IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON EMERGING TECHNOLOGIES FOR DEVICE TO DEVICE COMMUNICATIONS

Received September 4, 2018, accepted September 29, 2018, date of publication October 5, 2018, date of current version October 31, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2874066

Robust and Scalable Data Access Control in D2D Communications

QI LI[1,2], LIZHI HUANG[1], RUO MO[3], HAIPING HUANG[1,2], AND HONGBO ZHU[4]

[1]School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
[2]Jiangsu Key laboratory of Big Data Security & Intelligent Processing, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
[3]School of Cyber Engineering, Xidian University, Xi'an 710071, China
[4]Jiangsu Key Laboratory of Wireless Communications, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

Corresponding author: Haiping Huang (hhp@njupt.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61502248, Grant 61672297, and Grant 61427801, in part by the China Postdoctoral Science Foundation under Grant 2018M632350, and in part by the Natural Science Foundation of Jiangsu Province under Grant BK20181394.

ABSTRACT As an emerging technique in 5G cellular networks, D2D communication efficiently utilizes the available resources. However, the concerns of data security, identity privacy, and system scalability have not been sufficiently addressed. In this paper, we propose a robust and scalable data access control scheme (RSDAC) in D2D communication, where the key build block is a multi-authority ciphertext-policy attribute-based encryption (MA-CP-ABE) with the large universe and verifiable outsourced decryption. In RSDAC, the system attribute universe is scalable, which is exponentially large without resource waste. Each base station (BS) governs the whole attribute universe individually. The data owner can define any monotonic access structure to encrypt its data. During the key generation phase, each BS can independently verify the user's legitimacy and then generate an intermediate key for the legal user according to its attribute set. A core network server (CNS) acts as the central authority which will generate the final private key for the user basing on his intermediate key. We also design an efficient method to offload the complicated decryption to some devices with adequate computation resource and further check the correctness of decryption result. The security analysis and performance comparison indicate that our scheme is secure, efficient, and applicable.

INDEX TERMS D2D, access control, CP-ABE, multi-authority, large universe, efficient decryption.

I. INTRODUCTION

In recent years, device to device (D2D) communication has emerged as a promising technique to efficiently utilize the spectral resources in 5G cellular networks [1], [2], because of its inherent features, e.g., improving spectral efficiency, delay constrained, improving system capacity, etc. D2D communication enables the user equipments (UEs) to directly communicate with each other without being involved in the fixed network infrastructures, such as bluetooth, base stations (BSs) and access points (APs). By using D2D communication techniques, people can efficiently and rapidly share their data via various UEs. However, despite the above advantages, there are three main issues: **data security**, **identity privacy** and **system scalability** to be addressed before applying D2D communication in practice.

A. DATA SECURITY

As the UE connects with others directly, D2D communication might be vulnerable to many security attacks, such as channel eavesdropping and modification of data [3]. To resist suck attacks, a feasible way is to encrypt the data before transmitting it to others. The data owner should also indicate who is allowed to access the encrypted data. Meanwhile, the data should be accessed only by the authorized users and is confidential to the unauthorized users. However, traditional symmetric encryption and public key cryptology are not suitable for D2D communication applications, due to the complexity of key agreement and management.

B. IDENTITY PRIVACY

During sharing the data with some users, the data owner may want to hide his or the UE's identification information. For instance, a data owner shoots a scandal video by his mobile phone and transmits it to someone else, but he do not want to expose any information of himself and his device. If the identity privacy can not be guaranteed, it may result in inferior user experience of D2D communication.

C. SYSTEM SCALABILITY

While deploying D2D communication in real applications, the scalability of system is worth considering, due to that plenty of users and UEs are coexisting in the system. Once the system parameter size is set too small, the system may be thoroughly reconstructed in future. If the system parameter size is set too large, it would incur superfluous waste of resource.

To address the issues mentioned above, in this paper, we present a robust and scalable data access control scheme (RSDAC) for D2D communication. We construct a multi-authority ciphertext-policy attribute-based encryption (MA-CP-ABE) scheme with large universe and verifiable outsourced decryption, and take it as the basis of the data access control scheme for D2D communication. In RSDAC, there are multiple base stations (BSs) and a core network server (CNS). Each D2D user equipment (DUE) can link to a BS directly or via the relay of a cellular user equipment (CUE), and is described by some attributes, such as spectrum, brand and trust level. Aiming to improve the efficiency of data encryption, we use key encapsulation mechanism (KEM) to encrypt original data. That is, the original data is first encrypted by a chosen symmetric key (SEK), then SEK is encrypted under a chosen access structure associated with attributes. Only the DUE whose attributes match the access structure can recover SEK and further decrypt the encrypted data. Different from most existing MA-CP-ABE schemes [4]–[7], each BS in our RSDAC manages the whole attribute universe, handles the DUE legitimacy verification and generates the intermediate key for legal DUE according to its attribute set. The CNS is in charge of the registration of BSs and DUEs, and generates the private key for each DUE basing on its intermediate key. In summary, we make the following contributions:

1. To solve the issue of single-point bottleneck, the DUE legitimacy verification is separated from the private key generation. Every BS could independently verify the legitimacy of a DUE. We use an additional randomly chosen parameter to remove the restriction in [8] where the timestamp numbers should be different and not been used before.

2. RSDAC supports exponentially large attribute universe and constant size of system public parameters. We design a method to alleviate the user decryption cost by outsourcing the most complicated decryption operations to a third party (such as the DUE with sufficient computation resource). The correctness of returned partial decryption ciphertext from the third party can also be efficiently checked.

3. RSDAC supports any monotonic access structure. The security analysis and performance results demonstrate that RSDAC is secure, efficient and applicable.

II. RELATED WORK

A. DATA ACCESS CONTROL IN D2D COMMUNICATIONS

Most extensive works [9]–[13] focused on interference management and resource allocation. Aiming to realize confidentiality and integrity for D2D communication in LTE-Advanced, Zhang *et al*. [3] presented a data sharing protocol by using signature and public key technique. However, the content providing server which administrates the register of all the devices might be a security and performance bottleneck of the system. Kwon *et al*. [14] showed that how to adopt ciphertext-policy ABE (CP-ABE) to design a D2D authentication protocol, where a group manager should be available. Huang *et al*. [15] and Yue *et al*. [16] investigated the fine-grained access control in cellular communication networks, where the connection between only UEs was not considered. Yan *et al*. [17] realized flexible data access control among lots of devices in D2D communication by employing ABE, where the attributes are described by two-dimensional trust levels. However, their scheme can not support multiple authorities and the decryption cost is linear with the scale of involved attributes.

B. ATTRIBUTE-BASED ENCRYPTION AND ITS APPLICATIONS

Various approaches [18]–[21] have been employed to preserve user privacy and data security in practice. As one of the most promising cryptographic techniques, ABE has been regarded as an important building block to design fine-grained access control systems.

ABE was first introduced in [22] and further classified to two types: key-policy ABE (KP-ABE) [23]–[25] and CP-ABE [26]–[30]. Different from CP-ABE, KP-ABE associates the ciphertext with attributes and the private key with the access structure. In [31], Yu *et al*. first adopted ABE to design fine-grained access control scheme for cloud computing. Since then, various data access control schemes based on ABE have been introduced.

