base g is equivalent to the problem of computing a value of the following function [29]:

$$CDHP(N, g, X, Y) : \langle g \rangle_N \times \langle g \rangle_N \rightarrow \langle g \rangle_N,$$

which is defined by

$$CDHP(N, g, g^a, g^b) = g^{ab} \pmod N.$$

Here, $\langle g \rangle_N$ represents a cyclic subgroup of Z_N^* generated by g. The adversary $\mathcal{A}$ advantage in solving the CDHP is:

$$Adv^{CDHP}_{Z_N,\mathcal{A}}(\rho) = Pr[\mathcal{A}(N, g, g^a, g^b) = g^{ab}].$$

We say that $(t_{CDHP}, \epsilon_{CDHP})$-CDH assumption holds if $Adv^{CDHP}_{Z_N,\mathcal{A}}(\rho) \leq \epsilon_{CDHP}$, for any sufficiently small $\epsilon_{CDHP} > 0$, with its running time at most t_{CDHP}.

As stated in [29], any algorithm that will break the CDHP for a non-negligible proportion of the possible inputs can be used to factor N. This implies any algorithm that will break the CDHP for a given modulus N can also be used to break the original Diffie-Hellman scheme for the prime moduli that are factors of N.

Definition 1 ((t, ϵ)-Hard n-IF-CDH Problem): We say that a t-polynomial time algorithm $\mathcal{A}$, which outputs a bit $\gamma \in \{0, 1\}$, has an advantage $Adv^{IF-CDH}_{Z_N,\mathcal{A}}(\rho) = \epsilon$ in solving the n-IF-CDH problem in Z_N if

$$\Big| Pr\big[\mathcal{A}(N, p_1, \cdots, p_n, g, g^k, g^x, g^{kr}, g^{xr}, g^d, g^{rd}) = 0\big] - Pr\big[\mathcal{A}(N, p_1, \cdots, p_n, g, g^k, g^x, g^{kr}, g^{xr}, g^d, T) = 0\big] \Big| \geq \epsilon.$$

C. DEFINITION OF CP-ABE SCHEME

A CP-ABE encryption scheme is composed of four algorithms, namely, Setup, Encrypt, KeyGen, and Decrypt. These algorithms are defined as follows [24]:

- **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 then outputs 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 plaintext M as inputs. The encryption algorithm $E[\mathbb{P}, M]$ 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 outputs a user secret key (decryption key) k_u corresponding to $\mathbb{A}$.
- **Decrypt:** It takes a ciphertext C generated with 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 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 (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 corrected plaintext M. Otherwise, the plaintext in $E[\mathbb{P}, M]$ cannot be decrypted using the key k_u.

D. 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 [21], [24]. The CP-ABE game captures the indistinguishability of messages and the collision-resistance of user secret keys, namely, 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 described 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 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 $\mathbb{P}'$. $\mathcal{B}$ answers with a secret key k_{u^i} for these attributes.
  - The decryption query on ciphertext $E[\mathbb{P}^i, M^i]$.
- **Challenge:** In this phase, 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 ciphertext $E[\mathbb{P}', M_{c'}]$ for challenge to $\mathcal{A}$.
- **Query:** The adversary $\mathcal{A}$ can continue with the secret key queries and decryption queries except with a secret key query on any $\mathbb{A}$ fulfilling $\mathbb{P}'$ 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 2: The CP-ABE scheme is said to be (t, q_e, q_c, ϵ) selectively secure against a chosen-ciphertext attack, if for all t-polynomial time adversaries who make the q_e secret key queries at most and q_c decryption queries at most, ϵ is a negligible function of ρ.

III. KEY MANAGEMENT IN DEFINED ACCESS STRUCTURE

In this section, we discuss the key management in the defined access structure motivated by the scheme in [30], which is a variant of Akl-Taylor's scheme [31]. The scheme in [30] is proven secure against key recovery attacks. Let Z_N be the set of equivalence classes of the integers modulo $N = pq$, where p and q are RSA secure primes with $p \neq q$. For any non-zero element $a \in Z_N$, $\gcd(a, N) = 1$ if and only if there exists a multiplicative inverse b for $a \pmod N$, that is, $ab \equiv 1 \pmod N$ or $b \equiv a^{-1} \pmod N$ which can be computed efficiently using the extended Euclidean gcd algorithm, where $1 \in Z_N$ is the multiplicative identity. The key management is described below.

Pick a secure prime number p_i such that $\gcd(p_i, \phi(N)) = 1$, $\forall i = 1, 2, \cdots, n$, to each attribute $A_i \in \mathbb{U}$. Then, compute the inverse q_i of p_i such that $p_i q_i \equiv 1 \pmod{\phi(N)}$, where $p_i \neq p_j$ if and only if $i \neq j$. Assume that $\{\phi(N), q_1, \cdots, q_n\}$ be the secret parameters and $\{N, p_1, \cdots, p_n\}$ the public parameters. Since factoring the product $N = pq$ is computationally hard problem, computing $\phi(N) = (p-1)(q-1)$ without the knowledge of secure primes p and q is also computationally infeasible. This implies that computing the secret primes q_i using the corresponding public prime p_i depends on the integer factorization problem, and as a result, computing the prime q_i such that $p_i q_i \equiv 1 \pmod{\phi(N)}$ is also computationally hard problem.

Choose a random number g such that $2 < g < N - 1$, and $\gcd(g, N) = 1$, and compute the secret keys $K_{\mathbb{A}}$ and $K_{\mathbb{P}}$ associated to the attribute set $\mathbb{A}$ and access policy $\mathbb{P}$, respectively, as follows:

$$K_{\mathbb{A}} = g^{d_{\mathbb{A}}} \pmod N,$$
$$K_{\mathbb{P}} = g^{d_{\mathbb{P}}} \pmod N,$$

where $d_{\mathbb{A}} = \prod_{i=1}^{n} q_i^{a_i}$, $a_i \in \mathbb{A}$ and $d_{\mathbb{P}} = \prod_{i=1}^{n} q_i^{b_i}$, $b_i \in \mathbb{P}$.

Proposition 1: The attribute set $\mathbb{A}$ fulfills access policy $\mathbb{P}$ (that is, $\mathbb{P} \subseteq \mathbb{A}$) if and only if $\frac{e_{\mathbb{A}}}{e_{\mathbb{P}}}$ is an integer, where $e_{\mathbb{P}} = \prod_{i=1}^{n} p_i^{b_i}$, $e_{\mathbb{A}} = \prod_{i=1}^{n} p_i^{a_i}$, and $K_{\mathbb{P}} = K_{\mathbb{A}}^{\frac{e_{\mathbb{A}}}{e_{\mathbb{P}}}} \pmod N$. In this case, we can write $\frac{e_{\mathbb{A}}}{e_{\mathbb{P}}} = \prod_{i=1}^{n} p_i^{a_i - b_i}$ as an integer.

Proof: Assume that $\mathbb{A}$ does not fulfill $\mathbb{P}$, that is, $\mathbb{P} \not\subseteq \mathbb{A}$. Then, $a_i - b_i \in \{-1, 0, 1\}$ as $a_i, b_i \in \{0, 1\}$. This implies that in the fraction $\frac{e_{\mathbb{A}}}{e_{\mathbb{P}}}$ at least one inverse term, say p_j^{-1} exists, and thus, computing p_j^{-1} without factoring $N = pq$ is a hard problem. As a result, $\frac{e_{\mathbb{A}}}{e_{\mathbb{P}}}$ can not be an integer when $\mathbb{P} \not\subseteq \mathbb{A}$.

