Multi-Authority CP-ABE Scheme With Cryptographic Reverse Firewalls for Internet of Vehicles

Ye Lin, Hu Xiong, *Senior Member, IEEE*, Hui Su, and Kuo-Hui Yeh, *Senior Member, IEEE*

***Abstract*— Internet of vehicles, featured with widely distributed vehicle nodes and limited computing power, usually have high performance requirements. Because of this feature, efficient and reliable access control has raised a challenge in Internet of vehicles. Ciphertext-policy attribute-based encryption (CP-ABE) could be denoted as an efficient solution for this problem. However, directly applying traditional single-authority CP-ABE schemes may result in single-point performance bottleneck. Besides, the secrets of the whole system may be leaked if any node is attacked. To solve these challenging tasks, we proposed MA-CP-ABE-CRF, a multi-authority CP-ABE scheme with cryptographic reverse firewalls. The system is designed to grant vehicles fine-grained access control by encrypting data under vehicle attributes. Besides, load balancing of authorization in distributed systems is achieved based on the characteristic of multi-authority. Meanwhile, specific nodes are equipped with cryptographic reverse firewalls (CRFs) to prevent information leakage. As the first scheme with the above features for Internet of vehicles, the system achieves adaptive CPA-security and ASA-security. Through rigorous theoretical analysis and experimental comparison, MA-CP-ABE-CRF is proved to be highly efficient and practical.**

***Index Terms*— Internet of Vehicles, attribute-based encryption, cryptographic reverse firewall, multi-authority, compute control.**

I. Introduction

INTERNET of vehicles(IoVs), is a comprehensive network system that integrates advanced information technology, data communication transmission technology, electronic sensing technology and many other technologies [1]. It combines the car with the Internet to achieve a full range of information exchange and communication. This not only enables vehicles to automatically collect, process and share traffic information, but also improves road use efficiency, reduces traffic accidents and optimizes traffic management. IoVs have a wide range of applications, from enhancing the personal driving experience to promoting the development of intelligent transportation systems [2].

The security of IoV systems is of significant importance. For example, the system proposed in [3] attempts to safeguard privacy within IoV systems, and the mechanism in [4] attempts to ensure the CIA security of the whole system. In practical application, Internet of vehicles usually consist of widely distributed nodes(e.g., vehicles, transportation management center, etc.), making it hard to enforce flexible and fine-grained access control over the data sent and received by the nodes. Besides, even if only one node in this system is under attack, the entire system will be threatened. What's more, due to limited computing power [5], nodes in IoV systems are usually demanding in power-saving, and may affect user experience when processing complex algorithms. Therefore, it is essential to design an secure and efficiently fine-grained access control mechanism for IoVs.

Ciphertext-policy attribute-based encryption (CP-ABE) [6], [7], [8], [9], a special extension of public key encryption, is able to satisfy fine-grained access control, and is expected to serve as the security solution for IoVs. In CP-ABE systems, user attributes(i.e., vehicle attributes) are embedded in keys to decrypt the messages. Meanwhile, each ciphertext is related to a specific access structure which is designated by data owners(i.e., vehicles) and can determine the attributes required to decrypt the ciphertext. In this way, the system can gain flexible and fine-grained access control. The interesting feature of CP-ABE determines that it is perfect for access control of IoV nodes with various attributes. This is crucial for defending against common IoV security threats such as Sybil attacks, where malicious nodes forge multiple identities to disrupt the network, and data tampering attacks, where adversaries manipulate sensitive vehicle communication. CP-ABE's ability to enforce strict access control based on vehicle attributes mitigates these risks by ensuring only legitimate users can decrypt and access critical information. The interesting feature of CP-ABE determines that it is perfect for access control of IoV nodes with various attributes.

The first CP-ABE scheme is proposed by Bethcourt et al. [6] in 2007. However, in traditional CP-ABE system, the private key is generated and distributed by Key Generation Center (KGC). As mentioned above, nodes in IoVs are always widely distributed, so simply applying traditional CP-ABE scheme may cause performance bottlenecks. For instance, heavy computation requirements may result in a performance decline of KGC. What's worse, the system will collapse completely if the

Received 28 March 2024; revised 27 October 2024; accepted 31 December 2024. Date of publication 4 February 2025; date of current version 31 March 2025. This work was supported by the National Key Research and Development Program of China under Grant 2022YFB2701400. The Associate Editor for this article was M. H. Anisi. *(Ye Lin, Hu Xiong, and Hui Su contributed equally to this work.) (Corresponding author: Kuo-Hui Yeh.)*

Ye Lin and Hu Xiong are with the School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China, and also with the Network and Data Security Key Laboratory of Sichuan Province, Chengdu 610054, China (e-mail: ylin@alu.uestc.edu.cn; xionghu.uestc@gmail.com).

Hui Su is with the Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: rhondasu928@gmail.com).

Kuo-Hui Yeh is with the School of Industry Academia Innovation, Institute of Artificial Intelligence Innovation, National Yang Ming Chiao Tung University, Hsinchu 300093, Taiwan, and also with the Department of Information Management, College of Management, National Dong Hwa University, Hualien 97401, Taiwan (e-mail: khyeh@nycu.edu.tw).

Digital Object Identifier 10.1109/TITS.2025.3533757

KGC is damaged. To conclusion, traditional CP-ABE scheme is not suitable for distributed systems with limited resources. To overcome such shortcomings, the idea of multi-authority attribute-based encryption system has been introduced by Chase [9]. After that, Müller et al. [10] firstly proposed a multi-authority ciphertext-policy attribute-based encryption system. Inspired by these schemes, a series of CP-ABE systems with multiple authorities are designed to improve the functionality [11], efficiency [12] and security [13], [14]. In a multi-authority CP-ABE system, a private key consists of a central authority key and attribute authority keys, which are generated by the central authority (CA) and multiple attribute authorities (AAs) respectively. The introduction of multiple AAs can greatly reduce the burden of CA in key generation. Meanwhile, AAs are widely distributed, and each AA can independently generate and send the AA secret key to nodes. Overall, multi-authority CP-ABE schemes can provide reliable and efficient access control for the Internet of Vehicles.

Standard multi-authority CP-ABE schemes, however, still suffer security drawbacks. By considering that Internet of vehicles usually consist of widely distributed nodes, it is difficult to resist the infiltration attack in case the multi-authority CP-ABE scheme is deployed to secure the whole system. Moreover, the security of the whole system cannot be guaranteed even if there is only one node being compromised. For example, attackers may attempt to intercept or tamper with the data packets sent or received by vehicles to gain access to sensitive information such as vehicle location, driving routes, and driver identity. This breach of privacy can enable the tracking of specific vehicles or be exploited for illicit financial gains. Based on this, cryptographic reverse firewall (CRF) should be introduced. A CRF can be thought as an invisible entity deployed between different network nodes. It can prevent the leak of user privacy by re-randomizing messages received or sent by a user. After the Snowden incident, Mironov and Stephens-Davidowitz [15] creatively presented cryptographic reverse firewalls. CRF must be functionality-maintaining, security-preserving and exfiltration-resistant. To date, CRF has been successfully used in various scenarios such as key negotiation protocol [16], ABE scheme [17], searchable public-key encryption [18] and digital signature [19]. Owing to the re-randomization of messages by CRF, confidential information will not be disclosed even when a node is controlled by adversaries and the cryptographic algorithms are modified. Thus, the security of remote distribution system is assured.

As mentioned above, an efficient multi-authority CP-ABE scheme equipped with CRFs is highly desirable for widely-distributed Internet of vehicles. However, the CP-ABE scheme featured with multi-authority and CRF has not been treated in the literature so far. Moreover, existing multi-authority CP-ABE systems are implemented in symmetric prime-order groups, which resulted in high communication cost and computation cost. Hence, directly applying existing multi-authority CP-ABE schemes will result in efficiency problems. To fill this gap, we present a more efficient multi-authority CP-ABE scheme, and firstly applied CRFs to the CP-ABE algorithm. In the proposed scheme, a key generation center will firstly issue the public key and the main secret key, distributing them through reverse firewalls for security. The central authority and attribute authorities will then generate specific keys for vehicles, which ensure that only authorized entities can decrypt communications based on a designated access structure. Through rigorous experiments, our scheme is proved to fulfill the needs of IoVs with limited battery resources, and is superior to existing algorithms in terms of function, performance and security. Our contributions can be briefly described as follows.

1) In consideration of the characteristics of Internet of vehicles, we presented a MA-CP-ABE (**M**ulti-**A**uthority **C**iphertext-**P**olicy **A**ttribute-**B**ased **E**ncryption) system. Specifically, vehicles can encrypt messages embedded with specific access policies, while only the nodes hold the corresponding attribute keys can decrypt it. Our system not only realizes the flexible and fine-grained management of nodes, but also solves the difficulty of user key management in distributed systems. Our scheme gets better efficiency and adaptability in resource-constrained systems than existing schemes, making it better for Internet of vehicles.
2) To enhance the security, cryptographic reverse firewalls are deployed in our system, and a more secure MA-CP-ABE-CRF scheme is proposed. The introduction of CRFs prevents entities from being affected by infiltration attack, and specific entities in the proposed system are defended with corresponding CRFs. In this way, even if an attacker infects a number of nodes and tries to send out secret message, the information will not be leaked for the secret message has already been re-randomized by the CRFs.
3) The concrete theoretical analysis and experiments are conducted, thus prove that our system performs excellently in efficiency and practicality in various scenarios. In addition to higher performance, our scheme is more secure because it can resist infiltration attack thanks to the deployment of CRFs.