Aiming to resolve the problem of single-point bottleneck, Xue *et al*. [8] proposed a new MA-ABE mechanism where the operation of user legitimacy verification is moved to the attribute authorities (AAs), and every AA can execute the user legitimacy verification by itself and generate intermediate key over the whole attribute universe. The randomness of private keys and collusion resistance rely on the difference of timestamp at that moment. To ensure the timestamp numbers are unique, the CA has to check the timestamp numbers are in the pre-defined time interval. Such method may bring additional computation cost for CA and the delay of key generation.

The large universe problem was first addressed in [22]. On composite order groups, Lewko *et al*. [32] introduced the first exponentially large universe KP-ABE scheme, whereafter Rouselakis *et al*. [33] demonstrated how to construct large universe ABE on prime order groups.

To realize efficient user decryption in ABE, Green *et al*. [34] introduced a decryption outsourcing method to offload most decryption operation to a third-party, which then returns a partial decryption ciphertext (PDC). Only one time of exponential operation on PDC is required by the user to recover the plaintext. However, the correctness of PDC

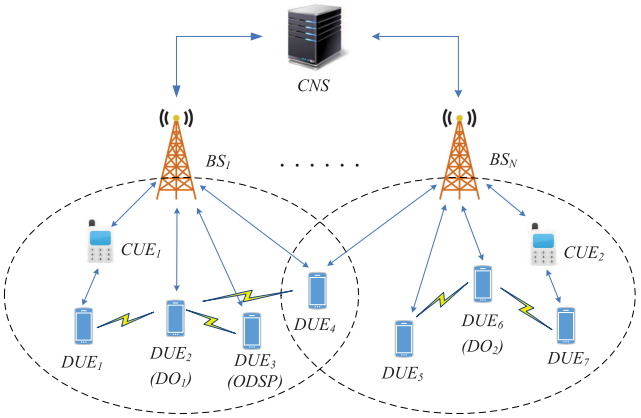


FIGURE 1. System Model.

can not be guaranteed. Lai *et al*. [35] designed a verification method to check the correctness of PDC. The ciphertext length and the encryption cost are almost twice of that in [34]. Ning *et al*. [36] presented an auditable CP-ABE scheme without adding any extra encryption overhead or ciphertext element, where the PDC is verified by taking in the system master secret key.

III. SYSTEM MODEL, ADVERSARY MODEL AND SECURITY REQUIREMENTS

A. SYSTEM MODEL

Fig. 1 describes the system model of RSDAC, which consists of four entities: core network server (CNS), base stations (BSs), cellular UEs (CUEs) and D2D UEs (DUEs). In RSDAC, the DUE can connect to the BS which covers it directly or by the relay of a CUE. In particular, we call a DUE the data owner (DO) if it launches the data sharing. Similarly, we call a DUE the data user (DU) if it is the receiver of some data. In additionally, a DUE or CUE with sufficient computation resource can serve as the outsourced decryption service provider (ODSP) for the DUs. The detailed function of each entity is given as follows:

CNS: CNS is a trusted central authority, which is in charge of initializing the system and generating the corresponding parameters. It also accepts the registration of the BSs and DUs. It labels each BS with a unique *Bid* and each DU with a unique *Uid*. Meanwhile, it creates the public-private key pairs for the BSs and DUs. Additionally, it also creates the final private key for each DU by employing the intermediate key (*IK*) generated by a BS. If necessary, CNS can help DUs check the correctness of PDC.

BS: Every BS is in charge of verifying the legitimacy of a DU. If so, it generates *IK* corresponding to the DU's attribute set. Note that every BS in our system governs the whole attribute universe rather than a disjoint attribute subset which was introduced in prior works [4], [5], [24], [37]. The DUE_4 is covered by BS_1 and BS_N as in Fig. 1, it can obtain the *IK* from either BS_1 or BS_N.

DO: DO chooses a symmetric encryption key (*SEK*) to encrypt its data. Then the DO defines an access structure under which *SEK* is encrypted. Finally, the encrypted data along with the ciphertext of *SEK* will be shared with the DUs.

DU: Each DU is assigned a unique *Uid* by the CNS and issued a public key and a user decryption key (*UDK*). Each DU can call for the decryption service from the ODSP by submitting his private key. The DU can also call the CNS to check whether the returned PDC is correctly computed. If so, he can recover *SEK* by the *UDK* and further decrypt the encrypted data.

ODSP: ODSP could help the DU pre-decrypt a ciphertext according to its private key. If the DU's attributes match the access structure in *SEK* ciphertext, the ODSP will return a PDC.

B. ADVERSARY MODEL AND SECURITY REQUIREMENTS

In RSDAC, CNS is fully trusted. We assume that the BSs could be compromised and they may collude with each other to obtain the *MSK*. The ODSP is honest-but-curious. That is, it executes its task honestly, but it would try to get as much information as possible of the encrypted data. The DUs might be malicious by colluding with each other to obtain extra access privilege that none of them has.

Concretely, we consider the following security requirements:

1. Fine-grained access control. In order to indicate who is authorized to access its data, the DO should be enabled to define flexible access structure.
2. Data Confidentiality. The data must be confidential to unauthorized access from both unauthorized DUs and ODSP.
3. DUs Collusion Resistance. The malicious DUs may combine their private keys to get access to the ciphertext that none of them is allowed. Such collusion resistance should be resisted.
4. BSs' Ultra Vires Resistance. The BS can not directly issue private keys for the DUs. That is, the BS could not obtain the *MSK* of the system, even if it colludes with the others.
5. Verifiability. Once the ODSP returns a wrong or invalid partial decryption ciphertext, such malicious behavior must be efficiently detected.

IV. PRELIMINARIES

A. BILINEAR MAPS

$\mathbb{G}$ and $\mathbb{G}_1$ refer to two multiplicative cyclic groups of prime order p. η refers to a generator of $\mathbb{G}$. $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$ is called a bilinear map if:

1. Bilinearity: $e(\zeta^x, \xi^y) = e(\zeta, \xi)^{xy}$ $\forall \zeta, \xi \in \mathbb{G}$ and $x, y \in \mathbb{Z}_p$;
2. Non-degeneracy: $e(\eta, \eta) \neq 1$ for g.
3. Symmetric: $e(\eta^\iota, \eta^\upsilon) = e(\eta, \eta)^{\iota\upsilon} = e(\eta^\upsilon, \eta^\iota)$.

B. LINEAR SECRET SHARING SCHEME (LSSS)

Definition 1: A secret sharing scheme Π over a set of parties $\mathbb{P}$ is linear (over $\mathbb{Z}_p$) if

1. The shares of a secret for each party form a vector over $\mathbb{Z}_p$.

2. A matrix A with ℓ rows and n columns is called the share-generating matrix for Π. ρ is a function which maps $\{i = 1, \ldots, \ell\}$ to $\mathbb{P}$. While considering the vector $\overrightarrow{\upsilon} = (s, r_2, \ldots, r_n)^T$, where $r_2, \ldots, r_n$ are randomly picked from $\mathbb{Z}_p$ and $s \in \mathbb{Z}_p$ is the secret to be shared, then $A\overrightarrow{\upsilon}$ denotes the vector of ℓ shares of s. The share $(A\overrightarrow{\upsilon})_i$ belongs to the party $\rho(i)$.