On the other hand, if $\mathbb{P} \subseteq \mathbb{A}$, the secret key $K_{\mathbb{P}}$ is computed as follows:

$$\begin{aligned}
K_{\mathbb{P}} &= K_{\mathbb{A}}^{\frac{e_{\mathbb{A}}}{e_{\mathbb{P}}}} \pmod N \\
&= \left(g^{d_{\mathbb{A}}} \pmod N\right)^{\frac{\prod_{i=1}^{n} p_i^{a_i}}{\prod_{i=1}^{n} p_i^{b_i}}} \pmod N \\
&= g^{d_{\mathbb{A}}(\prod_{i=1}^{n} p_i^{a_i - b_i})} \pmod N \\
&= g^{(\prod_{i=1}^{n} (q_i)^{a_i})(\prod_{i=1}^{n} p_i^{a_i - b_i})} \pmod N \\
&= g^{(\prod_{i=1}^{n} q_i^{a_i - b_i + b_i})(\prod_{i=1}^{n} p_i^{a_i - b_i})} \pmod N \\
&= g^{(\prod_{i=1}^{n} q_i^{b_i})(\prod_{i=1}^{n} q_i^{a_i - b_i} (p_i)^{a_i - b_i})} \pmod N \\
&= g^{(\prod_{i=1}^{n} q_i^{b_i})(\prod_{i=1}^{n} (q_i p_i)^{a_i - b_i})} \pmod N \\
&= g^{\prod_{i=1}^{n} q_i^{b_i}} \pmod N \\
&= g^{d_{\mathbb{P}}} \pmod N.
\end{aligned}$$

Thus, we arrive at the result. □

Example 1: This is an example related to the key management problem in the defined access structure. Let 1101 and 1001 be the 4-bit strings associated with the attribute set $\mathbb{A}$ and access policy $\mathbb{P}$, respectively. Suppose the chosen RSA pairs corresponding to the attributes A_i's are (p_i, q_i), where $i = 1, 2, 3, 4$. Thus, $\mathbb{A} = \{A_1, A_2, A_4\}$ and $\mathbb{P} = \{A_1, A_4\}$. It is clearly that $\mathbb{P} \subseteq \mathbb{A}$. Then, we have $K_{\mathbb{A}} = g^{q_1 q_2 q_4}$, $K_{\mathbb{P}} = g^{q_1 q_4}$, $e_{\mathbb{A}} = p_1 p_2 p_4$ and $e_{\mathbb{P}} = p_1 p_4$. $K_{\mathbb{P}}$ using $K_{\mathbb{A}}$ is computed as follows:

$$\begin{aligned}
K_{\mathbb{P}} &= K_{\mathbb{A}}^{\frac{e_{\mathbb{A}}}{e_{\mathbb{P}}}} \pmod N \\
&= (g^{q_1 q_2 q_4})^{\frac{p_1 p_2 p_4}{p_1 p_4}} \pmod N \\
&= (g^{q_1 q_2 q_4})^{p_2} \pmod N \\
&= g^{(q_1 q_4)(q_2 p_2)} \pmod N \\
&= g^{q_1 q_4} \pmod N.
\end{aligned}$$

IV. PROPOSED CP-ABE-CSKC SCHEME

In this section, we present the proposed CP-ABE scheme with constant size secret keys and ciphertexts, hereafter referred to as CP-ABE-CSKC. The notations used in our scheme are listed in Table 2. For ease of reading, mod(N) will be omitted from $g^z \pmod N$ for the remainder of this paper (i.e. g^z instead of $g^z \pmod N$). The CP-ABE-CSKC scheme consists of the following four phases, namely: Setup, Encrypt, KeyGen and Decrypt.

A. 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 two RSA primes p and q with $p \neq q$, and compute $N = pq$. Then, randomly select the RSA public exponent p_i with $\gcd(p_i, \phi(N)) = 1$, and compute q_i such that $p_i q_i \equiv 1 \pmod{\phi(N)}$ corresponding to each attribute $A_i \in \mathbb{U}$, $\forall i = 1, 2, \cdots, n$. Further, pick two system private keys k and x such that

TABLE 2. Notations.

Notation	Description
(k, x)	The system private key pair.
$N = pq$	RSA modulus with large primes p and q, $p \neq q$.
Z_N	Set of equivalence classes of integers modulo N.
$\phi(\cdot)$	Euler's phi (totient) function, and $\phi(N) = (p-1)(q-1)$.
H_1, H_2, H_3	Three one-way collision-resistance hash functions.
$\mathbb{U}$	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 $\mathbb{X}$.

$\gcd(k, \phi(N)) = 1$, $\gcd(k, q_i) = 1$ and $\gcd(x, q_i) = 1$ for all $i = 1, 2, \cdots, n$. Next, select a random number g such that $2 < g < N-1$ and $\gcd(g, N) = 1$.

S2. Choose three one-way collision-resistance hash functions H_1, H_2 and H_3 as follows:

$$H_1 : \{0,1\}^* \rightarrow \{0,1\}^{\rho},$$
$$H_2 : \{0,1\}^* \rightarrow \{0,1\}^{l_\sigma},$$
$$H_3 : \{0,1\}^* \rightarrow \{0,1\}^{l_m},$$

where l_σ is the length of a random string under the security parameter and l_m the length of plaintext message M.

S3. Compute the public parameters $D_{\mathbb{U}} = g^{d_{\mathbb{U}}}$, $Y = g^x$ and $R = g^k$, where $d_{\mathbb{U}} = \prod_{A_i \in \mathbb{U}} q_i$.

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

$$MSK = \{k, x, p, q, q_1, \cdots, q_n\},$$
$$MPK = \{N, D_{\mathbb{U}}, Y, R, H_1, H_2, H_3, p_1, \cdots, p_n\}.$$

B. ENCRYPT PHASE

Our encryption is based on the approach presented in [9], [24], [32] to achieve security against chosen-ciphertext attack:

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

where $E(\sigma_m, H_1(\mathbb{P}, M, \sigma_m)$ represents an attribute-based encryption on a random secret σ_m using the hash output $r_m = H_1(\mathbb{P}, M, \sigma_m)$ as the random number. More precisely, the random secret σ_m is encrypted with the key $g^{r_m d_{\mathbb{P}}}$, and the plaintext M is encrypted with random secret σ_m, and they are denoted by C_{σ_m} and C_m, respectively, in the ciphertext C. In addition, we compute the signature $S_m = H_1(\sigma_m, M)$ on the plaintext M using the random secret σ_m in order to verify the validity of the derived plaintext M. The other components of the ciphertext C are Y_m and R_m.