II. Related Work

A. Ciphertext-Policy Attribute-Based Encryption

Attribute-Based Encryption(ABE), firstly presented by Goyal et al. [20], is featured with secure access structure and fine-grained access control. The CP-ABE scheme is firstly proposed by Bethcourt et al. [6]. This system creatively associates secret keys with specific attributes, but is proved to be secure only in specific models. Inspired by this construction, more CP-ABE schemes [7], [8] with stronger security or higher efficiency have been proposed. However, the above schemes are all single-authority systems that generate and distribute private keys through a single authority, thus resulted in the bottleneck of single point in performance. In order to solve the shortcoming of single-authority systems, Chase [9] firstly proposed an ABE system with multiple authorities. This multi-authority ABE system uses multiple attribute authorities to manage the attribute sets and distribute corresponding keys, while no central authority (CA) is introduced into the scheme. Then, Chase and Chow [21] proposed an ABE system with

multiple authorities of a free CA. Inspired by the firstly CP-ABE scheme [6], plenty of multi-authority systems have come into being. A decentralized CP-ABE scheme is proposed by lewko et al. [22], in which the secret key can be completely generated by multiple attribute authorities. Inspired by [22], Ruj et al. [23] focused on the access structure of cloud servers, and proposed a methodology that supports user revocation. Lin et al. [24] presented a system with threshold mechanism, which is in fact an access control system with decentralized property. Then, a plenty of multi-authority algorithms are subsequently proposed by many researchers [25], [26], [27]. In the last few years, multi-authority ciphertext-policy attributed-based encryption has demonstrated its effectiveness in IoT-enabled infrastructure [28] and IoMT [29]. Recently, several effective improved CP-ABE algorithms have also been proposed. MA-ABE [30] achieved shorter ciphertexts and smaller key sizes in decentralized CP-ABE algorithms, while the algorithm in [31] also contributed to reducing ciphertext size. Though existing multi-authority schemes reduce the risk of single-point performance bottleneck, performance defects still exist in large-scale systems. For example, each attribute is managed only by one authority, so only this authority can generate the secret key bounded with this attribute. Thus, there remains much scope for improvements in CP-ABE schemes.

B. Cryptographic Reverse Firewall

Inspired by Snowden incident, Mironov and Stephens-Davidowitzthe designed an algorithm named cryptographic reverse firewall (CRF) [15] in 2015. In this paper, CRF is proved to satisfy three distinct characteristics: functionality maintaining, security preservation and exfiltration resistance. In practice, CRF is invisible to users, and an arbitrary number of CRFs can be combined with any cryptographic protocols. By taking advantage of CRF, any compromised machines can be prevented from information disclosure. In 2016, a protocol of massage transmission with CRFs is designed by Dodis [32]. Then, Chen et al. [16] designed a CRF framework for multiple cryptographic protocols based on the projective hash function (SPHF). In 2018, Ma et al. [17] introduced cryptographic reverse firewall into an attribute-based encryption system based on ciphertext attributes of online/offline. Later in 2019, Zhou et al. [33] proposed an identity-based encryption (IBE) scheme with CRF (IBE-CRF). In recent years, several systems based on CRF [18], [19] have been proposed. In the latest researches, CRFs have been integrated with IoT applications [34] and public key encryption in cloud storage [35].

III. Preliminaries And Definitions

A. Access Structures

Definition 1 (Access Structure): Let π denotes the attribute universe, $\mathbb{A}$ denotes an access structure of non-empty subsets of π, and only the sets existed in $\mathbb{A}$ can be called authorized. $\mathbb{A}$ is monotone if for $\forall\ B$ and C, $B \in \mathbb{A}$, $B \subseteq C$, then $C \in \mathbb{A}$ holds.

Definition 2 (Monotone Span Program(MSP)): A MSP for the attribute universe π is composed of a pair $(\mathbf{M}, \upsilon)$, where $\mathbf{M}$ is a matrix of n_1 rows and n_2 columns over $\mathbb{Z}_p$, and υ is a mapping $\upsilon : \{1, \ldots, n_1\} \to \pi$. An effective way to generate the monotone span program has been proposed by Lewko et al. [36], and all elements of $\mathbf{M}$ must be ± 1 or 0. If an attribute set μ is accepted by a pair $(\mathbf{M}, \upsilon)$, there will exist the coefficients $\{\gamma_x\}_{x\in\chi}$ such that

$$\sum_{x\in\chi} \gamma_x (\mathbf{M})_x = (1, 0, \cdots, 0)$$

where $\chi = \{x \mid x \in (1, \cdots, m), \upsilon(x) \in \mu\}$, $(\mathbf{M})_x$ denotes the x-th row of $\mathbf{M}$. It is noteworthy that the Gaussian elimination can be used to compute coefficients $\{\gamma_x\}$ in the size of matrix $\mathbf{M}$ in polynomial time. And the coefficients are always 0 or 1 according to [36].

B. Asymmetric Prime-Order Bilinear Group

Definition 3 (Asymmetric Prime-Order Bilinear Group): Suppose that an algorithm $\mathcal{G}$ can generate asymmetric pairing groups. When taking a security parameter k as input, $\mathcal{G}$ computes (p, G, H, g, h, G_T, e). In the above parameters, G, G_T and H are cyclic groups of prime order p, g denotes the generator of group G while h denotes the generator of group H. A bilinear map is a function $e : G \times H \to G_T$ satisfies two properties:

- Bilinear: For any $a, b \in \mathbb{Z}_p$, $e(g^a, h^b) = e(g, h)^{ab}$.
- Non-Degenerate: For any $g_1 \in \mathbb{G}$ and $h_1 \in \mathbb{H}$, $e(g_1, h_1) \neq 1$.

C. Cryptographic Reverse Firewall

Definition 4 (Cryptographic Reverse Firewall (CRF)): The cryptographic reverse firewall is an algorithm with a state $\mathcal{W}$ which takes a massage and a state as input and outputs a message and the updated state. CRFs are deployed between user entities (e.g. vehicles) and the outside world. The state of $\mathcal{W}$ is implicitly omitted for simply writing. For an entity α and a CRF $\mathcal{W}$, we can define the composed party $\mathcal{W} \circ \alpha$. When the component α participates in a protocol, the system public parameter will be initialized as the state of $\mathcal{W}$, and $\mathcal{W}$ can be called the CRF of α if $\mathcal{W}$ is composed with α.

Definition 5 (Functionality-maintaining CRFs): For any CRF $\mathcal{W}$ and entity α, let $\mathcal{W}^1 \circ \alpha = \mathcal{W} \circ \alpha$. Concretely, $\mathcal{W}^k \circ \alpha = \mathcal{W} \circ (\mathcal{W}^{k-1} \circ \alpha)$ for $k \geq 2$. For any polynomial bounded $k \geq 1$ in scheme $\mathcal{P}$ with functionality $\mathcal{F}$, the reverse firewall is regarded as functionality-maintaining when the cooperation of $\mathcal{W}^k \circ \alpha$ maintains $\mathcal{F}$ for α in $\mathcal{P}$. That is to say,

$$(\mathcal{W}^k \circ \alpha = \mathcal{W} \circ \alpha) \cap (\mathcal{F}_{\mathcal{W}\circ\alpha} = \mathcal{F}_\alpha) = 1$$

Definition 6 (Weakly Security-preserving CRFs): For a CRF $\mathcal{W}$ and a protocol $\mathcal{P}$ that satisfies security requirement $\mathcal{S}$ with functionality $\mathcal{F}$, we can draw a conclusion that $\mathcal{W}$ weakly preserves the security requirement $\mathcal{S}$ if for any adversary $\hat{\alpha}$, the protocol $\mathcal{P}_{\alpha\Rightarrow\mathcal{W}\circ\hat{\alpha}}$ maintains the security requirement $\mathcal{S}$. Specifically, $\hat{\alpha}$ is used to represent the algorithm-substitution adversary who replaces the original entity α without changing the functionality $\mathcal{F}$. For a scheme

$$
\begin{aligned}
&\text{proc.LEAK}(\mathcal{P}, \alpha, \mathcal{J}, \mathcal{W}, \lambda) \\
&(\alpha_{\mathcal{A}}{}^*, \alpha_{\mathcal{B}}{}^*, I) \leftarrow \mathcal{A}(1^\lambda) \\
&b \xleftarrow{\$} \{0,1\} \\
&\text{IF } b = 1, \alpha^* \leftarrow \mathcal{W} \circ \alpha_{\mathcal{A}}{}^* \\
&\text{ELSE}, \alpha^* \leftarrow \mathcal{W} \circ \alpha \\
&\mathcal{T}^* \leftarrow \mathcal{P}_{\alpha \Rightarrow \alpha^*}^{\mathcal{J} \Rightarrow \alpha_{\mathcal{B}}{}^*}(I) \\
&b^* \leftarrow A(\mathcal{T}^*, \sigma_{\alpha_{\mathcal{B}}{}^*}) \\
&\text{OUTPUT}(b^* = b)
\end{aligned}
$$

Fig. 1. $LEAK(\mathcal{P}, \alpha, \mathcal{J}, \mathcal{W}, \lambda)$. Security game for a reverse firewall $\mathcal{W}$ of an entity α, which consists of $\mathcal{W}$, α, a protocol $\mathcal{P}$, an entity $\mathcal{J}$ which has been controlled by the adversary, and security parameters λ. Entities $\alpha_{\mathcal{A}}{}^*$ and $\alpha_{\mathcal{B}}{}^*$ are controlled from within by adversaries. I represents the valid input of $\mathcal{P}$ and $\sigma_{\alpha_{\mathcal{B}}{}^*}$ represents the status of $\alpha_{\mathcal{B}}^*$ after running the protocol. In polynomial time, $\alpha_{\mathcal{A}}{}^*$ can leak secret information to $\alpha_{\mathcal{B}}{}^*$.

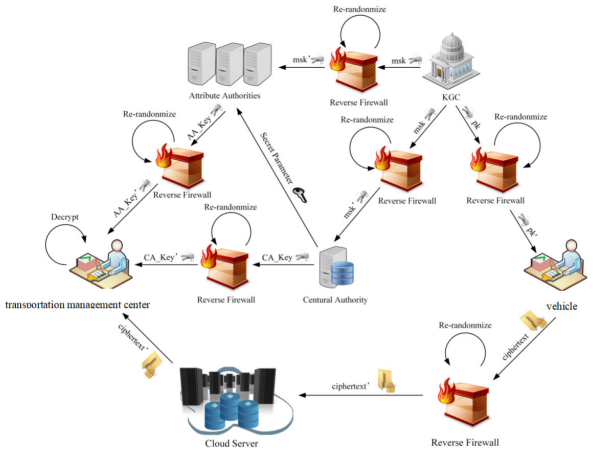

Fig. 2. System model.