Every LSSS has the linear reconstruction property [38]. Suppose that Π is an LSSS of an access structure $\mathbb{A}(A, \rho)$ and $S \in \mathbb{A}$ is any authorized set. Let $I \subseteq \{1, 2, \ldots, \ell\}$ be $I = \{i : \rho(i) \in S\}$. There exist constants $\omega_i \in \mathbb{Z}_p$, such that, if $\lambda_i = (A\upsilon)_i$ are valid shares of s, then $\sum_{i \in I} \omega_i \lambda_i = s$.

C. ħ-TYPE ASSUMPTION

Choose a generator η from group $\mathbb{G}$ of prime order p. Randomly pick $\hbar + 2$ exponents $x, s, y_1, y_2, \ldots, y_\hbar \in \mathbb{Z}_p$. If an adversary is given $(p, \mathbb{G}, \mathbb{G}_1, e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1)$ and all of the following elements:

$$
\begin{aligned}
\aleph = {} & \eta, \eta^s \\
& \eta^{x^i}, \eta^{y_j}, \eta^{sy_j}, \eta^{x^i y_j}, \eta^{x^i/y_j^2}, \quad \forall (i,j) \in [\hbar, \hbar] \\
& \eta^{x^i/y_j}, \quad \forall (i,j) \in [2\hbar, \hbar] \text{with} i \neq \hbar + 1 \\
& \eta^{x^i y_j/y_{j'}^2}, \quad \forall (i,j,j') \in [2\hbar, \hbar, \hbar] \quad \text{with } j \neq j' \\
& \eta^{sx^i y_j/y_{j'}}, \eta^{x^i y_j/y_{j'}^2}, \quad \forall (i,j,j') \in [\hbar, \hbar, \hbar] \quad \text{with } j \neq j'
\end{aligned}
$$

The advantage with which an algorithm $\mathcal{B}$ can solve the above decisional ħ-type problem is defined as: $Adv_{\mathcal{B}(\lambda)} = | Pr[\mathcal{B}(\aleph, \Re = e(\eta, \eta)^{x^{\hbar+1}s}) = 0] - Pr[\mathcal{B}(\aleph, \Re = R) = 0] |$, where $e(\eta, \eta)^{x^{\hbar+1}s} \in \mathbb{G}_1$ and $R \in \mathbb{G}_1$ is randomly selected.

Definition 2: The ħ-type assumption holds if $Adv_{\mathcal{B}(\lambda)}$ is negligible of λ for all probabilistic polynomial time (PPT) adversaries.

D. DEFINITION OF MA-CP-ABE WITH VERIFIABLE OUTSOURCED DECRYPTION

A MA-CP-ABE scheme with verifiable outsourced decryption is comprised of the following nine algorithms:

Global Setup $(\lambda, U) \to (GPK, MSK)$: A CA runs this algorithm by taking in a security parameter λ along with the system attribute universe U. It outputs the global public parameters GPK and master secret key MSK.

AA Setup $(GPK, AAid) \to (PK_{AAid}, SK_{AAid})$: On input the AA's identifier $(AAid)$ and GPK, this AA setup algorithm outputs this AA's public key PK_{AAid} and private key SK_{AAid}.

User Setup $(GPK, Uid) \to (PK_{Uid}, UDK_{Uid})$: On input GPK and a user's identification information Uid, this user setup algorithm outputs this user's public key PK_{Uid} and the corresponding user decryption key UDK_{Uid}.

AA KeyGen $(S, GPK, SK_{AAid}) \to (IK)$: On input an attribute set S, GPK and SK_{AAid}, this AA key generation algorithm outputs the intermediate key IK of S.

CA KeyGen $(IK, GPK, MSK, PK_{AAid}) \to (SK)$: On input IK, GPK, MSK and PK_{AAid}, this CA key generation algorithm outputs the final private key SK.

Encrypt $(GPK, \mathbb{A}, M) \to (CT)$: On input GPK, an access structure $\mathbb{A}$ and a message M, this encryption algorithm outputs a ciphertext CT.

Transform $(GPK, SK, CT) \to (PDC)$: On input GPK, SK and CT, if S matches $\mathbb{A}$, this transformation algorithm outputs a partial decryption ciphertext PDC. Otherwise, it outputs $\perp$.

Decrypt $(PDC, UDK_{Uid}) \to (M)$: This decryption algorithm takes in PDC and UDK_{Uid}. If **Verify** $(PK_{Uid}, MSK, CT, PDC) \to 1$, it outputs M. Otherwise, it aborts.

Verify $(PK_{Uid}, MSK, CT, PDC) \to 1$ or 0: The verify algorithm takes in PK_{Uid}, MSK, CT and PDC. If PDC is correctly computed, it outputs 1. Otherwise, it outputs 0.

E. SECURITY MODEL

The security definition of our MA-CP-ABE is given by the following game between an adversary $\mathcal{A}$ and a challenger $\mathcal{B}$. Identical to the security model in [8], [33], in our game, the challenge access structure chosen by $\mathcal{A}$ has to be declared before initializing GPK.

Initialization. $\mathcal{A}$ specifies the challenge access structure $\mathbb{A}^*$.

Setup. By running the **Global Setup**, **AA Setup** and **User Setup** algorithms, $\mathcal{B}$ generates the corresponding parameters and transmits the public parameters to $\mathcal{A}$.

Phase 1. $\mathcal{A}$ can make key queries of the attribute sets $S_1, S_2, \cdots, S_{q_1}$, under such restriction that none of the sets can match $\mathbb{A}^*$.

Challenge. $\mathcal{A}$ submits two massages M_0 and M_1 with equal length. $\mathcal{B}$ encrypts M_b under $\mathbb{A}^*$ and gets a ciphertext CT^*, where b is randomly picked from $\{0, 1\}$. Then CT^* is transmitted to $\mathcal{A}$.

Phase 2. $\mathcal{A}$ acts the same as in **Phase 1**.

Guess. $\mathcal{A}$ guesses b' on b.

The advantage of $\mathcal{A}$ in the above scheme is defined as $| Pr[b' = b] - 1/2 |$.

Definition 3: A MA-CP-ABE scheme is selectively secure if $| Pr[b' = b] - 1/2 |$ is negligible for any PPT adversary.

F. VERIFIABILITY

Similarly, the verifiability model of our MA-CP-ABE is defined by the following security game between $\mathcal{A}$ and $\mathcal{B}$.

Setup. $\mathcal{A}$ and $\mathcal{B}$ act the same as in the above security game.

Phase 1. $\mathcal{A}$ can request the private keys the same as in the above security game.

Challenge Phase. Once receiving the challenge $\mathbb{A}^*$ from $\mathcal{A}$, $\mathcal{B}$ gets CT^* from the **Encrypt** algorithm and transmits it to $\mathcal{A}$.