Our new 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 $C = \{Y_m, R_m, C_{\sigma_m}, C_m, S_m\}$ using the following steps:

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

E2. Compute K_m as

$$\begin{aligned} K_m &= D_{\mathbb{U}}^{r_m \frac{e_{\mathbb{U}}}{e_{\mathbb{P}}}} \\ &= \left(g^{d_{\mathbb{U}}}\right)^{r_m \frac{e_{\mathbb{U}}}{e_{\mathbb{P}}}} \\ &= g^{r_m d_{\mathbb{P}}}, \end{aligned}$$

where $d_{\mathbb{P}} = \prod_{A_i \in \mathbb{P}} q_i$, $e_{\mathbb{P}} = \prod_{A_i \in \mathbb{P}} p_i$ and $e_{\mathbb{U}} = \prod_{A_i \in \mathbb{U}} p_i$.

E3. Compute $Y_m = g^{x r_m}$, $R_m = g^{k r_m}$, $C_{\sigma_m} = H_2(K_m) \oplus \sigma_m$, $C_m = H_3(\sigma_m) \oplus M$, and $S_m = H_1(\sigma_m, M)$.

Finally, output the ciphertext C as $C = \{\mathbb{P}, Y_m, R_m, C_{\sigma_m}, C_m, S_m\}$.

C. 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 a user secret key k_u using the following steps:

K1. Compute $d_{\mathbb{A}} = \prod_{i=1}^{n} q_i^{a_i}$, where $a_i = 1$ if $A_i \in \mathbb{A}$ and $a_i = 0$ if $A_i \notin \mathbb{A}$.

K2. Pick two random numbers r_u and t_u, and compute s_u such that it satisfies the condition $d_{\mathbb{A}} = k s_u + r_u x \pmod{\phi(N)}$. Then, compute $k_1 = s_u + x t_u \pmod{\phi(N)}$ and $k_2 = r_u - k t_u \pmod{\phi(N)}$.

Finally, this algorithm outputs the user secret key k_u as $k_u = (k_1, k_2)$.

D. DECRYPT PHASE

This phase describes our decryption algorithm. The decryption algorithm takes the secret key $k_u = (k_1, k_2)$ corresponding to the attribute set $\mathbb{A}$ and ciphertext $C = \{\mathbb{P}, Y_m, R_m, C_{\sigma_m}, C_m, S_m\}$ corresponding to the access policy $\mathbb{P}$, and outputs the plaintext message M using the following steps:

D1. From Proposition 1, $\frac{e_{\mathbb{A}}}{e_{\mathbb{P}}}$ is an integer, if and only, if $\mathbb{P} \subseteq \mathbb{A}$. In this case, compute

$$\begin{aligned} K_m &= \left(Y_m^{k_2} R_m^{k_1}\right)^{\frac{e_{\mathbb{A}}}{e_{\mathbb{P}}}} \\ &= \left(g^{x r_m (r_u - k t_u)} g^{k r_m (s_u + x t_u)}\right)^{\frac{e_{\mathbb{A}}}{e_{\mathbb{P}}}} \\ &= \left(g^{r_m (x r_u + k s_u)} g^{x r_m (-k t_u) + k r_m (x t_u)}\right)^{\frac{e_{\mathbb{A}}}{e_{\mathbb{P}}}} \\ &= \left(g^{r_m d_{\mathbb{A}}}\right)^{\frac{e_{\mathbb{A}}}{e_{\mathbb{P}}}} \\ &= g^{r_m d_{\mathbb{P}}}. \end{aligned}$$

Otherwise, $\frac{e_{\mathbb{A}}}{e_{\mathbb{P}}}$ is not an integer; thus, computation of K_m is computationally infeasible.

D2. Compute $\sigma'_m = H_2(K_m) \oplus C_{\sigma_m}$ and $M' = C_m \oplus H_3(\sigma'_m)$.

D3. Checks whether the condition $S_m = H_1(\sigma'_m, M')$ holds or not. If it holds, output the plaintext message M; otherwise, output null $(\perp)$.

V. SECURITY ANALYSIS

In this section, we analyze the security of the proposed CP-ABE-CSKC scheme for different possible 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, attackers are not able to generate a new user secret key by combining their secret keys (see [27], [33]). In this paper, we follow the group generic model to prove that our scheme is secure against possible known attacks under the hardness assumption of factorization of RSA modulus $N = pq$ and hardness of solving computational Diffie-Hellman problem (CDHP) in Z_N, where p and q are large primes and $p \neq q$. We then prove that our scheme is secure against chosen-ciphertext attack under the selective security game.

Proposition 2: Let $c_i = a_i y + b_i z$, for $i = 1, 2, \cdots, l$, be a system of l linear equations in y and z, where $a_i = a_j$ and $b_i = b_j$ if and only if $i = j$. We define 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.*

Example 2: When $i = 2$, we have two linear equations $c_1 = a_1 y + b_1 z$ and $c_2 = a_2 y + b_2 z$ in the variables y and z. If the values a_1, a_2, b_1, and b_2 are known, these equations turn out to be a system of two linear equations with two unknowns y and z. In this case, the system is solvable and will have a unique solution. Otherwise, the system is still solvable, but it will have infinitely many solutions.

Theorem 1: Our scheme is secure against an adversary for deriving the system private key pair (k, x) by collision attack.

Proof: Assume that a group of users u^i, $i = 1, \cdots, l$, corresponding to 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 $k_{u^i} = (k_1^i, k_2^i)$, where

$$k_1^i = s_{u^i} + x \cdot t_{u^i} \pmod{\phi(N)}, \tag{1}$$

$$k_2^i = r_{u^i} - k \cdot t_{u^i} \pmod{\phi(N)}. \tag{2}$$

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

$$d_{\mathbb{A}^i} = k \cdot s_{u^i} + x \cdot r_{u^i} \pmod{\phi(N)}. \tag{3}$$

From Equation (3), it is clear that if s_{u^i} and r_{u^i} are known, it is solvable for k and x, and has a unique solution. Thus, the solution produces the original values of k and x. However, Equations (1) and (2) respectively form the system of l linear equations with $2l + 1$ unknowns. From Proposition 2, note that Equation (1) requires to randomly guess two unknowns (s_{u^i}, t_{u^i}) in order to solve x, and Equation (2) also requires to randomly guess two unknowns (r_{u^i}, t_{u^i}) to solve k. Hence, from the corrupted user secret keys k_{u^i}, $\forall i = 1, 2, \cdots, l$, the system's private key pair (k, x) is unknown, and as 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 $k_u = (k_1, k_2)$ corresponding to the attribute set $\mathbb{A}$.

Proof: From Theorem 1, it follows that computing the system private key pair (k, x) 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 $k_u = (k_1, k_2)$ 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 $d_{\mathbb{A}} = ks_u + r_u x \pmod{\phi(N)}$. However, to compute the value s_u, $\mathcal{A}$ requires the system private key pair (k, x) and RSA secret $d_{\mathbb{A}}$. Thus, generating the valid user secret key k_u is computationally infeasible problem by $\mathcal{A}$ due to the intractability of the Integer Factorization Problem (IFP) because it depends on the Euler's totient function $\phi(N) = (p - 1)(q - 1)$. □

Theorem 3: Under the hardness of solving the integer factorization problem, our scheme is secure against an adversary (also a legitimate user u) for deriving the key K_m from a ciphertext $C = \{\mathbb{P}, Y_m, R_m, C_{\sigma_m}, C_m, S_m\}$ corresponding to the attribute set $\mathbb{A}$ with $\mathbb{P} \not\subseteq \mathbb{A}$. Hence, it is computationally infeasible problem for the user u to decrypt the unauthorized ciphertexts.