$\mathcal{P}$ with an entity α, the protocol $\mathcal{P}_{\alpha \Rightarrow \hat{\alpha}}$ denotes that α is substituted by the algorithm-substitution adversary $\hat{\alpha}$.

Definition 7 (Weakly Exfiltration-resistant CRFs): A cryptographic reverse firewall is weakly exfiltration-resistant if no information will be leaked through the CRF even when the entity α is tampered. To be more specific, we can define weak exfiltration-resistance by a security game $LEAK$ shown in Fig. 1. For a CRF $\mathcal{W}$, we can draw the conclusion that it satisfies weak exfiltration-resistance if $\alpha_{\mathcal{B}}{}^*$ cannot distinguish whether the messages are from $\mathcal{W} \circ \alpha_{\mathcal{A}}{}^*$ or from the entity α which is working normally.

IV. Our Scheme

A. System Model

The entities involved in MA-CP-ABE-CRF are shown in Fig. 2.

- **Key Generation Center (KGC):** KGC is responsible for initializing system parameters to attribute authorities, the central authority and each transportation management center node.
- **Central Authority (CA):** CA is not only responsible for generating the central authority secret key, but also for sending authorization information which are essential for generating the attribute authority secret keys to each attribute authority.
- **Attribute Authorities (AAs):** AAs are responsible for generating the attribute authority secret keys under the attribute sets from nodes and the secret parameters from CA. It is worth noting that each AA has the capacity to independently perform this process for any vehicle nodes, and the introduction of multiple AAs greatly reduces the burden of CA during key generation.
- **Cryptographic Reverse Firewalls (CRFs):** CRFs in MA-CP-ABE-CRF are composed with four parts: $\mathcal{W}_{\mathsf{KGC}}$, $\mathcal{W}_{\mathsf{CA}}$, $\mathcal{W}_{\mathsf{AA}}$ and $\mathcal{W}_{\mathsf{V}}$. Specifically, $\mathcal{W}_{\mathsf{KGC}}$ is deployed to re-randomize the main secret key and the public keys from KGC in case the setup algorithm is compromised. $\mathcal{W}_{\mathsf{CA}}$ and $\mathcal{W}_{\mathsf{AA}}$ are deployed to re-randomize the central authority secret keys from CA and the attribute authority secret keys from AAs respectively in case the CA-KeyGen and AA-KeyGen algorithms are compromised. $\mathcal{W}_{\mathsf{V}}$ is reponsible for re-randomizing the ciphertext encrypted by specific vehicle nodes. The characteristics of CRF prevent original secrets (i.e. secret keys) stored in nodes or authorities from being obtained by the adversary even if they are compromised, because they have been re-randomized before being sent to the attacker.
- **Vehicle:** Vehicle node selects the access policy and utilizes the public keys to encrypt message locally under the selected policy, then uploading the encrypted data to the server for storage or directly sending it to the transportation management center node.
- **Cloud Server (optional):** Served as a transfer station for messages, cloud server, usually with strong performance, can provide store and forward for messages.
- **Transportation Management Center:** The transportation management center node is assigned to a private key generating by both CA and AAs. I can discretionarily received the ciphertext from data owner nodes or download interested ciphertext via the cloud server, and can only perform decryption when the attributes embedded in the secret key meet the requirements of the encrypted messages.

Specifically, our system works as the following steps:

During the setup phase, KGC initializes the system, generates public key PK and main secret key MSK. Then, KGC sends PK to all vehicle nodes, and sends MSK to CA and AAs. It should be noted that PK and MSK will be firstly sent to the cryptographic reverse firewall $\mathcal{W}_{\mathsf{KGC}}$, which will then send the re-randomized keys to other entities. After obtaining the public key, a specific vehicle node can perform encryption under chosen access structure. The ciphertext will be updated by reverse firewalls and then be transmitted to the cloud server. After the receipt of main secret key, CA will generate identity key (i.e. CA_key) for transportation management center, and authorize each attribute authority to generate the vehicle attribute keys (i.e. AA_key). After being authorized, AAs will generate the attribute authority secret key AA_key to help CA to undertake a part of the key generation. In fact, each attribute authority is responsible for a disjoint subset in attribute universe, while each vehicle node always

has multiple authorities. Thus, the authority secret key for a vehicle may be distributed by different AAs. Fortunately, the properties of multiple authorities prevent different AAs from conflicting when distributing attribute secret keys to the same vehicle node. Finally, a transportation management center node can correctly decrypt the ciphertext after obtaining CA_key and AA_key that satisfies the access structure embedded in the ciphertext. Similarly, CA_key and AA_key will be re-randomized by reverse firewalls $\mathcal{W}_{\mathsf{CA}}$ and $\mathcal{W}_{\mathsf{AA}}$.

B. Security Model

To protect data confidentiality, the proposed MA-CP-ABE-CRF system is supposed to achieve adaptively CPA-security. Moreover, the scheme should be able to resist algorithm substitution attacks (ASAs). Thus, two types of adversaries $\mathcal{A}_I$ and $\mathcal{A}_{II}$ should be taken into account respectively. The adversary $\mathcal{A}_I$ can perform chosen-plaintext attacks on the unmodified MA-CP-ABE system. Meanwhile, the adversary $\mathcal{A}_{II}$ can stealthily replace the Setup, CA-KeyGen, AA-KeyGen and Encrypt algorithms without changing the functionality. Next, the adaptive CPA security game between challenger $\mathcal{C}$ and $\mathcal{A}_I$ will be introduced. Besides, the security game between $\mathcal{C}$ and $\mathcal{A}_{II}$ will also be discussed to prove that our scheme is ASA-secure.

–**Game 1:** The adversary in this security game is $\mathcal{A}_I$ that can perform chosen-plaintext attacks.

- Setup: $\mathcal{C}$ calls the algorithm $Setup(1^k) \rightarrow (PK, MSK)$, then gives PK to $\mathcal{A}_I$.
- Phase 1: $\mathcal{A}_I$ can repeatedly queries with the attribute set S. $\mathcal{C}$ first runs $CA\text{-}KeyGen(MSK) \rightarrow CA\_key$ to obtain CA_key and two random parameters r_1 and r_2, then runs $AA\text{-}KeyGen(S, MSK, r_1, r_2) \rightarrow AA\_key$. Finally $\mathcal{C}$ returns CA_key and the corresponding AA_key to $\mathcal{A}_I$.
- Challenge: $\mathcal{A}_I$ submits two plaintexts M_0, M_1 with same length and an access structure $(\mathbf{M}, \upsilon)$. It is worth noting that all attribute sets queried during Phase 1 should not match with $(\mathbf{M}, \upsilon)$. Then, $\mathcal{C}$ randomly chooses $b \in \{0, 1\}$ and encrypts M_b. Finally, $\mathcal{C}$ sends the encrypted message CT to $\mathcal{A}_I$.
- Phase 2: $\mathcal{A}_I$ repeats Phase 1 as many times as $\mathcal{A}_I$ desires. Note that every S submitted by $\mathcal{A}_I$ must not satisfy the submitted $(\mathbf{M}, \upsilon)$.
- Guess: $\mathcal{A}_I$ guesses a bit $b' \in \{0, 1\}$. If $b' = b$, $\mathcal{A}_I$ wins the game.

Definition 8 (Adaptively CPA-secure): The MA-CP-ABE scheme is adaptively CPA-secure if for any polynomial time adversary, its advantage in breaking GAME-1 is negligible.

–**Game 2:** The adversary in this security game is $\mathcal{A}_{II}$.

- Init: $\mathcal{A}_{II}$ firstly selects the tampered algorithms $Setup^*, CAKeyGen^*, AAKeyGen^*$ and $Encrypt^*$ and submits them to $\mathcal{C}$. Then, $\mathcal{C}$ replaces the original algorithms with the tampered algorithms.
- Setup: $\mathcal{C}$ runs $Setup^*(1^k) \rightarrow (PK, MSK)$, and re-randomizes PK with $\mathcal{W}_{KGC} \cdot Setup$. Then, $\mathcal{C}$ sends the re-randomized PK' to $\mathcal{A}_{II}$.
- Phase 1: $\mathcal{A}_{II}$ can repeatedly queries with the attribute set S. The challenger $\mathcal{C}$ first calls $CA\text{-}KeyGen^*(MSK) \rightarrow CA\_key$ to obtain CA_key and two random parameters r_1 and r_2, then runs $AA\text{-}KeyGen^*(S, MSK, r_1, r_2) \rightarrow AA\_key$. After that, $\mathcal{C}$ runs $\mathcal{W}_{CA} \cdot CA\text{-}KeyGen(CA\_key) \rightarrow CA\_key'$ and $\mathcal{W}_{AA} \cdot AA\text{-}KeyGen(AA\_key) \rightarrow AA\_key'$ and transmits the re-randomized CA_key' and AA_key' to $\mathcal{A}_{II}$.
- Challenge: $\mathcal{A}_{II}$ submits two messages M_0, M_1 with same length and an access structure $(\mathbf{M}, \upsilon)$. It is worth noting that all attribute sets queried during Phase 1 should not match with $(\mathbf{M}, \upsilon)$. Then, $\mathcal{C}$ randomly picks $b \in \{0, 1\}$, encrypts M_b with $Encrypt^*$, and calls $\mathcal{W}_{DO} \cdot Encrypt$ to obtain re-randomized ciphertext CT'. Finally, $\mathcal{C}$ sends CT' to $\mathcal{A}_{II}$.
- Phase 2: $\mathcal{A}_{II}$ repeats Phase 1 as many times as $\mathcal{A}_{II}$ desires. Note that every S submitted by $\mathcal{A}_{II}$ does not satisfy the aforementioned $(\mathbf{M}, \upsilon)$.
- Guess: $\mathcal{A}_{II}$ guesses a bit $b' \in \{0, 1\}$. If $b' = b$, $\mathcal{A}_{II}$ wins the game.