Phase 2. Similar to **Phase 1**.

Output. $\mathcal{A}$ outputs an attribute set S^* along with two partial decryption ciphertext PDC_1^* and PDC_2^* for CT^*. $\mathcal{A}$ wins if the entry (PDC_1^*, PDC_2^*) can pass **Verify**, and **Decrypt** $(PDC_1^*, UDK_{Uid}) \neq$ **Decrypt** (PDC_2^*, UDK_{Uid}).

TABLE 1. Notations employed in RSDAC.

Notation	Description
CNS	core network server
BS	base station
DO	data owner
DU	data user
ODSP	outsourced decryption service provider
LSSS	linear secret sharing scheme
Bid	identifier of a BS
Uid	identifier of a DU
GPK	system global public parameters
MSK	system master secret key
PK_{Bid}, SK_{Bid}	public key and secret key of Bid
SEK	a symmetric key used to encrypt original data
EN_{KEM}	data encrypted by SEK
CT	ABE ciphertext of SEK
$\mathbb{A}$	access structure
(A, ρ)	$\mathbb{A}$ expressed by LSSS matrix A and map ρ
PK_{Uid}	DU's public key
UDK_{Uid}	user decryption key of Uid
S_{Uid}	attribute set of Uid
IK_{Uid}	intermediate key for S_{Uid}
SK_{Uid}	final private key for S_{Uid}
PDC	partial decryption ciphertext

Definition 4: Our MA-CP-ABE is verifiable if no PPT adversary can get a non-negligible advantage in the above game.

V. PROPOSED SCHEME

This section presents the detailed construction of the proposed RSDAC. Table 1 gives the description of notations employed in this scheme.

A. INITIALIZATION

1) GLOBAL SETUP

The CNS first calls the group generator and gets the terms $GG = (p, \mathbb{G}, \mathbb{G}_1, e)$, where p refers to the prime order of groups $\mathbb{G}$ and $\mathbb{G}_1$, and e denotes a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$. Then, CNS randomly picks η, w, ϑ, ψ, v from $\mathbb{G}$ and α, β from $\mathbb{Z}_p$. Besides, CNS chooses a hash function $H : (0, 1)^* \to \mathbb{Z}_p$. The system attribute universe is implicitly set as $\mathbb{Z}_p$. Finally, the system public key is published as: $GPK = (GG, \eta, w, \vartheta, \psi, v, e(\eta, \eta)^\alpha, H)$. The system master secret key is $MSK = (\alpha, \beta)$ which will not be transmitted to any other entity.

2) BS SETUP

When a BS joins in the system, it has to register itself from the CNS. For each BS, CNS labels the BS by a unique identifier Bid and randomly selects $SK_{Bid} = k_{Bid} \in \mathbb{Z}_p$, CNS then sets its public key as $PK_{Bid} = (\eta^{k_{Bid}}, w^{k_{Bid}})$. Then CNS sends (PK_{Bid}, SK_{Bid}) to the corresponding BS with identity Bid.

B. DATA OUTSOURCING

Same as [36], we use key encapsulation mechanism (KEM) to encrypt original data. That is, the original data is encrypted by a symmetric key (SEK) which will be encrypted under a chosen access structure.

Encrypt. The DO performs the data encryption algorithm as follows: DO defines an LSSS access structure $\mathbb{A}(A, \rho)$, where A refers to a $\ell \times n$ matrix and ρ maps each row A_τ to an attribute. DO randomly picks $s, \upsilon_2, \ldots, \upsilon_n$ from $\mathbb{Z}_p$ and sets a vector $\overrightarrow{\upsilon} = (s, \upsilon_2, \ldots, \upsilon_n)^\top$. In then computes $\overrightarrow{\lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_\ell)^\top = A \cdot \overrightarrow{\upsilon}$ and $C_0 = \eta^s$. For each $\tau \in \{1, 2, \ldots, \ell\}$, it randomly picks $x_\tau \in \mathbb{Z}_p$ and computes:

$C_{\tau,1} = (w^{\lambda_\tau} v^{x_\tau})$, $C_{\tau,2} = (\vartheta^{\rho(\tau)}\psi)^{-x_\tau}$ and $C_{\tau,3} = \eta^{x_\tau}$.

The SEK in KEM is set as $e(\eta, \eta)^{\alpha s}$ and the encrypted data is denoted as EN_{KEM}. The ciphertext of SEK is $CT = (C_0, \{C_{\tau,1}, C_{\tau,2}, C_{\tau,3}\}_{\tau \in \{1,2,\ldots,\ell\}})$.

C. USER KEY GENERATION

1) USER SETUP

The new joined DU has to register itself from the CNS. For each DU, CNS assigns a unique identification Uid and randomly picks $c_{Uid} \in \mathbb{Z}_p$. It then sets the DU's public key $PK_{Uid} = \eta^{c_{Uid}}$. Finally, CNS gives PK_{Uid} and the corresponding user decryption key ($UDK = c_{Uid}$) to the user with identity Uid.

2) BS KEYGEN

When receiving the private key request from a DU with identity Uid, the BS_i first checks if the DU's Uid has the specified attribute set S_{Uid} that it claimed as in [8]. If not, BS_i submits the identity information of Uid to CNS which may subsequently kick this user out. Otherwise, BS_i works as follows:

Firstly, BS_i queries the current timestamp value TSV and calculates $t_1 = H(Uid||TSV||0)$ and $t_2 = H(Uid||TSV||1)$.

Secondly, for each $AT_\tau \in S_{Uid}$, BS_i randomly picks $a_j \in \mathbb{Z}_p$ and computes:

$$\Gamma_{\tau,1} = \eta^{k_{Bid} a_j t_1}$$
$$\Gamma_{\tau,2} = \eta^{a_j t_2}$$
$$\Gamma_{\tau,3} = (\vartheta^{AT_{(\tau)}}\psi)^{k_{Bid} a_j t_1} v^{-k_{Bid} t_1}$$
$$\Gamma_{\tau,4} = (\vartheta^{AT_{(\tau)}}\psi)^{a_j t_2} v^{-t_2}$$

The intermediate key of S_{Uid} is set as $IK_{Uid} = \{\Gamma_{\tau,1}, \Gamma_{\tau,2}, \Gamma_{\tau,3}, \Gamma_{\tau,4}\}_{AT_\tau \in S_{Uid}}$.

Finally, the terms: $(Uid, Bid_i, S_{Uid}, TSV, IK_{Uid})$ are securely sent to CNS.

3) CNS KEYGEN

After receiving the terms from BS_i, CNS checks if the transmission delay is appropriate. If not, CNS refuses to accept the terms. Otherwise, CNS works as follows:

Firstly, CNS obtains PK_{Uid} and PK_{Bid_i} by Uid and Bid_i. It then sets $t_1 = H(Uid||TSV||0)$ and $t_2 = H(Uid||TSV||1)$.