Proof: Let $k_u = (k_1, k_2)$ be the secret key of a user u corresponding to the attribute set $\mathbb{A}$, and $C = \{\mathbb{P}, Y_m, R_m, C_{\sigma_m}, C_m, S_m\}$ be the ciphertext to decrypt, where $\mathbb{P} \not\subseteq \mathbb{A}$. The user u can compute $g^{r_m d_{\mathbb{A}}}$ as

$$\begin{aligned} Y_m^{k_2} R_m^{k_1} &= g^{xr_m(r_u - kt_u)} g^{kr_m(s_u + xt_u)} \\ &= g^{r_m(xr_u + ks_u)} g^{xr_m(-kt_u) + kr_m(xt_u)} \\ &= g^{r_m d_{\mathbb{A}}}. \end{aligned}$$

However, if $\mathbb{P} \not\subseteq \mathbb{A}$, from Proposition 1, it is computationally infeasible to compute K_m, where $K_m = \left(g^{r_m d_{\mathbb{A}}}\right)^{\frac{e_{\mathbb{A}}}{e_{\mathbb{P}}}}$ without solving the integer factorization problem. Thus, decrypting C is as hard as factoring the RSA modulus $N = pq$. Consequently, our scheme is secure against unauthorized decryption of ciphertexts. □

Remark 1: Note that if an attacker $\mathcal{A}$ (a legitimate user u) has the ability to compute the inverse q_i of p_i modulo $\phi(N)$ with the valid secret key k_u corresponding to the attribute set $\mathbb{A}$, he/she can derive the key K_m from any ciphertext C corresponding to the access policy $\mathbb{P}$ such that $\mathbb{P} \not\subseteq \mathbb{A}$ as follows. First, $\mathcal{A}$ can compute $g^{r_m d_{\mathbb{A}}}$ using his/her secret key k_u and the ciphertext $C = \{\mathbb{P}, Y_m, R_m, C_{\sigma_m}, C_m, S_m\}$. Then, $\mathcal{A}$ can compute K_m as

$$e_{\mathbb{P}}^{-1} \pmod{\phi(N)} \leftarrow \mathit{IFP}(N, e_{\mathbb{P}}),$$

$$K_m = \left(\left(g^{r_m d_{\mathbb{A}}}\right)^{e_{\mathbb{A}}}\right)^{e_{\mathbb{P}}^{-1}} = g^{r_m d_{\mathbb{P}}},$$

where $d_{\mathbb{P}} \pmod{\phi(N)} = e_{\mathbb{P}}^{-1} \pmod{\phi(N)}$.

Theorem 4: Under the hardness of solving CDHP (or IFP), our scheme is secure against deriving the key K_m corresponding to a ciphertext $C = \{\mathbb{P}, Y_m, R_m, C_{\sigma_m}, C_m, S_m\}$ by a group of collaborative unauthorized users u^i's corresponding to the attribute sets $\mathbb{A}^i$, $i = 1, \cdots, l$, where $\mathbb{P} \nsubseteq \mathbb{A}^i$.

Proof: We prove this theorem for two users and the same argument is then extended for a group of users. Suppose u_1 and u_2 be two users corresponding to the attribute sets $\mathbb{A}$ and $\mathbb{B}$, respectively, and try to decrypt the cipher $C = \{\mathbb{P}, Y_m, R_m, C_{\sigma_m}, C_m, S_m\}$, where $\mathbb{P} \nsubseteq \mathbb{A}$, $\mathbb{P} \nsubseteq \mathbb{B}$, and $\mathbb{P} \subseteq (\mathbb{A}$ OR $\mathbb{B}) = \mathbb{D}$. From Theorem 2, both u_1 and u_2 cannot succeed to derive the valid secret key k_u corresponding to the attribute policy $\mathbb{D}$ such that $\mathbb{P} \subseteq \mathbb{D}$. However, they derive $g^{r_m d_{\mathbb{A}}}$ and $g^{r_m d_{\mathbb{B}}}$ using their own secret keys k_{u_1} and k_{u_2}, respectively. Let $g_1 = g^{r_m} = \left(g^{r_m d_{\mathbb{A}}}\right)^{e_{\mathbb{A}}}$, and we then have $g_1^{d_{\mathbb{A}}} = g^{r_m d_{\mathbb{A}}}$ and $g_1^{d_{\mathbb{B}}} = g^{r_m d_{\mathbb{B}}}$. If $\mathcal{A}$ can solve the CDH problem, then he/she can compute the key K_m as follows:

$$g_1^{d_{\mathbb{A}} d_{\mathbb{B}}} \leftarrow CDHP(g_1, g_1^{d_{\mathbb{A}}}, g_1^{d_{\mathbb{B}}}),$$
$$K_m = \left(\left(g_1^{d_{\mathbb{A}} d_{\mathbb{B}}}\right)^{e_{\mathbb{C}}}\right)^{\frac{e_{\mathbb{D}}}{e_{\mathbb{P}}}},$$

where $\mathbb{C} = \mathbb{A}$ AND $\mathbb{B}$.

For example, assume $U = \{A_1, A_2, A_3, A_4\}$ is an attribute universe with four attributes A_1, A_2, A_3, A_4. Let $\mathbb{A} = 0110$, $\mathbb{B} = 1100$, and $\mathbb{P} = 1010$. Therefore, $\mathbb{D} = (\mathbb{A}$ OR $\mathbb{B}) = 1110$ and $\mathbb{C} = (\mathbb{A}$ AND $\mathbb{B}) = 0100$. Then, $\mathbb{P} \nsubseteq \mathbb{A}$, $\mathbb{P} \nsubseteq \mathbb{B}$, and $\mathbb{P} \subseteq \mathbb{D}$. The key K_m derivation is as follows:

$$g_1^{(q_2 q_3)(q_1 q_2)} \leftarrow CDHP(g_1, g_1^{q_2 q_3}, g_1^{q_1 q_2}),$$
$$K_m = \left(\left(g_1^{(q_2 q_3)(q_1 q_2)}\right)^{p_2}\right)^{\frac{p_1 p_2 p_3}{p_1 p_3}}$$
$$= \left(g_1^{(q_1 q_2 q_3)}\right)^{p_2} = g_1^{(q_1 q_3)} = g_1^{d_{\mathbb{P}}} = g^{r_m d_{\mathbb{P}}}.$$

Since solving the CDH problem in Z_N is as hard as solving factorization of RSA modulus $N = pq$, no collaborative user can derive the valid key K_m of C when $\mathbb{P} \nsubseteq \mathbb{A}$ and $\mathbb{P} \nsubseteq \mathbb{B}$ under the CDH assumption. □

Remark 2: In the defined attribute-based encryption, the components are computed as $C_{\sigma_m} = H_2(K_m) \oplus \sigma_m$, $C_m = H_3(\sigma_m) \oplus M$. The random secret σ_m is encrypted with the key $K_m = g^{r_m d_{\mathbb{P}}}$ and the plaintext M is encrypted with random secret σ_m. Thus, without the knowledge of valid user key, if an adversary derives the key K_m using the available public information $\{N, p_1, \cdots, p_n, g, g^k, g^x, g^{kr_m}, g^{xr_m}, g^{d_{\mathbb{P}}}\}$, then he/she can succeed in retrieving the plaintext M by computing the random secret σ_m. From the above analysis, we show that deriving the key K_m without the valid user key is computationally hard problem to the adversary. In Theorem 5, we show that the indistinguibility of chosen ciphertext under the hardness of solving the CDH problem in Z_N.