Definition 9 (ASA-secure): A MA-CP-ABE-CRF scheme can resist exfiltration attack if for any polynomial time adversary, its advantage in breaking GAME-2 is negligible.

C. Construction

The proposed algorithm can be described as follows.

1) Setup: The setup algorithm is capable to generate public key pk and main secret key msk. Suppose that k is the security parameter, KGC executes the algorithm as follows.

a) run $\mathcal{G}(k)$ to obtain $(p, g, \mathbb{G}, h, \mathbb{H}, \mathbb{G}_T, e)$
b) randomly pick $d_1, d_2, d_3 \leftarrow_R \mathbb{Z}_p$ and $a_1, a_2, b_1, b_2 \leftarrow_R$
c) choose hash functions: $\mathcal{H} : \{0, 1\}^* \rightarrow \mathbb{G}$
d) compute $H_1 = h^{a_1}$, $H_2 = h^{a_2}$, $T_1 = e(g, h)^{d_1 a_1 + d_3}$, $T_2 = e(g, h)^{d_2 a_2 + d_3}$

Output the public key $pk = (h, H_1, H_2, T_1, T_2)$, the main secret key $msk = \left(g, h, a_1, a_2, b_1, b_2, g^{d_1}, g^{d_2}, g^{d_3}\right)$.

2) $\mathcal{W}_{KGC}$·Setup: After receiving msk and pk, the reverse firewall $\mathcal{W}_{\mathsf{KGC}}$ executes the algorithm as follows.

a) randomly pick $a, c, \hat{a}_1, \hat{a}_2, \hat{b}_1, \hat{b}_2, \hat{d}_1, \hat{d}_2, \hat{d}_3, \leftarrow \mathbb{Z}_p$
b) compute $g' = g^a$, $h' = h^c$
c) compute $a'_1 = a_1 + \hat{a}_1$, $a'_2 = a_2 + \hat{a}_2$, $b'_1 = b_1 + \hat{b_1}$, $b'_2 = b_2 + \hat{b_2}$
d) compute $d'_1 = d_1 + \hat{d}_1$, $d'_2 = d_2 + \hat{d}_2$, $d'_3 = d_3 + \hat{d}_3$
e) compute $H'_1 = h'^{a'_1}$, $H'_2 = h'^{a'_2}$, $T'_1 = e(g', h')^{d'_1 a'_1 + d'_3}$, $T'_2 = e(g', h')^{d'_2 a'_2 + d'_3}$

The reverse firewall $\mathcal{W}_{\mathsf{KGC}}$ outputs the updated public key $pk' = \left(h', H'_1, H'_2, T'_1, T'_2\right)$ and the updated main secret key $msk' = \left(g', h', a'_1, a'_2, b'_1, b'_2, g'^{d'_1}, g'^{d'_2}, g'^{d'_3}\right)$, then broadcasts pk' and sends msk' to the central authority and the attribute authorities.

3) CA-KeyGen: After receiving msk, the central authority executes the algorithm as follows.

a) randomly pick $r_1, r_2, \sigma' \leftarrow_R \mathbb{Z}_p$
b) compute $sk_0 = (sk_{0,1}, s\ k_{0,2}, s\ k_{0,3}) = (h^{b_1 r_1}, h^{b_2 r_2}, h^{r_1 + r_2})$
c) for $\eta = 1, 2$, compute $\bar{sk}_\eta = g^{d_\eta} \cdot \mathcal{H}(011\eta)^{\frac{b_1 r_1}{a_\eta}} \cdot \mathcal{H}(012\eta)^{\frac{b_2 r_2}{a_\eta}} \cdot \mathcal{H}(013\eta)^{\frac{r_1 + r_2}{a_\eta}} \cdot g^{\frac{\sigma'}{a_\eta}}$

d) compute $\bar{sk}_3 = g^{d_3} \cdot g^{-\sigma'}$
e) set $\bar{sk} = (\bar{sk}_1, \bar{sk}_2, \bar{sk}_3)$

Output the central authority secret key $CA\_key = \left(sk_0, \bar{sk}\right)$.

4) $\mathcal{W}_{CA}$· CA-KeyGen: After receiving the central authority secret key CA_key, the reverse firewall $\mathcal{W}_{CA}$ executes the algorithm as follows.

a) randomly pick $\sigma'', \eta_1, \eta_2, \eta_3 \leftarrow_R \mathbb{Z}_p$
b) compute $sk'_0 = (sk'_{0,1}, s\ k'_{0,2}, s\ k'_{0,3}) = (sk_{0,1}^{\eta_1}, s\ k_{0,2}^{\eta_2}, sk_{0,3}^{\eta_3})$
c) for $\eta = 1, 2$, compute $\bar{sk}'_\eta = \bar{sk}_\eta \cdot g^{\frac{\sigma''}{a_\eta}}$
d) compute $\bar{sk}'_3 = \bar{sk}_3 \cdot g^{-\sigma''}$
e) compute $\bar{sk}' = (\bar{sk}'_1, \bar{sk}'_2, \bar{sk}'_3)$

The reverse firewall $\mathcal{W}_{CA}$ outputs the updated central authority secret key $CA\_key' = \left(sk'_0, \bar{sk}'\right)$.

5) AA-KeyGen: After receiving msk, two secret parameters r_1, r_2, and the attribute set S, the attribute authority executes the algorithm as follows.

a) for each y in S, randomly pick $\sigma_y \leftarrow_R \mathbb{Z}_p$
for $\eta = 1, 2$, compute $sk_{y,\eta} = \mathcal{H}(y1\eta)^{\frac{b_1 r_1}{a_\eta}} \cdot \mathcal{H}(y2\eta)^{\frac{b_2 r_2}{a_\eta}} \cdot \mathcal{H}(y3\eta)^{\frac{r_1+r_2}{a_\eta}} \cdot g^{\frac{\sigma_y}{a_\eta}}$
b) compute $sk_{y,3} = g^{-\sigma_y}$
c) set $sk_y = \left(sk_{y,1}, sk_{y,2}, sk_{y,3}\right)$

Output the attribute authority secret key $AA\_key = \left\{sk_y\right\}_{y \in S}$.

6) $\mathcal{W}_{AA}$·AA-KeyGen: After receiving AA_key, the reverse firewall $\mathcal{W}_{AA}$ executes the algorithm as follows.

a) for each y in S, randomly pick $\sigma'_y \leftarrow_R \mathbb{Z}_p$
for $\eta = 1, 2$, compute $sk'_{y,\eta} = sk_{y,\eta} \cdot g^{\frac{\sigma'_y}{a_\eta}}$
b) compute $sk'_{y,3} = sk_{y,3} \cdot g^{-\sigma'_y}$
c) set $sk'_y = (sk'_{y,1}, sk'_{y,2}, sk'_{y,3})$

Output the updated $AA\_key' = \{sk'_y\}_{y \in S}$.

7) Encrypt: This algorithm uses pk, a plaintext msg and an access structure $(\mathbf{M}, \upsilon)$ as input, where $\mathbf{M}$ has n_1 rows and n_2 columns. Then, the vehicle node executes the algorithm as follows.

a) randomly pick $s_1, s_2 \leftarrow_R \mathbb{Z}_p$
b) compute $ct_0 = \left(H_1^{s_1}, H_2^{s_2}, h^{s_1+s_2}\right)$
c) for $x = 1, \ldots, n_1$ and $\rho = 1, 2, 3$
compute $ct_{x,\rho} = \mathcal{H}(\upsilon(x)\rho 1)^{s_1} \cdot \mathcal{H}(\upsilon(x)\rho 2)^{s_2} \cdot \prod_{y=1}^{n_2} \left[\mathcal{H}(0y\rho 1)^{s_1} \cdot \mathcal{H}(0y\rho 2)^{s_2}\right]^{(\mathbf{M})_{x,y}}$
set $ct_x = \left(ct_{x,1}, ct_{x,2}, ct_{x,3}\right)$
d) set $\bar{ct} = T_1^{s_1} \cdot T_2^{s_2} \cdot msg$

Output the ciphertext $ct = \left(ct_0, ct_1, ct_2, \ldots, ct_{n_1}, \bar{ct}\right)$.

8) $\mathcal{W}_V$·Encrypt: After receiving the ciphertext $ct = \left(ct_0, ct_1, \ldots, ct_{n_1}, \bar{ct}\right)$, the reverse firewall $\mathcal{W}_V$ executes the algorithm as follows.

a) run the Extended Euclidean algorithm to obtain $\eta_4, \eta_5, \eta_6 \leftarrow_R \mathbb{Z}_p$, where $\eta_1\eta_4 = 1$, $\eta_2\eta_5 = 1$, $\eta_3\eta_6 = 1$
b) for $x = 1, \ldots, n_1$, compute $ct'_x = \left(ct_{x,1}^{\eta_4}, ct_{x,2}^{\eta_5}, ct_{x,3}^{\eta_6}\right)$

The reverse firewall $\mathcal{W}_V$ outputs the updated $ct' = \left(ct_0, ct'_1, \ldots, ct'_{n_1}, \bar{ct}\right)$, and transmits it to the transportation management center.

9) Decrypt: The algorithm takes pk, a ciphertext ct, the central authority secret key $CA\_key = \left(sk_0, \bar{sk}\right)$ and the attribute authority secret key $AA\_key = \left\{sk_y\right\}_{y \in S}$ as input. If the attribute set in AA_key satisfies $MSP(\mathbf{M}, \upsilon)$ in ct, the constants $\{\gamma_x\}_{x \in \chi}$ which defined in preliminary can be computed. Then, the transportation management center executes the algorithm as follows.

a) compute $D_1 = \bar{ct} \cdot \prod_{\rho=1}^{3} e(\prod_{x \in \chi} ct_{x,\rho}^{\gamma_x}, sk_{0,\rho})$
b) compute $D_2 = \prod_{\rho=1}^{3} e(\bar{sk}_\rho \cdot \prod_{x \in \chi} sk_{\upsilon(x),\rho}^{\gamma_x}, ct_{0,\rho})$
c) compute $msg = D_1 / D_2$

Output the message msg.