Secondly, CNS randomly chooses $d \in \mathbb{Z}_p$ and uses MSK to create the private key SK_{Uid}:

$$\Upsilon_0 = (PK_{Uid})^\alpha (w^{k_{Bid}})^{d\beta t_1} w^{d\alpha t_2} = \eta^{\alpha c_{Uid}} w^{k_{Bid} d\beta t_1 + d\alpha t_2}$$
$$\Upsilon_1 = (\eta^{k_{Bid}})^{d\beta t_1} \eta^{d\alpha t_2} = \eta^{k_{Bid} d\beta t_1 + d\alpha t_2}$$

For each $AT_\tau \in S_{Uid}$, compute:

$$\Upsilon_{\tau,2} = (\Gamma_{\tau,1})^{d\beta}(\Gamma_{\tau,2})^{d\alpha} = \eta^{k_{Bid}d\beta a_j t_1 + d\alpha a_j t_2}$$
$$\Upsilon_{\tau,3} = (\Gamma_{\tau,3})^{d\beta}(\Gamma_{\tau,4})^{d\alpha} = (\vartheta^{AT_{(\tau)}}\psi)^{k_{Bid}d\beta a_j t_1 + d\alpha a_j t_2} v^{-(k_{Bid}d\beta t_1 + d\alpha t_2)}$$

For simplicity, we let $r_\tau = k_{Bid}d\beta a_j t_1 + d\alpha a_j t_2$ and $r = k_{Bid}d\beta t_1 + d\alpha t_2$.

Therefore, SK_{Uid} can be denoted as:

$$\begin{aligned} \Upsilon_0 &= \eta^{\alpha c_{Uid}} w^r \\ \Upsilon_1 &= \eta^r \\ \forall AT_\tau &\in S_{Uid}: \\ \Upsilon_{\tau,2} &= \eta^{r_\tau} \\ \Upsilon_{\tau,3} &= (\vartheta^{AT_{(\tau)}}\psi)^{r_\tau} v^{-r} \end{aligned}$$

Finally, $SK_{Uid} = (\Upsilon_0, \Upsilon_1, \{\Upsilon_{\tau,2}, \Upsilon_{\tau,3}\}_{\forall AT_\tau \in S_{Uid}})$ is sent to the DU via BS_i.

D. DECRYPTION AND VERIFICATION

1) TRANSFORM

After receiving EN_{KEM} and CT from DO, DU can request the ODSP to decrypt the data that it wants to access by submitting its attribute set S_{Uid}, SK_{Uid} and CT. If S_{Uid} satisfies $\mathbb{A}(A, \rho)$, the ODSP works as follows:

Set $X = \{x : \rho(x) \in S_{Uid}\}$ and compute such coefficients $\{\mu_x \in \mathbb{Z}_p\}_{x\in X}$ satisfying $\sum_{x\in X} = \mu_x \lambda_x = s$. Then compute

$$PDC = \frac{e(C_0, \Upsilon_0)}{\prod_{x\in X}\left(e\left(C_{x,1}, \Upsilon_1\right) e\left(C_{x,2}, \Upsilon_{\tau,2}\right) e\left(C_{x,3}, \Upsilon_{\tau,3}\right)\right)^{\mu_x}} = e(\eta, \eta)^{\alpha s c_{Uid}}$$

The ODSP sends PDC to the DU.

2) USER DECRYPTION

The DU can recover SEK by computing $SEK = PDC^{1/UDK} = (e(\eta, \eta)^{\alpha s c_{Uid}})^{1/c_{Uid}} = e(\eta, \eta)^{\alpha s}$.

3) VERIFICATION

After receiving (PDC, PK_{Uid}, C_0), the CNS checks if the following equation holds: $e((PK_{Uid})^\alpha, C_0) = PDC$. If so, CNS outputs 1 to indicate that the ODSP computes PDC correctly. Otherwise, It outputs 0 to indicate that the ODSP does not correctly compute PDC.

VI. SECURITY ANALYSIS

A. FINE-GRAINED ACCESS CONTROL

In RSDAC, the attribute universe is exponentially large. The DO can define arbitrary monotonic access structure over descriptive attributes, to indicate who has the access privilege to its data. Moreover, if a DO receives and stores the system public parameters on its device, then it can independently encrypt its data under the access structure, no matter it has connected to a BS or not.

B. DATA CONFIDENTIALITY

The data confidentiality of RSDAC is proved by the following theorem:

Theorem 1: Assume the $\hbar$-type assumption holds, then our RSDAC is selectively secure.

Proof: Recall that the DU's private key SK_{Uid} is in the form of:

$$\begin{aligned} \Upsilon_0 &= \eta^{\alpha c_{Uid}} w^r \\ \Upsilon_1 &= \eta^r \\ \forall AT_\tau &\in S_{Uid}: \\ \Upsilon_{\tau,2} &= \eta^{r_\tau} \\ \Upsilon_{\tau,3} &= (\vartheta^{AT_{(\tau)}}\psi)^{r_\tau} v^{-r} \end{aligned}$$

where $k_{Bid}d\beta a_j t_1 + d\alpha a_j t_2$ and $k_{Bid}d\beta t_1 + d\alpha t_2$ are simplified as r_τ and r, respectively. Meanwhile, because of the randomly chosen a_j and d, $\{r_\tau\}$ and r can be seen as totally random numbers. Thus, this theorem can be proved similarly to that in [36], where the details of proof are given. Theorem 1 holds means that the ciphertext is confidential to the DU if its attributes do not match $\mathbb{A}(A, \rho)$ in CT.

Moreover, even if the ODSP obtains the user's private key while providing outsourced decryption service, the encrypted data remains secret since that the user decryption key UDK is not given to the ODSP.

C. USER COLLUSION RESISTANCE

By combining their private keys, the malicious DUs may attempt to recover $SEK = e(\eta, \eta)^{\alpha s}$ that none of them can independently do. Unfortunately, they will fail due to the fact that each DU's private key elements are bounded by a unique chosen number d. Since d is chosen by CNS and is unknown to the DUs, it remains impossible for colluding DUs to access unauthorized data.

Different from the scheme [8], the randomness of the DU's private key in RSDAC not only relies on the timestamp numbers t_1 and t_2, but also the unique number d. Thus, there is no requirement of employing extra master secret key b and computing $\eta^{-(t_1+t_2)}$ and $\eta^{(t_1+t_2)}$ as in [8]. Moreover, a malicious DU in our RSDAC can not deduce any useful element from his private key to gain additional access privilege.

D. BSS' ULTRA VIRES RESISTANCE

The BSs may collude with each other to gain the system secret information about α and β. In [8], the authors showed how the colluded BSs act. Suppose BS_1 and BS_2 choose the same terms (t_1, t_2), η^α can be computed by theses two BSs, which then can generate any effective private key and access any encrypted data. Such collusion attacks are resisted by ensuring the terms (t_1, t_2) are different and never used before. However, in RSDAC, we introduce an additional parameter d which is unique for every attribute set. Even if BS_1 and BS_2 set the same terms (t_1, t_2), they can not cancel $d\alpha t_2$ in the exponents because of the different d_i for each attribute set. Thus, the colluded BSs can not obtain any useful information of η^α.

TABLE 2. Feature comparison of CP-ABE works.