Remark 3: From the above discussion, it is clear that our scheme is secret-key collision resistance. Thus, computing the key K_m from any ciphertext C corresponding to the access policy $\mathbb{P}$ without the valid user secret key is as hard as the integer factorization (or computational Diffi-Hellman problem). Let $N = pq$ be the RSA modulus and $g \in Z_N$ such that $2 < g < N - 1$. Given $\{N, p_1, \cdots, p_n, g, g^k, g^x, g^{kr_m}, g^{xr_m}, g^{d_{\mathbb{P}}}\}$ and $T \in Z_N$, the n-IF-CDH problem reduces to deciding whether T is equal to $g^{r_m d_{\mathbb{P}}}$ or a random element in Z_N.

Theorem 5: Our CP-ABE-CSKC scheme is (t, q_e, q_c, ϵ) selectively secure if the n-IF-CDH problem is (t', ϵ')-hard, where $t' = t + \mathcal{O}(q_c t_c + q_e t_{inv} + q_{H_1} t_{exp})$, $\epsilon' = \frac{1}{q_c + q_{H_2}}\left(\epsilon - \frac{q_{H_1}}{N}\right)$, $n = |\mathbb{U}|$, t_c-time to respond for the decryption query, t_{inv} and t_e respectively represent the average time required for group inverse and exponentiation operations, q_{H_1} and q_{H_2} respectively denote the number of queries made to the random oracles H_1 and H_2, and $|\mathbb{U}|$ denotes the number of attributes in $\mathbb{U}$.

Proof: We follow the contradiction proof method as presented in [9], [24], [36] to prove that an algorithm $\mathcal{B}$ has an advantage more than $\frac{1}{q_c + q_{H_2}}\left(\epsilon - \frac{q_{H_1}}{N}\right)$ in solving the CDH problem.

The following three random oracles are used by an adversary:

- H_2 oracle: Let the query to this oracle be K_m. The response of the query $H_2(K_m)$ is a random number $R_i \in \{0, 1\}^{l_{\sigma_m}}$.
- H_3 oracle: Let the query to this oracle be t_i. The response of the query $H_3(t_i)$ is a random number $Q_i \in \{0, 1\}^{l_m}$.
- H_1 oracle: Let the query to this oracle be $(\mathbb{P}_i, M_i, t_i)$. The query to $H_1(\mathbb{P}_i, M_i, t_i)$ responds with a random number $r_i \in \{0, 1\}^{\rho}$.

Then, the adversary queries for the secret keys and the query responds with the valid secret keys (user secret keys). 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. Assume that no query will be aborted since all valid encryptions need the response from hash oracles, and the response contains the random number r_i used in encryption.

Next, the adversary outputs two messages (M_0, M_1) for the challenge, and then the challenge query replies with the following ciphertext $C_{c'}$ corresponding to the challenged access policy $\mathbb{P}'$ such that no queried secret keys satisfy $\mathbb{P}'$:

- Choose $R' \in \{0, 1\}^{l_{\sigma_m}}$, $Q' \in \{0, 1\}^{l_m}$, and $S' \in \{0, 1\}^{\rho}$.
- Choose a random number $r'_m \in \{0, 1\}^{\rho}$.
- Compute the challenge ciphertext $C_{c'} = \{\mathbb{P}', Y'_m, R'_m, C'_{\sigma_m}, C'_m, S'_m\}$, where $Y'_m = g^{xr'_m}$, $R'_m = g^{kr'_m}$, $C'_{\sigma_m} = R'$, $C'_m = Q'$, and $S'_m = S'$ which is a valid encryption of access policy $\mathbb{P}'$.

In this case, the challenged ciphertext $C_{c'}$ is indistinguishable with a real ciphertext. The adversary outputs a guess c'_g of c' and wins the game if $c'_g = c'$. Otherwise, $T = g^{r'_m d_{\mathbb{P}}}$ is a random group element.

The advantage of algorithm $\mathcal{B}$ in solving the CDH problem in the RSA group Z_N is denoted by $Adv^{CDHP}_{Z_N, \mathcal{B}}$. Suppose $Pr[Abort]$ denotes the probability that $\mathcal{B}$ aborts. Then, we have $Pr[Abort] \leq q_{H_1}/N$. If $\mathcal{B}$ does not abort, the adversary $\mathcal{A}$'s view is identical to its view in the real attack. Thus, we have

$$|Pr[c'_g = c'] - Pr[c'_g \neq c']| \geq \epsilon - \frac{q_{H_1}}{N}.$$

Let S be an event that the adversary $\mathcal{A}$ queries the oracle H_2 at an element $T = g^{r'_m d_{\mathbb{P}}} \in Z_N$. Then, we have

$$Pr[S] \geq |Pr[c'_g = c'] - Pr[c'_g \neq c']|.$$

From Theorem 4, $\mathcal{B}$ knows the private keys, which do not satisfy the challenge ciphertext $C_{c'}$. Then, $g^{r_m d_{\mathbb{P}}}$ can be computed only if the CDH problem can be solved in the RSA group Z_N. When $\mathcal{B}$ chooses randomly a tuple in the H_2 query list, the probability that the chosen tuple is equal to $g^{r_m d_{\mathbb{P}}}$ is given by $\frac{1}{q_c+q_{H_2}} Pr[S]$. Thus, we have

$$Adv^{CDHP}_{Z_N,\mathcal{B}} = \frac{1}{q_c + q_{H_2}} Pr[S] \geq \frac{1}{q_c + q_{H_2}} \left(\epsilon - \frac{q_{H_1}}{N}\right).$$

The computation of each secret key requires $\mathcal{O}(1)$ group inverse operations and each decryption requires $\mathcal{O}(1)$ group exponentiation operations. According to $\mathcal{B}$, time to solve the CDH problem in Z_N is $t' = t + \mathcal{O}(q_c t_c + q_e t_{inv} + q_{H_1} t_{exp})$. From the above result, we see that it is contradictive with

$$\epsilon' = Adv^{CDHP}_{Z_N,\mathcal{B}} = \frac{1}{q_c + q_{H_2}} \left(\epsilon - \frac{q_{H_1}}{N}\right).$$

Hence, the theorem is proved. □

VI. PERFORMANCE COMPARISON

Both ZZCLL [4] and our scheme require only $\mathcal{O}(1)$ time complexity for each encryption and decryption (see Table 3). However, from Table 1, it is clear that the ZZCLL scheme [4] does not provide constant size secret keys for the users, which is an essential security requirement for mobile device deployment. On the other hand, the EMNOS scheme [21] offers constant size ciphertexts and secret keys. However, it provides only (n, n)-threshold and incurs significant computational cost for encryption. The GSWV scheme [24] is efficient for shorter secret keys, but it fails to provide constant size ciphertexts or efficient encryption and decryption with $\mathcal{O}(1)$ time-complexity.