V. Security Analysis

A. Correctness Analysis

The correctness of original decryption procedure will be firstly verified. After receiving the ciphertext $ct = \left(ct_0, ct_1, \ldots, ct_{n_1}, \bar{ct}\right)$, the node decrypts the ciphertext using the attribute authority secret key $AA\_key = \{sk_y\}_{y \in S}$ and the central authority secret key $CA\_key = \left(sk_0, \bar{sk}\right)$ as follows. When S is accepted by a pair $(\mathbf{M}, \upsilon)$, there will exist the coefficients $\{\gamma_x\}_{x \in \chi}$ as in Section III. For $\rho = 1, 2, 3$:

$$\begin{aligned}
\prod_{x \in \chi} \mathrm{ct}_{x,\rho}^{\gamma_x} &= \prod_{x \in \chi} \Bigg(\mathcal{H}(\upsilon(x)||\rho||1)^{\gamma_x s_1} \cdot \mathcal{H}(\upsilon(x)||\rho||2)^{\gamma_x s_2} \cdot \\
&\quad \cdot \prod_{y=1}^{n_2} \left[\mathcal{H}(0y\rho 1)^{s_1} \cdot \mathcal{H}(0y\rho 2)^{s_2}\right]^{\gamma_x (\mathbf{M})_{x,y}} \Bigg) \\
&= \left(\prod_{x \in \chi} \mathcal{H}(\upsilon(x)||\rho 1)^{\gamma_x s_1} \cdot \mathcal{H}(\upsilon(x)||\rho 2)^{\gamma_x s_2} \right) \\
&\quad \cdot \left(\prod_{y=1}^{n_2} [\mathcal{H}(0y\rho 1)^{s_1} \cdot \mathcal{H}(0y\rho 2)^{s_2}]^{\sum_{x \in \chi} \gamma_x (\mathbf{M})_{x,y}} \right) \\
&= \left(\prod_{x \in \chi} \mathcal{H}(\upsilon(x)\rho 1)^{\gamma_x s_1} \cdot \mathcal{H}(\upsilon(x)\rho 2)^{\gamma_x s_2} \right) \\
&\quad \cdot \mathcal{H}(01\rho 1)^{s_1} \cdot \mathcal{H}(01\rho 2)^{s_2}
\end{aligned}$$

Bringing the intermediate result above, D_1 can be simplified:

$$\begin{aligned}
D_1 &= \bar{ct} \cdot \prod_{\rho=1}^{3} e(\prod_{x \in \chi} ct_{x,\rho}^{\gamma_x}, sk_{0,\rho}) \\
&= \bar{ct} \cdot \prod_{\rho=1}^{3} e\Bigg(\Bigg(\prod_{x \in \chi} \mathcal{H}(\upsilon(x)||\rho||1)^{\gamma_x s_1} \cdot \mathcal{H}(\upsilon(x)||\rho||2)^{\gamma_x s_2} \Bigg) \\
&\quad \cdot \mathcal{H}(01\rho 1)^{s_1} \cdot \mathcal{H}(01\rho 2)^{s_2}, sk_{0,\rho} \Bigg) \\
&= \bar{ct} \cdot \prod_{\eta \in \{1,2\}} \Bigg[e(\mathcal{H}(011\eta), h)^{b_1 r_1 s_\eta} \\
&\quad \cdot e(\mathcal{H}(012\eta), h)^{b_2 r_2 s_\eta} \\
&\quad \cdot e(\mathcal{H}(013\eta), h)^{(r_1+r_2) s_\eta} \\
&\quad \cdot \prod_{x \in \chi} \Bigg(e\left(\mathcal{H}(\upsilon(x)||1\eta)^{\gamma_x}, h\right)^{b_1 r_1 s_\eta}
\end{aligned}$$

$$\cdot e\left(\mathcal{H}(\upsilon(x)||2\eta)^{\gamma_x}, h\right)^{b_2 r_2 s_\eta} \cdot e\left(\mathcal{H}(\upsilon(x)||3\eta)^{\gamma_x}, h\right)^{(r_1+r_2)s_\eta}\Big)\Big]$$

$$D_2 = \prod_{\rho=1}^{3} e(s\bar{k}_\rho \cdot \prod_{x\in\chi} sk_{\upsilon(x),\rho}^{\gamma_x}, ct_{0,\rho})$$

$$= \prod_{\eta\in\{1,2\}} \Big[e(\mathcal{H}(011\eta), h)^{b_1 r_1 s_\eta} \cdot e(\mathcal{H}(012\eta), h)^{b_2 r_2 s_\eta} \cdot e(\mathcal{H}(013\eta), h)^{(r_1+r_2)s_\eta} \cdot \prod_{x\in\chi}\Big(e\left(\mathcal{H}(\upsilon(x)||1\eta)^{\gamma_x}, h\right)^{b_1 r_1 s_\eta} \cdot e\left(\mathcal{H}(\upsilon(x)||2\eta)^{\gamma_x}, h\right)^{b_2 r_2 s_\eta} \cdot e\left(\mathcal{H}(\upsilon(x)||3\eta)^{\gamma_x}, h\right)^{(r_1+r_2)s_\eta}\Big)\Big] \cdot e(g,h)^{d_1 a_1 s_1 + d_2 a_2 s_2 + d_3(s_1+s_2)}$$

Thus, the plaintext msg can be recovered as:

$$msg = D_1/D_2 = \bar{ct}/e(g,h)^{d_1 a_1 s_1 + d_2 a_2 s_2 + d_3(s_1+s_2)}$$

B. Security Strength

The security strength will be discussed as follows: First, the adaptive CPA security of the original scheme will be proved. Next, the MA-CP-ABE-CRF scheme will be further proved to be ASA-secure(i.e. functionality maintaining, security preservation and exfiltration resistance).

Theorem 1 (Adaptively CPA-secure): In case that the scheme FAME proposed in [37] is adaptively CPA-secure, then the proposed MA-CP-ABE scheme is also adaptively CPA-secure.

Proof: Suppose there is an adversary $\mathcal{A}_I$ who can win GAME-1 at a non-negligible advantage. On this basis, an algorithm $\mathcal{B}$ which is able to break the adaptive CPA-security of FAME [37] at a non-negligible advantage can be constructed.

Let $\mathcal{C}$ to be the challenger of $\mathcal{B}$ in the security model of FAME. $\mathcal{B}$ takes advantage of $\mathcal{A}_I$ to challenge $\mathcal{C}$ in the next few steps:

- Init: $\mathcal{C}$ runs $FAME.Setup(1^k) \rightarrow (PK, MSK)$ and sends $PK = (h, H_1, H_2, T_1, T_2)$ to $\mathcal{B}$.
- Setup: $\mathcal{B}$ sends $PK = (h, H_1, H_2, T_1, T_2)$ to the adversary $\mathcal{A}_I$
- Phase 1: $\mathcal{A}_I$ can repeatedly queries with a set of attributes S to $\mathcal{B}$. $\mathcal{B}$ calls $KeyGen(MSK, S) \rightarrow SK = (sk_0, \{sk_y\}_{y\in S}, sk')$ of $\mathcal{C}$ to obtain the secret key. Then, $\mathcal{B}$ returns $CA\_key = (sk_0, sk')$ and $AA\_key = \{sk_y\}_{y\in S}$ to $\mathcal{A}_I$.
- Challenge: $\mathcal{A}_I$ submits two plaintexts M_0, M_1 with same length and an access structure $(\mathbf{M}, \upsilon)$ to $\mathcal{B}$. $\mathcal{B}$ transmits M_0, M_1 and $(\mathbf{M}, \upsilon)$ to $\mathcal{C}$. $\mathcal{C}$ randomly picks $b \in \{0,1\}$, and runs $FAME.Encrypt(M_b)$ to generate ciphertext CT. Finally, $\mathcal{C}$ returns CT to $\mathcal{B}$ and $\mathcal{B}$ transmits CT to $\mathcal{A}_I$.
- Phase 2: $\mathcal{A}_I$ repeats Phase 1 as many times as $\mathcal{A}_I$ desires, and $\mathcal{B}$ responds the queries as in Phase 1.
- Guess: $\mathcal{A}_I$ outputs a guess bit $b' \in \{0,1\}$. $\mathcal{B}$ also takes b' as its output to $\mathcal{C}$.

Obviously, after receiving a respond, $\mathcal{A}_I$ is unable to distinguish whether it is from $\mathcal{B}$ or from its corresponding challenger. Therefore, $\mathcal{B}$ has properly simulated the challenger. Thus, if $\mathcal{A}_I$ has a non-negligible advantage in breaking GAME-1, $\mathcal{B}$ can break the IND-CPA game of FAME [37] at a non-negligible advantage, which is contrary to the conclusion proved in [37].

Theorem 2 (Functionality Maintaining): The CRF in our system is functionality maintaining, which means the functionality and security of the original MA-CP-ABE scheme will not be affected by the deployment of CRF.

Proof: The vehicle node executes the $Encrypt$ algorithm under the updated public key pk', and then sends the generated ciphertext $ct = \left(ct_0, ct_1, \ldots, ct_{n_1}, \bar{ct}\right)$ to CRF. To generate the re-randomized ciphertext $ct' = \left(ct_0, ct'_1, \ldots, ct'_{n_1}, \bar{ct}\right)$, CRF executes the $\mathcal{W}_{DO} \cdot Encrypt$ algorithm and then sends ct' to the cloud server. When the transportation management center node intends to obtain the message, it will download the data without going through the CRF.