Schemes	Multi-authority	Robust AA/BS [1]	large universe	access structure	outsourced decryption	Verifiability
[33]	×	\	√	LSSS	×	×
[17]	×	\	×	BF[2]	×	×
[36]	×	\	√	LSSS	√	√
[6]	√	×	×	LSSS	√	×
[7]	√	×	√	LSSS	√	×
[8]	√	√	×	LSSS	×	×
RSDAC	√	√	√	LSSS	√	√

Robust AA/BS means that each AA/BS governs the whole attribute universe rather than a distinct part of it.
BF is the abbreviation of 'Boolean Formula'.

TABLE 3. Size comparison between large universe schemes.

Schemes	PK	USK	CT	ESV
[33]	$5\|\mathbb{G}\|+1\|\mathbb{G}_1\|$	$(2\|S_U\|+2)\|\mathbb{G}\|$	$(3\|S_E\|+1)\|\mathbb{G}\|+1\|\mathbb{G}_1\|$	\
[36]	$5\|\mathbb{G}\|+1\|\mathbb{G}_1\|$	$(2\|S_U\|+3)\|\mathbb{G}\|$	$(3\|S_E\|+1)\|\mathbb{G}\|$	$2\|\mathbb{G}\|+1\|\mathbb{G}_1\|$
[7]	$(5+2\|S_A\|)\|\mathbb{G}\|+1\|\mathbb{G}_1\|$	$(2\|S_U\|+2)\|\mathbb{G}\|$	$(3\|S_E\|+1)\|\mathbb{G}\|+1\|\mathbb{G}_1\|$	\
RSDAC	$5\|\mathbb{G}\|+1\|\mathbb{G}_1\|$	$(2\|S_U\|+2)\|\mathbb{G}\|$	$(3\|S_E\|+1)\|\mathbb{G}\|$	$2\|\mathbb{G}\|+1\|\mathbb{G}_1\|$

E. VERIFIABILITY

Theorem 2: For all PPT adversaries, the advantage is at most negligible in the verifiability security game.

Proof: We assume there exists an adversary $\mathcal{A}$ which can break the verifiability of our scheme, then a simulator $\mathcal{B}$ can be built to interact with $\mathcal{A}$ as follows:

Setup. $\mathcal{B}$ initializes the system and sets the system parameters GPK, MSK and $\{(PK_{Bid}, k_{Bid})\}$ as in the real scheme. It then sends GPK and $\{(PK_{Bid}, k_{Bid})\}$ to $\mathcal{A}$.

Phase 1. $\mathcal{A}$ can query the keys of attribute sets $S_1, \ldots, S_{q_1}$. $\mathcal{B}$ then generates the corresponding private keys and sends them to $\mathcal{A}$.

Challenge. $\mathcal{A}$ declares a challenge LSSS access structure $\mathbb{A}^*(A^*, \rho)$. $\mathcal{B}$ obtains a challenge ciphertext CT^* by running **Encryption** and transmits it to $\mathcal{A}$.

Phase 2. Same as **Phase 1**.

Output. $\mathcal{A}$ has to output two partial decryption ciphertexts PDC_1^* and PDC_2^* of CT^*.

$\mathcal{A}$ wins if the following 3 conditions are fulfilled simultaneously.

(1). **Verification** outputs 1 on PDC_1^*;

(2). **Verification** outputs 1 on PDC_2^*;

(3). **User Decryption** $(PDC_1^*, UDK_{Uid}) \neq$ **User Decryption** (PDC_2^*, UDK_{Uid}).

From (1) and (2), we have $PDC_1^* = PDC_2^*$. However, condition (3) means that $PDC_1^* \neq PDC_2^*$. Thus, $\mathcal{A}$ has only negligible advantage to win the above game.

VII. PERFORMANCE ANALYSIS

A. FEATURES COMPARISON

Table 2 compares some features between previous related CP-ABE works and RSDAC, involving multi-authority, robust AA/BS, large universe, access structure, outsourced decryption and verifiability.

From Table 2, we can see that only the scheme in [8] and RSDAC achieve the robust AA/BS. That is, each AA/BS is in charge of governing the whole attribute universe of system. Except the schemes in [6], [8], [17], the other schemes can support large attribute universe. The user decryption overhead in [8], [17], [33] increases with the number of used attributes. On the contrary, the user decryption overhead in [6], [7], [36] and RSDAC is constant size by employing the outsourced decryption technique. Only RSDAC and the scheme in [36] enable the users to check the correctness of PDC. However, the scheme in [36] only supports the single authority, without considering multiple attribute authorities. In general, RSDAC is the only one which simultaneously achieves the promising features mentioned above.

B. NUMERAL COMPARISON

In Table 3, we compare the large universe schemes [7], [33], [36] and RSDAC, in terms of the size of system public parameters (PK), user's private keys (USK), ciphertext (CT) and the entry sent for verifying (ESV). Different form the AA's parameters $\{APK_f\}$ in the scheme [7], the BSs' parameters $\{PK_{Bid}\}$ in our scheme is only used by the CNS and will not be involved in the encryption phase. Thus, we do not record the size of $\{PK_{Bid}\}$ in the size of PK. In Table 3, $|\mathbb{G}|$ and $|\mathbb{G}_1|$ refer to an element in $\mathbb{G}$ and $\mathbb{G}_1$, respectively. S_E and S_U refer to the related attribute sets involved in the CT and SK, respectively. Besides, S_A denotes the set of attribute authorities.

Table 3 shows that the PK size of RSDAC is the same as in the schemes [33], [36], which is less than that in [7]. Except that in the scheme in [36], the size of USK is the same in other schemes. Specially, the size of CT and ESV in [36] and RSDAC is the same. RSDAC does not add any extra elements while achieving multi-authority and robust BSs. Thus, the proposed RSDAC is considerable and applicable in D2D communications.

C. IMPLEMENTATION RESULT

We implement our scheme, the NCDLMW scheme [36] and the LZ scheme [7]. All these three schemes are constructed on the large universe scheme [33]. The implementation is performed on a Ubuntu 18.04 LTS system (with 3.40GHz Inter Core i7 CPU and 8.00GB RAM), based on the JPBC library 2.0.0 [39]. We employ a Type A pairing which is