TABLE 3. Computational costs comparison.

Scheme	Encryption	Decryption
EMNOS [21]	$(n+1)T_G + 2T_{G_t}$	$2T_{G_t} + 2T_e$
ZZCLL [4]	$3T_G$	$2T_e$
ZH [22]	$2T_G$	$(2\lvert\mathbb{P}\rvert + 1)T_e$
GSWV [24]	$(2(n - \lvert\mathbb{P}\rvert) + 2)T_G$	$2(\lvert\mathbb{A}\rvert - \lvert\mathbb{P}\rvert)T_G + 1T_{G_t} + 3T_e$
Ours	$3T_{Z_N}$	$3T_{Z_N}$

Also demonstrated in Table 1, our scheme is the only scheme to provide both constant size secret keys and ciphertexts with expressive access structure, and efficient encryption and decryption with $\mathcal{O}(1)$ time-complexity without using bilinear maps.

Following the approach in [25], we will now evaluate the performance using experiments. The execution timings for various operations using MIRACL [37] and PBC [38] libraries are listed in Table 4. The experiment is conducted for the group G over the FST curve. Note that one point multiplication operation T_G in G requires 1.1 ms and the corresponding paring operation T_e requires 3.1 ms, whereas one 1024-bit RSA decryption and encryption operations require 3.88 ms and 0.02 ms, respectively. Also, one field exponentiation operation T_{Z_N} in Z_N^* ($|N| = 1024$) requires 0.64 ms. Since the computation cost required for hashing operation and AES encryption/decryption operation are negligible [25], [39], we omit these operations in our performance comparison.

TABLE 4. Execution timings for various operations used in the experiment.

Parameter	Value
T_G	$1.10\ ms$
T_{G_t}	$0.64\ ms$
T_{Z_N}	$0.64\ ms$
T_e	$3.10\ ms$

For the experiments, let the total number of attributes in the system be $n = 1000$. We also assume that $|\mathbb{P}| = 500$ and $|\mathbb{A}| = 600$. The parameters used in the experiment are shown in Table 5.

TABLE 5. Parameters used in the experiment.

Parameter	Value
n	1000
$\lvert\mathbb{P}\rvert$	500
$\lvert\mathbb{A}\rvert$	600

TABLE 6. Computational costs from the experiments: A comparative summary.

Scheme	Encryption (ms)	Decryption (ms)
EMNOS [21]	1102.38	7.48
ZZCLL [4]	3.30	6.20
ZH [22]	2.20	3103.10
GSWV [24]	1102.20	229.94
Ours	1.92	1.92

Table 6 lists the comparison of experimental computational costs among our scheme and other related schemes. We observe that encryption and decryption for EMNOS [21] require 1102.38 ms and 7.48 ms, respectively. ZZCLL [4], ZH [22] and GSWV [24] require 3.30 ms and 6.20 ms, 2.20 ms and 3103.10 ms, 1102.20 ms and 229.94 ms for encryption and decryption, respectively. On the other hand, our scheme needs only 1.92 ms and 1.92 ms for encryption and decryption, respectively. Thus, it clear that our scheme requires minimal computational costs for both encryption and decryption, compared to the other related CP-ABE schemes in Table 6.

VII. CONCLUDING REMARKS

In the current Internet-connected society, battery-limited mobile devices are likely to be more prevalent. For example, an Internet-of-Things (IoT) or Cloud-of-Things (CoT) environment generally consists of battery-limited devices such as Radio-Frequency Identification (RFID) tags, sensors, actuators, mobile devices, and wearable devices. Hence, IoT (or CoT) security [40], [41], forensics [42], [43] and privacy [44] are topics of current interest. Due to the nature (e.g. heterogeneous) and level of interactivity between IoT or CoT devices, the design of any security solution needs to take into consideration efficiency and lightweight requirements [2], [3]. Although CP-ABE is one efficient and viable method that can be widely applied to realize access control in a wide range of applications, such as in medical systems and education systems [45]–[48], it may not be naively deployed in an IoT and CoT environment due to its complexity and high overhead.

The scheme presented in this paper, however, is suited for IoT and CoT deployments. Our RSA-based CP-ABE-CSKC scheme offers constant size secret keys and constant size ciphertexts with an expressive AND gate access structure without using bilinear maps. To the best of our knowledge, this is the first such scheme. We demonstrated that the scheme provides an efficient solution to both encryption and decryption with $\mathcal{O}(1)$ time-complexity. We also proved that our scheme is secure against possible known attacks, such as key recovery and collision attacks, as well as under the chosen-ciphertext adversary.

REFERENCES

[1] S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya, "Cloud-based augmentation for mobile devices: Motivation, taxonomies, and open challenges," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 337–368, 1st Quart., 2014.

[2] Y. Yang, H. Cai, Z. Wei, H. Lu, and K.-K. R. Choo, "Towards lightweight anonymous entity authentication for IoT applications," in *Proc. Austral. Conf. Inf. Secur. Privacy*, 2016, pp. 265–280.

[3] Y. Yang, J. Lu, K.-K. R. Choo, and J. K. Liu, "On lightweight security enforcement in cyber-physical systems," in *Proc. Int. Workshop Lightweight Cryptogr. Secur. Privacy*, 2015, pp. 97–112.

[4] Y. Zhang, D. Zheng, X. Chen, J. Li, and H. Li, "Computationally efficient ciphertext-policy attribute-based encryption with constant-size ciphertexts," in *Provable Security*. Hong Kong, China: Springer, 2014, pp. 259–273.

[5] J. K. Liu, M. H. Au, W. Susilo, K. Liang, R. Lu, and B. Srinivasan, "Secure sharing and searching for real-time video data in mobile cloud," *IEEE Netw.*, vol. 29, no. 2, pp. 46–50, Mar./Apr. 2015.

[6] M. Ambrosin, C. Busold, M. Conti, A.-R. Sadeghi, and M. Schunter, "Updaticator: Updating billions of devices by an efficient, scalable and secure software update distribution over untrusted cache-enabled networks," in *Computer Security—ESORICS*. Wroclaw, Poland: Springer, 2014, pp. 76–93.

[7] Y. Yang, H. Zhu, H. Lu, J. Weng, Y. Zhang, and K.-K. R. Choo, "Cloud based data sharing with fine-grained proxy re-encryption," *Pervas. Mobile Comput.*, vol. 28, pp. 122–134, Jun. 2016.

[8] Y. Yang, J. K. Liu, K. Liang, K.-K. R. Choo, and J. Zhou, "Extended proxy-assisted approach: Achieving revocable fine-grained encryption of cloud data," in *Proc. Eur. Symp. Res. Comput. Secur.*, 2015, pp. 146–166.

[9] M. Zheng, Y. Xiang, and H. Zhou, "A strong provably secure IBE scheme without bilinear map," *J. Comput. Syst. Sci.*, vol. 81, no. 1, pp. 125–131, 2015.

[10] C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys," in *Advances in Cryptology—ASIACRYPT*. Kuching, Malaysia: Springer, 2007, pp. 200–215.

[11] F. Guo, Y. Mu, and W. Susilo, "Identity-based traitor tracing with short private key and short ciphertext," in *Computer Security—ESORICS*. Kuching, Malaysia: Springer, 2012, pp. 609–626.