The correctness of decryption will be verified by the attribute authority secret key $AA\_key' = \{sk'_y\}_{y\in S}$, the central authority secret key $CA\_key' = \left(sk'_0, s\bar{k}'\right)$ and the ciphertext ct':

$$D_1{}' = \bar{ct} \cdot \prod_{\rho=1}^{3} e(\prod_{x\in\chi} ct'^{\gamma_x}_{x,\rho}, sk'_{0,\rho}) = \bar{ct} \cdot \prod_{\rho=1}^{3} e(\prod_{x\in\chi} ct^{\gamma_x \eta_\rho}_{x,\rho}, sk^{-\eta_\rho}_{0,\rho}) = \bar{ct} \cdot \prod_{\rho=1}^{3} e(\prod_{x\in\chi} ct^{\gamma_x}_{x,\rho}, sk_{0,\rho})$$

$$D_2{}' = \prod_{\rho=1}^{3} e(s\bar{k}'_\rho \cdot \prod_{x\in\chi} sk'^{\gamma_x}_{\upsilon(x),\rho}, ct_{0,\rho}) = [\prod_{\rho=1}^{2} e(s\bar{k}_\rho \cdot g^{\frac{\sigma''}{a'_\rho}} \cdot \prod_{x\in\chi} (sk_{\upsilon(x),\rho} \cdot g^{\frac{\sigma'_{\upsilon(x)}}{a'_\rho}})^{\gamma_x}, h'^{a'_\rho s_\rho})] \cdot e(sk'_3 \cdot g^{-\sigma''} \cdot \prod_{x\in\chi} (sk_{\upsilon(x),3} \cdot g^{-\sigma'_{\upsilon(x)}})^{\gamma_x}, h'^{s_1+s_2}) = \prod_{\rho=1}^{3} e(s\bar{k}_\rho \cdot \prod_{x\in\chi} sk^{\gamma_x}_{\upsilon(x),\rho}, ct_{0,\rho})$$

Therefore, $D_1{}'$ and $D_2{}'$ are verified to be equal with the original equation, and the plaintext msg could be recovered by calculating D'_1/D'_2.

Theorem 3 (Weak Security Preservation and Exfiltration Resistance:) The CRF in MA-CP-ABE-CRF is weak security preservation and exfiltration resistance. The former property means that for any algorithm-substitution attackers $\hat{\alpha}$, the protocol $\mathcal{P}_{\alpha\Rightarrow\mathcal{W}\circ\hat{\alpha}}$ will still keep the original security. The

latter property means that any comportment to obtain private information by falsifying or divulging the information will be prevented by CRF.

Proof: For any algorithm-substitution attacks on the KGC, the central authority, the attribute authorities and the transportation management center, the original algorithm would be replaced with tampered algorithm $Setup^*$, CA_KeyGen^*, AA_KeyGen^* and $Encrypt^*$ as game $LEAK$ (see Fig. 1). The indistinguishability between the basic security game of the original scheme and MA-CP-ABE-CRF scheme will be verified, and then the CRF can be proved to satisfy the weak security preservation and exfiltration resistance properties. To complete the proof, the following security games are constructed:

–**Game 3:** Identical to **Game 2** in section IV.

–**Game 4:** Identical to **Game 3** except that PK, MSK are generated by $Setup$ algorithm instead of $Setup^*$ and $\mathcal{W}_{KGC} \cdot Setup$ during the setup phase.

–**Game 5:** Identical to **Game 4** except that AA_key and CA_key are generated by $AA\text{-}KeyGen$ and $CA\text{-}KeyGen$ instead of $AA\text{-}KeyGen^*, \mathcal{W}_{AA} \cdot AA\text{-}KeyGen, CA\text{-}KeyGen^*$ and $\mathcal{W}_{CA} \cdot CA\text{-}KeyGen$ when generating the secret key.

–**Game 6:** Identical to **Game 5** except that the challenge ciphertext CT is generated by $Encrypt$ instead of $Encrypt^*$ and $\mathcal{W}_{\mathsf{DO}} \cdot Encrypt$ during the challenge phase. It is easy to observe that, **Game 6** is identical to **Game 1** in section IV(i.e. the security game of the original MA-CP-ABE scheme).

Next, we will prove the indistinguishability between **Game 3** and **Game 4**, **Game 4** and **Game 5**, **Game 5** and **Game 6**, respectively.

For Game 3 and Game 4, regardless of any tempered algorithm $Setup^*$, the generated pk and msk would be re-randomized by the CRF in $\mathcal{W}_{\mathsf{KGC}} \cdot Setup$ algorithm. Due to the scalability of data, the updated keys will be redistributed and mapped to the uniform output space as original $Setup$ algorithm. Thus, even if the implementation of $Setup$ algorithm is falsified, it is virtually impossible for an adversary to distinguish whether the key is generated by $Setup$ algorithm or $Setup^*$ and $\mathcal{W}_{\mathsf{KGC}} \cdot Setup$ algorithms. Thus, Game 3 and Game 4 is indistinguishable.

Between Game 4 and Game 5, regardless of any tempered algorithms $AA\text{-}KeyGen^*$ and $CA\text{-}KeyGen^*$, the generated attribute authority secret key and central authority secret key will be re-randomized by the CRF in $\mathcal{W}_{\mathsf{AA}} \cdot AA\text{-}KeyGen$ and $\mathcal{W}_{\mathsf{CA}} \cdot CA\text{-}KeyGen$ algorithms. Due to the scalability of data, the updated keys will be redistributed and mapped to the uniform output space as original $AA\text{-}KeyGen$ and $CA\text{-}KeyGen$ algorithms. Thus, even if the implementation of $AA\text{-}KeyGen$ and $CA\text{-}KeyGen$ is falsified, it is virtually impossible for an adversary to distinguish whether the key is generated by $AA\text{-}KeyGen$ and $CA\text{-}KeyGen$ or $AA\text{-}KeyGen^*, \mathcal{W}_{\mathsf{AA}} \cdot AA\text{-}KeyGen, CA\text{-}KeyGen^*$ and $\mathcal{W}_{\mathsf{CA}} \cdot CA\text{-}KeyGen$. Thus, Game 4 and Game 5 is indistinguishable.

The indistinguishability between Game 5 and Game 6 can be proved similarly. For any tempered algorithm $Encrypt^*$, the generated challenge ciphertext will be re-randomized by the CRF in $\mathcal{W}_{\mathsf{DO}} \cdot Encrypt$ algorithm. Due to the scalability of data, the updated ciphertext will be redistributed and mapped to the uniform output space as original $Encrypt$ algorithm. Thus, even if the implementation of $Encrypt$ algorithm is falsified, it is virtually impossible for an adversary to distinguish whether the ciphertext is generated by $Encrypt$ algorithm or $Encrypt^*$ and $\mathcal{W}_{\mathsf{DO}} \cdot Encrypt$ algorithms. Thus, Game 5 and Game 6 is indistinguishable.

In conclusion, Game 3 and Game 6 are indistinguishable, therefore MA-CP-ABE-CRF keeps the identically adaptive CPA security as the original scheme, which proves that the CRFs for KGC, central authority, attribute authorities and vehicle are weakly security-preserving. The indistinguishability of Game 3, Game 4, Game 5 and Game 6 demonstrates that the CRFs are weakly exfiltration-resistant.

VI. Peformance Evaluation

To prove that our MA-CP-ABE-CRF system is not only more secure, but also more efficient and more flexible in the case of a distributed system with limited resources such as IoV, the comparison between the proposed approach as well as 4 latest state-of-the-art schemes(e.g., MABKS [11], HCMACP-ABE [12], RAAC [13], COO-CP-ABE-CRF [17]) has been carefully conducted from the perspectives of properties and performance.

A. Theoretical Analysis

The properties comparison between the proposed scheme and existing schemes is presented in TABLE I. The scheme suggested in [11] proposes an ABE system that supports keyword search, malicious AAs tracing and attribute update. The work proposed in [12] presents an efficient multi-authority CP-ABE system without central authority, which can realize fine-grained access control. The system RAAC involved in [13] allows users to trace the misbehavior of a particular AA. ABE scheme featured with online/offline encryption and cryptographic reverse firewalls is considered in [17]. Among these schemes, the work in [17] is designed for single-authority scenario, while [11], [12], [13] and the proposed approach are designed for multi-authority scenario in order to eliminate the single-point performance bottleneck. Only the proposed scheme is constructed based on the asymmetric pairings, and thus, improving the efficiency significantly. Besides, schemes in [11], [12], [13], and [17] are built on the LSSS access structure while the MSP are incorporated in our scheme in order to accommodate more expressive and complex access structures. Moreover, only our scheme and the scheme [12] achieve adaptive security, unfortunately, which is not the case of the schemes in [11], [13], and [17]. What's more, only the proposed scheme and scheme in [17] are proved to be exfiltration-resistant under the deployment of reverse firewalls, which can prevent tampered machines from leaking secret information.

In TABLE II, the computation cost of our MA-CP-ABE-CRF with the four prior schemes is compared. During the Setup phase, the computation cost in HCMACP-ABE [12], RAAC [13], COO-CP-ABE-CRF [17] and our system is constant while that in the scheme proposed in [11] is linearly

TABLE I
COMPARISON OF PROPERTIES IN DIFFERENT SCHEMES

Scheme	Policy	Security	Multi-Authority	Asymmetric Pairing	Exfiltration Resistance	Access Structure	Access Control
[11]	CP-ABE	Selectively	✓	×	×	LSSS	Attribute-Level
[12]	CP-ABE	Adaptively	✓	×	×	LSSS	Attribute-Level
[13]	CP-ABE	Selectively	✓	×	×	LSSS	Attribute-Level
[17]	CP-ABE	Selectively	×	×	✓	LSSS	Attribute-Level
Ours	MA-CP-ABE-CRF	Adaptively	✓	✓	✓	MSP	Attribute-Level

TABLE II
COMPARISON OF COMPUTATION COST IN DIFFERENT CP-ABE SCHEMES

Scheme	Setup	CA-KeyGenerate	AA-KeyGenerate	Encryption	Decryption
[11]	$(3+i)T'_G + T'_{GT} + T'_p$	$(5i+8)T'_G$	\	$(4n+3)T'_G + 2T'_{GT} + T'_p$	$(2i+1)T'_p + iT'_{GT}$
[12]	$2T'_G + T'_{GT} + T'_p$	\	$2iT'_G$	$(3n+1)T'_G + T'_{GT}$	$(2i+1)T'_p + iT'_{GT}$
[13]	$T'_G + T'_{GT} + T'_p$	$(4i+4)T'_G$	$2iT'_G$	$(3n+1)T'_G + T'_{GT}$	$(2i+1)T'_p + iT'_{GT}$
[17]	$T'_{GT} + T'_p$	\	\	$(5n+1)T'_G + T'_{GT}$	$(3i+1)T'_p + (i+1)T'_{GT}$
Ours	$3T_G + 2T_{GT} + 2T_p + 2T_H$	$9T_G + 3T_H$	$5iT_G$	$(9nn_2+6n)T_G + 2T_{GT} + 3T_H$	$6T_p + 6iT_G$

† T_p: pairing operation of asymmetric prime-order bilinear groups; T_G, T_H, T_{GT}: exponentiation operation of pairings in asymmetric prime-order bilinear groups $\mathbb{G}, \mathbb{H} and \mathbb{G}_T$ respectively; T'_p: pairing operation of symmetric prime-order bilinear groups; T'_G, T'_{GT}: exponentiation operation of pairings in symmetric prime-order bilinear groups $\mathbb{G}'$ and $\mathbb{G}'_T$ respectively; n: number of rows in a MSP matrix(i.e. attribute quantity); n_2: the number of columns in a MSP matrix; i: the size of the attribute set.