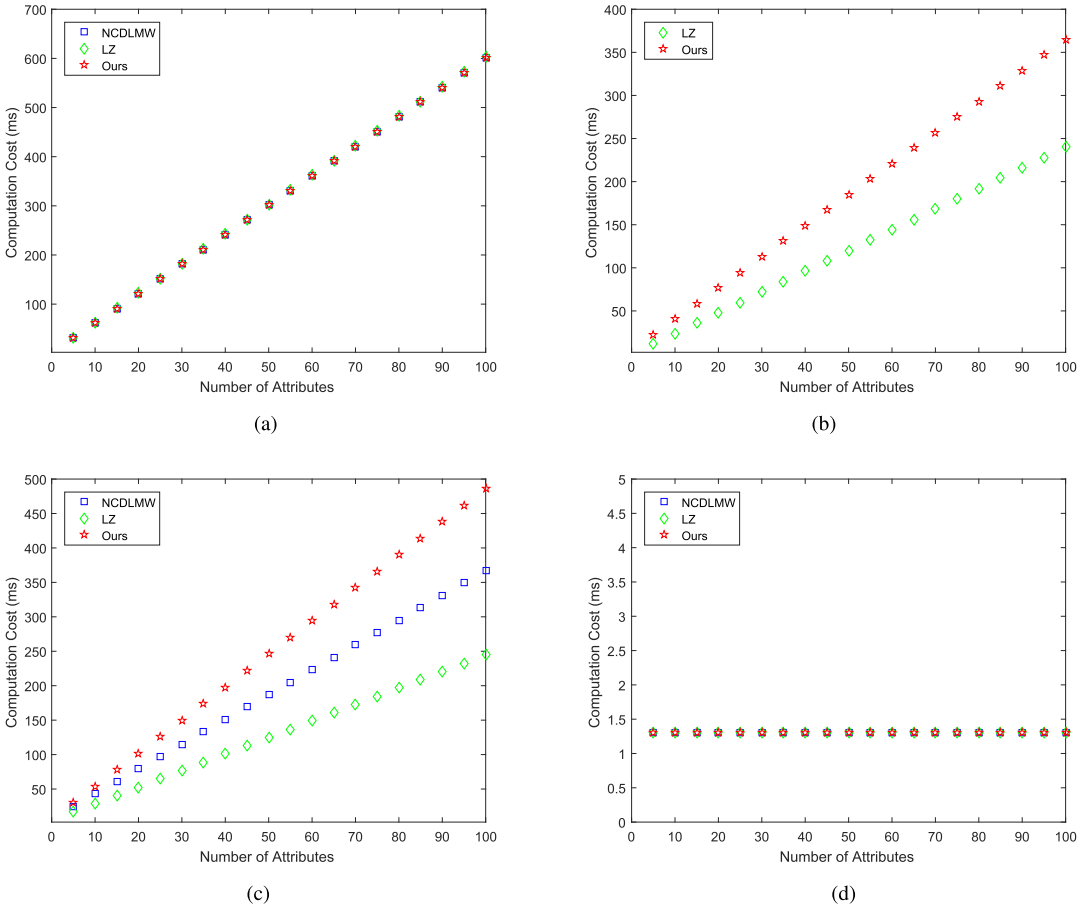


FIGURE 2. Implementation Results. (a) Encryption. (b) AA/BS KeyGen. (c) CA/CNS KeyGen. (d) User Decryption.

constructed over a symmetric elliptic curve α-curve with 160-bit prime order p.

In Fig. 2, we evaluate the computation cost during the phase of encryption, key generation and user decryption. Each simulation result is the average of 30 trials.

Fig. 2(a) and Fig. 2(d) demonstrate that the time of encryption and user decryption in RSDAC is almost the same as that in NCDLMW scheme and LZ scheme. More precisely, the encryption overhead of these three schemes is linear with the scale of access structure. The only difference is that the element $e(\eta, \eta)^{\alpha s}$ in NCDLMW scheme and RSDAC is set as SEK in KEM, while $e(\eta, \eta)^{\alpha s}$ is used to encrypt the data encryption key in LZ scheme. Additionally, the user decryption in these three schemes only costs one time of exponential operation due to the usage of outsourced decryption technique [34].

Fig. 2(b) and Fig. 2(c) show that our scheme requires more computation time in the phase of AA/BS keygeneration and CA/CNS keygeneration than that in NCDLMW scheme and LZ scheme. This is due to the fact that we use the method to avoid the single-point bottleneck as in [8], where the computation cost for each attribute is twice of that in the original scheme [40].

VIII. CONCLUSION

In this work, we have addressed three major problems of data security, identity privacy and system scalability in D2D communication, by presenting a data access control scheme for D2D communication with robust multiple authorities, large attribute universe and verifiable outsourced decryption. In particular, each of multiple BSs can complete the task of DU legitimacy verification individually. Different from most prior multi-authority works, each BS can generate intermediate attribute keys according to arbitrary subset of whole system attribute universe. Such keys would be employed by the CNS to create the finally private keys. we also provided an efficient approach to help DUs offload most decryption overhead to a third device and check whether the device has correctly computed. The security analysis, numeral comparison and experimental results showed that RSDAC is secure, efficient and applicable in D2D communication scenario.

Although the verification of DU legitimacy is offloaded to the BSs, the single CNS remains has to create the final private keys for all DUs in the system. It would be interesting to design a more efficient key generation algorithm, where multiple CNSs exist and each of them can independently finish the generation of final private keys.