[12] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology—EUROCRYPT*. Pisa, Italy: Springer, 2005, pp. 457–473.

[13] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS)*, 2006, pp. 89–98.

[14] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS)*, 2007, pp. 195–203.

[15] N. Attrapadung, B. Libert, and E. de Panafieu, "Expressive key-policy attribute-based encryption with constant-size ciphertexts," in *Public Key Cryptography—PKC*. Taormina, Italy: Springer, 2011, pp. 90–108.

[16] J. Herranz, F. Laguillaumie, and C. Ràfols, "Constant size ciphertexts in threshold attribute-based encryption," in *Public Key Cryptography—PKC*. Paris, France: Springer, 2010, pp. 19–34.

[17] C. Chen *et al.*, "Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures," in *Topics in Cryptology—CT-RSA*. San Francisco, CA, USA: Springer, 2013, pp. 50–67.

[18] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Advances in Cryptology—EUROCRYPT*. French Riviera: Springer, 2010, pp. 62–91.

[19] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Public Key Cryptography—PKC*. Taormina, Italy: Springer, 2011, pp. 53–70.

[20] A. Lewko and B. Waters, "New proof methods for attribute-based encryption: Achieving full security through selective techniques," in *Advances in Cryptology—CRYPTO*. Santa Barbara, CA, USA: Springer, 2012, pp. 180–198.

[21] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," in *Information Security Practice and Experience*. XiŠan, China: Springer, 2009, pp. 13–23.

[22] Z. Zhou and D. Huang, "On efficient ciphertext-policy attribute based encryption and broadcast encryption: Extended abstract," in *Proc. 17th ACM Conf. Comput. Commun. Secur.*, 2010, pp. 753–755.

[23] N. Doshi and D. C. Jinwala, "Fully secure ciphertext policy attribute-based encryption with constant length ciphertext and faster decryption," *Secur. Commun. Netw.*, vol. 7, no. 11, pp. 1988–2002, 2014.

[24] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan, "CP-ABE with constant-size keys for lightweight devices," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 763–771, May 2014.

[25] H. Li, X. Lin, H. Yang, X. Liang, R. Lu, and X. Shen, "EPPDR: An efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 8, pp. 2053–2064, Aug. 2014.

[26] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2007, pp. 321–334.

[27] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS)*, 2007, pp. 456–465.

[28] D. Hofheinz and E. Kiltz, "Practical chosen ciphertext secure encryption from factoring," in *Advances in Cryptology—EUROCRYPT*. Tokyo, Japan: Springer, 2009, pp. 313–332.

[29] K. S. McCurley, "A key distribution system equivalent to factoring," *J. Cryptol.*, vol. 1, no. 2, pp. 95–105, 1988.

[30] L. Harn and H.-Y. Lin, "A cryptographic key generation scheme for multilevel data security," *Comput. Security*, vol. 9, no. 6, pp. 539–546, Oct. 1990.

[31] S. G. Akl and P. D. Taylor, "Cryptographic solution to a problem of access control in a hierarchy," *ACM Trans. Comput. Syst.*, vol. 1, no. 3, pp. 239–248, 1983.

[32] E. Fujisaki and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes," *J. Cryptol.*, vol. 26, no. 1, pp. 80–101, 2013.

[33] K. Emura, A. Miyaji, K. Omote, and A. Nomura, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," *Int. J. Appl. Cryptogr.*, vol. 2, no. 1, pp. 46–59, 2010.

[34] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 469–472, Jul. 1985.

[35] L. Harn and Y. Xu, "Design of generalised ElGamal type digital signature schemes based on discrete logarithm," *Electron. Lett.*, vol. 30, no. 24, pp. 2025–2026, 1994.

[36] J. Li, Q. Wang, C. Wang, and K. Ren, "Enhancing attribute-based encryption with attribute hierarchy," *Mobile Netw. Appl.*, vol. 16, no. 5, pp. 553–561, 2011.

[37] *Miracl Crypto*, accessed on Jan. 2017. [Online]. Available: https://certivox.com/solutions/miracl-crypto-sdk/

[38] B. Lynn. *PBC Library*, accessed on Jan. 2017. [Online]. Available: http://crypto.stanford.edu/pbc/
[39] W. Dai. (2009). *Crypto++ 5.6.0 Benchmarks*. [Online]. Available: http://www.cryptopp.com/benchmarks.html
[40] C. J. Dorazio, K.-K. R. Choo, and L. T. Yang, "Data exfiltration from Internet of Things devices: iOS devices as case studies," *IEEE Internet Things J.*, to be published.
[41] B. Do, Q. Martini, and K.-K. R. Choo, "Is the data on your wearable device secure? An Android Wear smartwatch case study," *Softw., Pract. Exper.*, vol. 47, no. 4, pp. 391–403, 2017.
[42] N. H. Ab Rahman, W. B. Glisson, Y. Yang, and K.-K. R. Choo, "Forensic-by-design framework for cyber-physical cloud systems," *IEEE Cloud Comput.*, vol. 3, no. 1, pp. 50–59, Jan./Feb. 2016.
[43] N. D. W. Cahyani, B. Martini, K.-K. R. Choo, and M. H. Al-Azhar, "Forensic data acquisition from cloud-of-things devices: Windows smartphones as a case study," *Concurrency Comput., Pract. Exper.*, to be published.
[44] B. Li, R. Lu, W. Wang, and K.-K. R. Choo, "DDOA: A Dirichlet-based detection scheme for opportunistic attacks in smart grid cyber-physical system," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2415–2425, Nov. 2016.
[45] X. Wang, J. Zhang, E. M. Schooler, and M. Ion, "Performance evaluation of attribute-based encryption: Toward data privacy in the IoT," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 725–730.
[46] M. Zhang, Y. Zhang, Y. Su, Q. Huang, and Y. Mu, "Attribute-based hash proof system under learning-with-errors assumption in obfuscator-free and leakage-resilient environments," *IEEE Syst. J.*, to be published, doi: 10.1109/JSYST.2015.2435518.
[47] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, and G. Marrocco, "RFID technology for IoT-based personal healthcare in smart spaces," *IEEE Internet Things J.*, vol. 1, no. 2, pp. 144–152, Apr. 2014.
[48] L. Touati, Y. Challal, and A. Bouabdallah, "C-CP-ABE: Cooperative ciphertext policy attribute-based encryption for the Internet of Things," in *Proc. Int. Conf. Adv. Netw. Distrib. Syst. Appl. (INDS)*, 2014, pp. 64–69.
[49] J. Li, X. Li, L. Wang, D. He, H. Ahmad, and X. Niu, "Fuzzy encryption in cloud computation: Efficient verifiable outsourced attribute-based encryption," *Soft Comput.*, pp. 1–8, Jan. 2017, doi: 10.1007/s00500-017-2482-1.

VANGA ODELU received the M.Tech. and Ph.D. degrees in computer science and data processing from IIT Kharagpur, India. He is currently an Assistant Professor with the Department of Computer Science and Engineering, Indian Institute of Information Technology at Sri City, Sri City, India. His research interests include cryptography, network security, hierarchical access control, remote user authentication, security in cloud computing, and smart grid. He has authored over 30 papers in international journals and conferences in the above areas. He is a member of the ACM.