TABLE III
COMPARISON OF COMMUNICATION COST IN DIFFERENT CP-ABE SCHEMES

Scheme	Public Parameters	CA-Key	AA-Key	Ciphertext
[11]	$(i+6)\|\mathbb{G}'\| + \|\mathbb{G}'_T\|$	$\|\mathbb{Z}_p\|$	$(3i+4)\|\mathbb{G}'\|$	$(3n+3)\|\mathbb{G}'\| + 2\|\mathbb{G}'_T\|$
[12]	$3\|\mathbb{G}'\| + \|\mathbb{G}'_T\|$	$(i+1)\|\mathbb{G}'\|$	\	$(2n+1)\|\mathbb{G}'\| + \|\mathbb{G}'_T\|$
[13]	$(i+2)\|\mathbb{G}'\| + \|\mathbb{G}'_T\|$	$2i\|\mathbb{G}'\|$	$(2i+2)\|\mathbb{G}'\|$	$(2n+1)\|\mathbb{G}'\| + \|\mathbb{G}'_T\|$
[17]	$5\|\mathbb{G}'\| + \|\mathbb{G}'_T\|$	\	\	$(3n+1)\|\mathbb{G}'\| + \|\mathbb{G}'_T\|$
Ours	$3\|\mathbb{H}\| + 2\|\mathbb{G}_T\|$	$3i\|\mathbb{G}\|$	$3\|\mathbb{H}\| + 3\|\mathbb{G}\|$	$3n\|\mathbb{G}\| + \|\mathbb{G}_T\| + 3\|\mathbb{H}\|$

† $|\mathbb{Z}_p|$: length of elements in $\mathbb{Z}_p$; $|\mathbb{G}'|, |\mathbb{G}'_T|$: length of elements in symmetric prime-order bilinear groups $\mathbb{G}' and \mathbb{G}'_T$ respectively; $|\mathbb{G}|, |\mathbb{H}|, |\mathbb{G}_T|$: length of elements in asymmetric prime-order bilinear groups $\mathbb{G}, \mathbb{H}$ and $\mathbb{G}_T$ respectively; n: number of rows in a MSP matrix(i.e. attribute quantity); i: the size of the attribute set.

dependent on variable size i of attribute sets. Compared with the MABKS scheme [11], our system remains low computation cost when the size of attribute sets is large. Meanwhile, compared with the schemes suggested in [12], [13], and [17], our MA-CP-ABE-CRF scheme does not incur much extra cost. Furthermore, asymmetric groups, which greatly improve the performance, are used only in our scheme. To sum up, the computation cost during the Setup phase of our scheme is acceptable. As for CA-KeyGenerate, our scheme is obviously superior to [11] and [13] since the computation cost in aforementioned two schemes is linear with the size of attribute sets. In AA-KeyGenerate, Encryption and Decryption phases, the exponent operation and pairing operation of our proposed scheme are faster due to smaller elements in asymmetric pairing groups, resulting in higher efficiency. It is worth noticing that the executing time of AA_key generation of the scheme in [11] is not taken into account for the reason that it randomly chooses AA_key in negligible time. To summarize, the proposed scheme is obviously more efficient, making it more applicable for IoV.

TABLE III lists the communication cost in detail. As the same reason mentioned in computation cost analysis, the proposed system is more efficient than prior systems in communication cost of Public Parameters and CA_key. As for AA_key, the MA-CP-ABE-CRF scheme gets a better performance than HCMACP-ABE [12] and RAAC [13] because the length of an element in asymmetric pairing groups is smaller than that in symmetric pairing groups at equivalent security levels. With the same reason, our system shows an advantage over other systems in communication cost of Ciphertext. In general, the proposed system achieves the reduction of computation and communication cost, which makes it suited for nodes in IoV, which have limited resources.

B. Experimental Analysis

To further evaluate the performance of our scheme as well as existing works presented in [11], [12], [13], and [17], experimental performance comparison is also provided. It should be emphasized that we only aim to highlight the performance improvement of the proposed MA-CP-ABE scheme compared to existing works, so the comparison with the CRF schemes is omitted. Specifically, the experiments are operated in a platform equipped with Intel Core i5-8400H@2.80GHz Processor with 16GB of memory, and the PBC library is used to initialize the parameters.

In Figs. 3a and 3b, the performance of system initialization in our system is approximate to that in existing schemes [12],

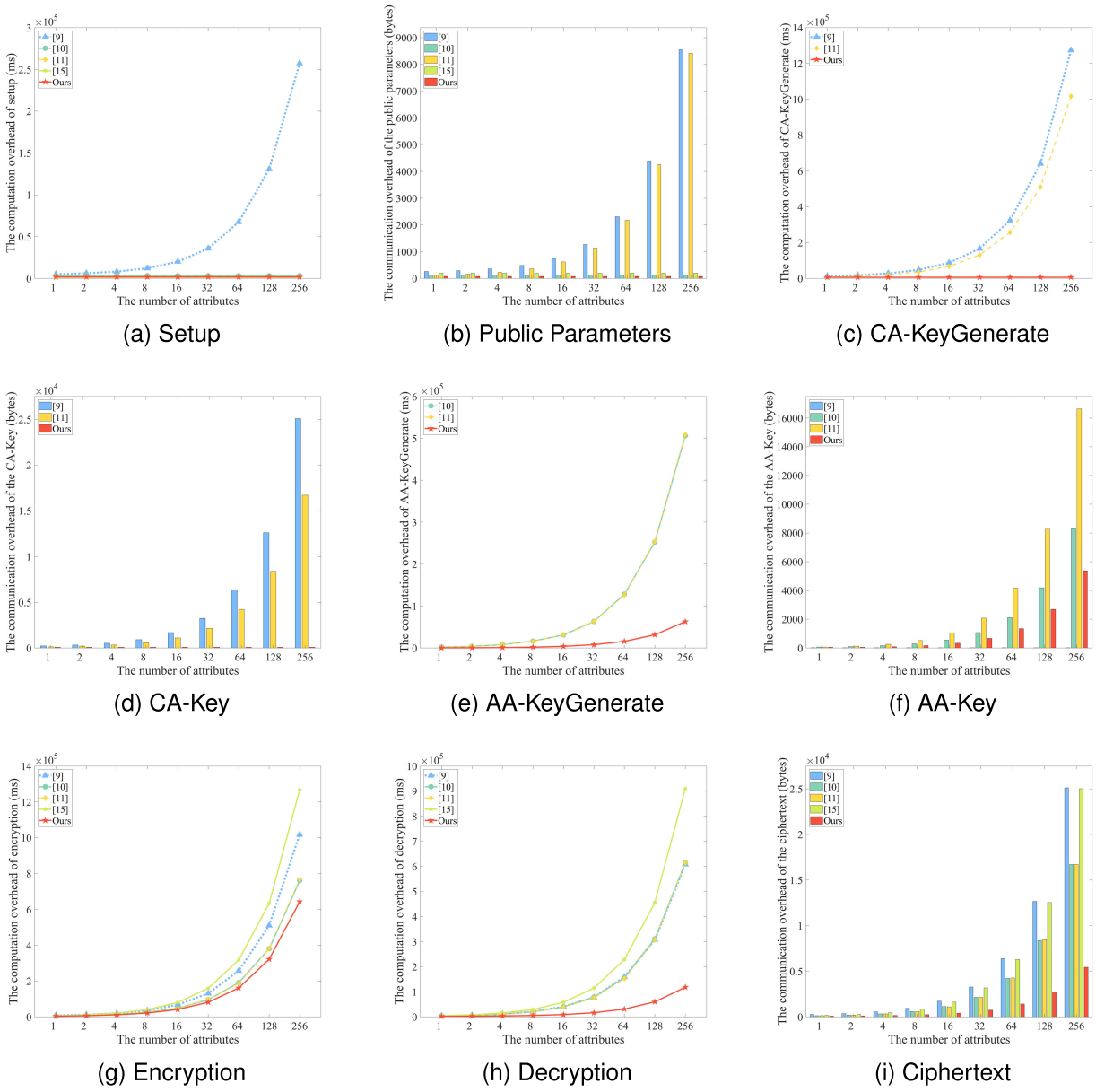

Fig. 3. Experimental Performance Analysis in existing CP-ABE schemes.

[13], [17] and is superior to that in MABKS [11]. For instance, when setting $i = 256$, our system takes (1.7 s, 0.0752 KB) to be initialized, while the existing systems [11], [12], [13], [17] take (257.37 s, 8.347 KB), (3.22 s, 0.127 KB), (2.23 s, 8.22 KB) and (1.24 s, 0.19 KB) respectively. Obviously, not only the computation overhead, but also the communication overhead of our system keeps unchanged, suggested that our scheme is appropriate for resource-limited devices.

When comparing the performance of CA-Key generation in Figs. 3c and 3d, it is easy to observe that our system outperforms MABKS [11] and RAAC [13]. The computation overhead $(9T_G + 3T_H)$ and communication overhead $(3|\mathbb{H}| + 3|\mathbb{G}|)$ of MA-CP-ABE-CRF remain nearly constant, while those of the other two schemes are affected by the number of attributes i. Furthermore, the superiority of our scheme becomes more obvious with the increase of the value of i. For instance, when i is setted 128, the computation and communication overhead of CA-Key generation in the proposed scheme are 6.3 s and 0.082 KB, which are a hundred times smaller than (640.8 s, 12.314 KB) and (510.3 s, 8.188 KB) of MABKS [11] and RAAC [13].