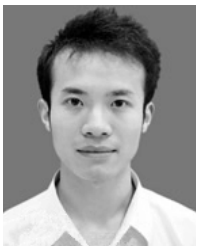
REFERENCES

[1] P. Gandotra *et al.*, "A survey on device-to-device (D2D) communication: Architecture and security issues," *J. Netw. Comput. Appl.*, vol. 78, pp. 9–29, Jan. 2017.
[2] F. Jameel, Z. Hamid, F. Jabeen, S. Zeadally, and M. A. Javed, "A survey of device-to-device communications: Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2133–2168, 3rd Quart., 2018.
[3] A. Zhang, J. Chen, R. Q. Hu, and Y. Qian, "SeDS: Secure data sharing strategy for D2D communication in LTE-advanced networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2659–2672, Apr. 2016.
[4] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 6632, K. Paterson, ed. Berlin, Germany: Springer, 2011, pp. 568–588.
[5] Z. Liu, Z. Cao, Q. Huang, D. S. Wong, and T. Yuen, "Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles," in *Computer Security—ESORICS* (Lecture Notes in Computer Science), vol. 6879, V. Atluri and C. Diaz, Eds. Berlin, Germany: Springer, 2011, pp. 278–297.
[6] Q. Li, J. Ma, R. Li, X. Liu, J. Xiong, and D. Chen, "Secure, efficient and revocable multi-authority access control system in cloud storage," *Comput. Secur.*, vol. 59, pp. 45–59, Jun. 2016.
[7] Q. Li and H. Zhu, "Multi-authority attribute-based access control scheme in mhealth cloud with unbounded attribute universe and decryption outsourcing," in *Proc. 9th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2017, pp. 1–7.
[8] K. Xue *et al.*, "RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 4, pp. 953–967, Apr. 2017.
[9] R. Wang, J. Yan, D. Wu, H. Wang, and Q. Yang, "Knowledge-centric edge computing based on virtualized D2D communication systems," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 32–38, May 2018.
[10] D. Wu, J. Yan, H. Wang, D. Wu, and R. Wang, "Social attribute aware incentive mechanism for device-to-device video distribution," *IEEE Trans. Multimedia*, vol. 19, no. 8, pp. 1908–1920, Aug. 2017.
[11] B. Zhou, H. Hu, S. Q. Huang, and H. H. Chen, "Intracluster device-to-device relay algorithm with optimal resource utilization," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2315–2326, Jun. 2013.
[12] H. Min, J. Lee, S. Park, and D. Hong, "Capacity enhancement using an interference limited area for device-to-device uplink underlaying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 12, pp. 3995–4000, Dec. 2011.
[13] H. Min, W. Seo, J. Lee, S. Park, and D. Hong, "Reliability improvement using receive mode selection in the device-to-device uplink period underlaying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 413–418, Feb. 2011.
[14] H. Kwon, D. Kim, C. Hahn, and J. Hur, "Secure authentication using ciphertext policy attribute-based encryption in mobile multi-hop networks," *Multimedia Tools Appl.*, vol. 76, no. 19, pp. 19507–19521, Oct. 2017.
[15] J. Huang *et al.*, "Modeling and analysis on access control for device-to-device communications in cellular network: A network-calculus-based approach," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1615–1626, Mar. 2016.
[16] J. Yue, C. Ma, H. Yu, and W. Zhou, "Secrecy-based access control for device-to-device communication underlaying cellular networks," *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2068–2071, Nov. 2013.
[17] Z. Yan, H. Xie, P. Zhang, and B. B. Gupta, "Flexible data access control in D2D communications," *Future Gener. Comput. Syst.*, vol. 82, pp. 738–751, May 2018.
[18] J. Xiong *et al.*, "Enhancing privacy and availability for data clustering in intelligent electrical service of IoT," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2018.2842773.
[19] J. Xiong, Y. Zhang, X. Li, M. Lin, Z. Yao, and G. Liu, "RSE-PoW: A role symmetric encryption pow scheme with authorized deduplication for multimedia data," *Mobile Netw. Appl.*, vol. 23, no. 3, pp. 650–663, 2018.
[20] D. Wu, S. Si, S. Wu, and R. Wang, "Dynamic trust relationships aware data privacy protection in mobile crowd-sensing," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2958–2970, Aug. 2018.
[21] D. Wu, F. Zhang, H. Wang, and R. Wang, "Security-oriented opportunistic data forwarding in mobile social networks," *Future Gener. Comput. Syst.*, vol. 87, pp. 803–815, Oct. 2018.
[22] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 3494, R. Cramer, ed. Berlin, Germany: Springer, 2005, pp. 457–473.
[23] 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.*, New York, NY, USA, 2006, pp. 89–98.
[24] M. Chase, "Multi-authority attribute based encryption," in *Theory of Cryptograph* (Lecture Notes in Computer Science), vol. 4392, S. Vadhan, ed. Berlin, Germany: Springer, 2007, pp. 515–534.
[25] Q. Li, J. Ma, R. Li, J. Xiong, and X. Liu, "Large universe decentralized key-policy attribute-based encryption," *Secur. Commun. Netw.*, vol. 8, no. 3, pp. 501–509, 2015.
[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] J. Li, Z. Guan, X. Du, Z. Zhang, and J. Wu, "An efficient encryption scheme with verifiable outsourced decryption in mobile cloud computing," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.
[28] Y. Yang, X. Liu, and R. H. Deng, "Lightweight break-glass access control system for healthcare Internet-of-Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3610–3617, Aug. 2018.
[29] Y. Wang and J. Gao, "A regulation scheme based on the ciphertext-policy hierarchical attribute-based encryption in bitcoin system," *IEEE Access*, vol. 6, pp. 16267–16278, 2018.
[30] Y. Yang, X. Chen, H. Chen, and X. Du, "Improving privacy and security in decentralizing multi-authority attribute-based encryption in cloud computing," *IEEE Access*, vol. 6, pp. 18009–18021, 2018.
[31] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.
[32] A. Lewko and B. Waters, "Unbounded HIBE and attribute-based encryption," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 6632, K. G. Paterson, ed. Berlin, Germany: Springer, 2011, pp. 547–567.
[33] Y. Rouselakis and B. Waters, "Practical constructions and new proof methods for large universe attribute-based encryption," in *Proc. ACM SIGSAC Conf. Comput., Commun. Secur.*, New York, NY, USA, 2013, pp. 463–474.
[34] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," in *Proc. 20th USENIX Conf. Secur.*, Berkeley, CA, USA: USENIX Association, 2011, p. 34.
[35] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 8, pp. 1343–1354, Aug. 2013.
[36] J. Ning, Z. Cao, X. Dong, K. Liang, H. Ma, and L. Wei, "Auditable σ -time outsourced attribute-based encryption for access control in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 94–105, Jan. 2018.
[37] J. Zhou, Z. Cao, X. Dong, and X. Lin, "TR-MABE: White-box traceable and revocable multi-authority attribute-based encryption and its applications to multi-level privacy-preserving e-healthcare cloud computing systems," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr./May 2015, pp. 2398–2406.
[38] A. Beimel, "Secret-sharing schemes: A survey," in *Coding and Cryptology* (Lecture Notes in Computer Science), vol. 6639. Berlin, Germany: Springer, 2011, pp. 11–46.
[39] A. De Caro and V. Iovino, "jPBC: Java pairing based cryptography," in *Proc. 16th IEEE Symp. Comput. Commun., (ISCC)*, Kerkyra, Greece, Jun./Jul. 2011, pp. 850–855.
[40] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Public Key Cryptography–PKC*. Berlin, Germany: Springer, 2011, pp. 53–70.

QI LI received the Ph.D. degree in computer system architecture from Xidian University, Xi'an, China, in 2014. He is currently a Lecturer with the School of Computer Science, Nanjing University of Posts and Telecommunications, China. His research interests include cloud security, information security, and applied cryptography.

LIZHI HUANG received the B.S. degree in information security from the Nanjing University of Posts and Telecommunications, China, in 2016, where she is currently pursuing the M.S. degree in information security. Her research interests include attribute-based encryption, cloud data security, and image recognition.

RUO MO received the B.S. degree from the School of Computer Science and Technology, Xidian University, in 2012, where he is currently pursuing the Ph.D. degree with the School of Cyber Engineering. His research interests include cryptography and network security.



HAIPING HUANG received the B.Eng. and M.Eng. degrees in computer science and technology from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2002 and 2005, respectively, and the Ph.D. degree in computer application technology from Soochow University, Suzhou, China, in 2009. He is currently a Professor with the School of Computer Science and Technology, Nanjing University of Posts and Telecommunications. His research interests include intelligent information processing and system reliability in Internet of Things. He is currently an Associate Editor of the *International Journal of Communication Systems* and an Editor of the *International Journal of Distributed Sensor Networks*.

HONGBO ZHU received the bachelor's degree in telecommunications engineering from the Nanjing University of Posts and Telecommunications, Nanjing, China, and the Ph.D. degree in information and communications engineering from the Beijing University of Posts and Telecommunications, Beijing, China, in 1982 and 1996, respectively. He is currently a Professor with the Nanjing University of Posts and Telecommunications. He is also the Head of the Coordination Innovative Center of IoT Technology and Application, Jiangsu, which is the first governmental authorized Coordination Innovative Center of IoT in China. He also serves as a referee or expert in multiple national organizations and committees.

He has published over 200 papers on information and communication area, such as the IEEE TRANSACTIONS. He is leading a big group and multiple funds on IoT and wireless communications with the current focus on architecture and enabling technologies for the Internet of Things.