ASHOK KUMAR DAS received the M.Sc. degree in mathematics, the M.Tech. degree in computer science and data processing, and the Ph.D. degree in computer science and engineering from IIT Kharagpur, Kharagpur, India. He is currently an Assistant Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology at Hyderabad, Hyderabad, India. His current research interests include cryptography, wireless sensor network security, hierarchical access control, data mining, security in vehicular ad hoc networks, smart grid and cloud computing, and remote user authentication. He has authored over 125 papers in international journals and conferences in the above areas. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He is in the Editorial Board of the *KSII Transactions on Internet and Information Systems*, and the *International Journal of Internet Technology and Secured Transactions* (Inderscience), and a Guest Editor of the *Computers & Electrical Engineering* (Elsevier) for the Special Issue on Big data and Internet of Things in e-healthcare, and has served as a Program Committee Member in many international conferences.

MUHAMMAD KHURRAM KHAN (SM'12) is currently working as a Full Professor with the Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia. He is one of the founding members of CoEIA and has served as the Manager Research and Development from 2009 to 2012. He is an Adjunct Professor with the Fujian University of Technology, China, and an Honorary Professor with IIIRC, Shenzhen Graduate School, Harbin Institute of Technology, China. He developed and successfully managed the research program of CoEIA, which transformed the center as one of the best centers of research excellence in Saudi Arabia as well as in the region. He has authored over 280 research papers in the journals and conferences of international repute. He holds ten US/PCT patents. He has edited seven books/proceedings published by the Springer-Verlag and the IEEE. He has secured several national and international research grants in the domain of information security. His research areas of interest are cybersecurity, digital authentication, biometrics, multimedia security, and technological innovation management.

Prof. Khurram is a fellow of the IET, U.K., a fellow of the BCS, U.K., a fellow of the FTRA, South Korea, a member of the IEEE Technical Committee on Security & Privacy, and a member of the IEEE Cybersecurity community. He was a recipient of the King Saud University Award for Scientific Excellence (Research Productivity) in 2015, the King Saud University Award for Scientific Excellence (Inventions, Innovations, and Technology Licensing) in 2016. He has secured an outstanding leadership award at the IEEE international conference on Networks and Systems Security 2009, Australia. He has been included in the Marquis Who's Who in the World 2010 edition. Besides, he has received certificate of appreciation for outstanding contributions in biometrics & information security research with the AIT international Conference, Japan, 2010. He received the Gold Medal for the Best Invention & Innovation Award at 10th Malaysian Technology Expo in 2011, Malaysia, the Bronze Medal at 41st International Exhibition of Inventions, Geneva, Switzerland, in 2013, for his invention, and the best paper award from the *Journal of Network & Computer Applications* (Elsevier) in 2015. He is one of the organizing chairs of over five dozen international conferences and a member of technical committees of over ten dozen international conferences. He has recently played a leading role in developing BS Cybersecurity Degree Program and Higher Diploma in Cybersecurity with King Saud University. He has been the Editor-in-Chief of a well-esteemed ISI-indexed international journal *Telecommunication Systems* (Springer-Verlag, since 1993) with an impact factor of 1.163 (JCR 2013). Furthermore, he is the full-time Editor/Associate Editor of several ISI-indexed international journals/magazines, including the *IEEE Communications Magazine*, the Journal of Network and Computer Applications (Elsevier), the IEEE Access Journal, the *Security and Communication Networks* (Wiley), the *IEEE Consumer Electronics Magazine*, the *PLOS ONE* (USA), the *IET Wireless Sensor Systems, Electronic Commerce Research* (Springer), the *Journal of Information Hiding and Multimedia Signal Processing*, the *International Journal of Biometrics* (Inderscience), the *Journal of Physical & Information Sciences*, and the *Journal of Independent Studies and Research-Computing*. He has also played role of the Guest Editor of several international ISI-indexed journals of Springer-Verlag and Elsevier Science. He is an Active Reviewer of many international journals.

KIM-KWANG RAYMOND CHOO (SM'15) received the Ph.D. in information security from the Queensland University of Technology, Australia, in 2006. He current holds the Cloud Technology Endowed Professorship with The University of Texas at San Antonio. He serves on the Editorial Board of the *Cluster Computing*, the *Digital Investigation*, the IEEE Cloud Computing, the *Future Generation Computer Systems*, the *Journal of Network and Computer Applications*, and the *PLoS ONE*, the Special Issue Guest Editor of the *ACM Transactions on Embedded Computing Systems* (2017; DOI: 10.1145/3015662), the *ACM Transactions on Internet Technology* (2016; DOI: 10.1145/3013520), the *Digital Investigation* (2016; DOI: 10.1016/j.diin.2016.08.003), the *Future Generation Computer Systems* (2016; DOI: 10.1016/j.future.2016.04.017), the IEEE Cloud (2015; DOI: 10.1109/MCC.2015.84), the IEEE Network (2016; DOI: 10.1109/MNET.2016.7764272), the *Journal of Computer and System Sciences* (2017; DOI: 10.1016/j.jcss.2016.09.001), the *Multimedia Tools and Applications* (2017; DOI: 10.1007/s11042-016-4081-z), and the *Pervasive and Mobile Computing* (2016; DOI: 10.1016/j.pmcj.2016.10.003). He was a recipient of various awards, including ESORICS 2015 Best Paper Award, Winning Team of the Germanys University of Erlangen-Nuremberg (FAU) Digital Forensics Research Challenge in 2015, the 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, the Fulbright Scholarship in 2009, the 2008 Australia Day Achievement Medallion, and the British Computer Societys Wilkes Award in 2008. He is also a fellow of the Australian Computer Society

MINHO JO (M'07–SM'16) received the B.A. degree from the Department of Industrial Engineering, Chosun University, South Korea, in 1984, and the Ph.D. degree from the Department of Industrial and Systems Engineering, Lehigh University, USA, in 1994. He is currently a Professor with the Department of Computer and Information Science, South Korea University, Sejong, South Korea. He is one of founders of Samsung Electronics LCD Division. Areas of his current interests include LTE-Unlicensed, cognitive radio, Internet of Things, HetNets in 5G, green (energyefficient) wireless communications, mobile cloud computing, network function virtualization, 5G wireless communications, optimization and probability in networks, network security, and massive MIMO. He received the Headong Outstanding Scholar Prize in 2011. He is currently an Editor of IEEE Wireless Communications, an Associate Editor of the IEEE Access, and an Associate Editor of the IEEE Internet of Things Journal, respectively. And he is currently an Associate Editor of the *Security and Communication Networks*, and an the *Wireless Communications and Mobile Computing*. He is the Founder and the Editor-in-Chief of the *KSII Transactions on Internet and Information Systems* (SCI and SCOPUS indexed). He is currently the Vice-President of Korea Society for Internet Informations and was the Vice-President of the Institute of Electronics and of the Korea Information Processing Society, respectively. His current research interests include LTE-unlicensed, cognitive radio, IoT, deep learning AI and big data in IoT, HetNets in 5G, green (energy-efficient) wireless communications, mobile cloud computing, wireless energy hatvesting, 5G wireless communications, optimization and probability in networks, network security, and massive MIMO.