As for AA-Key generation phase in Figs. 3e and 3f, MA-CP-ABE-CRF has lower computation and communication overhead than the works proposed in [12] and [13] due to the advantage of asymmetric pairing. When setting $i = 256$, it takes our system (62.91 s, 5.25 KB) to generate AA-Key, while schemes proposed in [11], [12], and [13] need (N/A, 0.0156 KB), (506.32 s, 8.157 KB) and (506.25 s, 16.25 KB) respectively. Although the cost of our system is higher than that of MABKS [11] when generating AA-Key, it can be ignored when considering the cost of the entire encryption process. Needless to say, MA-CP-ABE-CRF outperforms the other systems in AA-Key generation.

In Figs. 3g, 3h and 3i, the computation and communication overhead of our scheme and other four schemes are both affected by the number i of attributes. In Encryption, when setting $n_2 = 5$, it can be noticed that the computation overhead of all the five schemes linearly increases as the value of i increases. However, compared with symmetric pairing at same security levels, group elements in asymmetric pairing groups are smaller and the exponent operation and pairing operation can be computed faster. Hence, the performance of our system is much better than other schemes(i.e., [11], [12], [13], [17]). For instance, when setting $i = 256$, our system needs (643 s, 5.318 KB) to encrypt the message, while the other four systems need (1016.9 s, 24.534 KB), (760.62 s, 16.313 KB), (760.6 s, 16.312 KB), (1266.9 s, 24.438 KB) respectively. Besides, the MA-CP-ABE-CRF scheme uses 118.07 s to decrypt the ciphertext, and aforementioned four schemes use 614.29 s, 614.33 s, 614.28 s and 910.01 s. Clearly, the proposed scheme has distinct advantages over the related four schemes, which can greatly improve user experience.

Overall, the proposed system is more efficient while achieving a higher level of security compared with the schemes [11], [12], [13], [17] mentioned above. In supporting flexible and fine-grained management for IoV, the MA-CP-ABE-CRF system does not introduce additional computation or communication cost. This is mainly because the scheme is built on asymmetric pairing, which permits faster exponent and pairing operations over smaller prime-order groups. In particular, the work presented in this paper is better in efficiency than existing works in the scenario with large number of attributes and limited computational resources. Furthermore, our scheme achieves adaptive CPA-security, which allows adversaries to make all choices as the attack progresses. Hence, our system has a raised security level. In summary, the MA-CP-ABE-CRF scheme is feasible, and can be widely deployed in distributed systems designed for Internet of vehicles.

VII. Conclusion

In this papar, MA-CP-ABE-CRF, a multi-authority CP-ABE scheme with cryptographic reverse firewalls, is proposed to realize flexible and secure access for Internet of vehicles. To achieve flexible and fine-grained management of Internet of vehicles, a multi-authority CP-ABE methodology is introduced. Furthermore, CRFs are deployed in each nodes and other entities to enhance security. Through rigorous theoretical analysis, the proposed system is proved to obtain adaptive security and exfiltration resistance. In the detailed theoretical simulation experiments, the scheme is proved to get the superiority of computation cost as well as communication cost. In the end, ample theoretical analysis as well as experiments indicate that our system is applicable to the application scenarios of Internet of vehicles. The algorithm proposed in this paper holds practical significance across a wide range of real-world scenarios. However, due to time constraints, this study focuses exclusively on its application within IoV systems. As a direction for future work, we consider the application of the proposed algorithm to other scenarios. For instance, in light of the threats posed by quantum attacks, the development of quantum resistance MA-CP-ABE scheme represents a significant avenue for our future research. In conclusion, this paper contributes to the ongoing discourse on secure data management in IoV systems and encourages further exploration of advanced cryptographic solutions.

References

[1] D.-G. Zhang, X.-Y. Wang, J. Zhang, T. Zhang, and H.-T. Li, "Novel data return approach for Internet of Vehicles based on edge computing," *Ad Hoc Netw.*, vol. 146, Jul. 2023, Art. no. 103178, doi: 10.1016/j.adhoc.2023.103178.

[2] F. Yang et al., "Revisiting WiFi offloading in the wild for V2I applications," *Comput. Netw.*, vol. 202, Jan. 2022, Art. no. 108634, doi: 10.1016/j.comnet.2021.108634.

[3] H. Mun et al., "Privacy enhanced data aggregation based on federated learning in Internet of Vehicles (IoV)," *Comput. Commun.*, vol. 223, pp. 15–25, Jul. 2024, doi: 10.1016/j.comcom.2024.05.009.

[4] T. Hai, M. Aksoy, C. Iwendi, E. Ibeke, and S. Mohan, "CIA security for Internet of Vehicles and blockchain-AI integration," *J. Grid Comput.*, vol. 22, no. 2, p. 43, Jun. 2024, doi: 10.1007/s10723-024-09757-3.

[5] M. Mao, T. Hu, and W. Zhao, "Reliable task offloading mechanism based on trusted roadside unit service for Internet of Vehicles," *Ad Hoc Netw.*, vol. 139, Feb. 2023, Art. no. 103045. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870522002177

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

[7] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in *International Colloquium on Automata, Languages, and Programming*. Berlin, Germany: Springer, 2008, pp. 579–591.

[8] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proc. ACM Conf. Comput. Commun. Security*, 2007, pp. 456–465.

[9] M. Chase, "Multi-authority attribute based encryption," in *Proc. 4th Theory Cryptogr. Conf. (TCC)*, Amsterdam, The Netherlands. Berlin, Germany: Springer, Feb. 2007, pp. 515–534.

[10] S. Müller, S. Katzenbeisser, and C. Eckert, "Distributed attribute-based encryption," in *Proc. Int. Conf. Inf. Secur. Cryptol. (ICISC)* Seoul, South Korea, Dec. 2008, pp. 3–5.

[11] Y. Miao, R. H. Deng, X. Liu, K. R. Choo, H. Wu, and H. Li, "Multi-authority attribute-based keyword search over encrypted cloud data," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 4, pp. 1667–1680, Jul. 2021.

[12] M. Xie, Y. Ruan, H. Hong, and J. Shao, "A CP-ABE scheme based on multi-authority in hybrid clouds for mobile devices," *Future Gener. Comput. Syst.*, vol. 121, pp. 114–122, Aug. 2021.

[13] 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.

[14] W.-M. Li, X.-L. Li, Q.-Y. Wen, S. Zhang, and H. Zhang, "Flexible CP-ABE based access control on encrypted data for mobile users in hybrid cloud system," *J. Comput. Sci. Technol.*, vol. 32, no. 5, pp. 974–990, Sep. 2017.

[15] I. Mironov and N. Stephens-Davidowitz, "Cryptographic reverse firewalls," in *Proc. 34th Annu. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, Sofia, Bulgaria. Berlin, Germany: Springer, Jan. 2015, pp. 657–686.

[16] R. Chen, Y. Mu, G. Yang, W. Susilo, F. Guo, and M. Zhang, "Cryptographic reverse firewall via malleable smooth projective hash functions," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Berlin, Germany: Springer, 2016, pp. 844–876.

[17] H. Ma, R. Zhang, G. Yang, Z. Song, S. Sun, and Y. Xiao, "Concessive online/offline attribute based encryption with cryptographic reverse firewalls—Secure and efficient fine-grained access control on corrupted machines," in *Proc. 23rd Eur. Symp. Res. Comput. Secur. (ESORICS)*. Barcelona, Spain: Springer, Sep. 2018, pp. 507–526.

[18] Y. Zhou, Z. Hu, and F. Li, "Searchable public-key encryption with cryptographic reverse firewalls for cloud storage," *IEEE Trans. Cloud Comput.*, vol. 11, no. 1, pp. 383–396, Jan. 2023, doi: 10.1109/TCC.2021.3095498.

[19] M. Ouyang, Z. Wang, and F. Li, "Digital signature with cryptographic reverse firewalls," *J. Syst. Archit.*, vol. 116, Jun. 2021, Art. no. 102029, doi: 10.1016/j.sysarc.2021.102029.

[20] 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.*, Oct. 2006, pp. 89–98.
[21] M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *Proc. ACM Conf. Comput. Commun. Secur. (CCS)*, 2009, pp. 121–130.
[22] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2011, pp. 568–588.
[23] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," in *Proc. IEEE 10th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Nov. 2011, pp. 91–98.
[24] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," *Inf. Sci.*, vol. 180, no. 13, pp. 2618–2632, 2010.
[25] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "DAC-MACS: Effective data access control for multiauthority cloud storage systems," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1790–1801, Nov. 2013.
[26] J. Han, W. Susilo, Y. Mu, J. Zhou, and M. H. A. Au, "Improving privacy and security in decentralized ciphertext-policy attribute-based encryption," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 665–678, Mar. 2015.
[27] H. Wee, "Optimal broadcast encryption and CP-ABE from evasive lattice assumptions," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 13276, O. Dunkelman and S. Dziembowski, Eds., Berlin, Germany: Springer, May 2022, pp. 217–241, doi: 10.1007/978-3-031-07085-3_8.
[28] S. Das and S. Namasudra, "Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure," *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 821–829, Jan. 2023, doi: 10.1109/TII.2022.3167842.
[29] R. Guo, G. Yang, H. Shi, Y. Zhang, and D. Zheng, "O3-R-CP-ABE: An efficient and revocable attribute-based encryption scheme in the cloud-assisted IoMT System," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 8949–8963, Jun. 2021, doi: 10.1109/JIOT.2021.3055541.
[30] Y.-F. Yao, H.-Y. Chen, Y. Gao, K. Wang, and H.-Y. Yu, "A decentralized multi-authority CP-ABE scheme from LWE," *J. Inf. Secur. Appl.*, vol. 82, May 2024, Art. no. 103752, doi: 10.1016/j.jisa.2024.103752.
[31] C. Ma, H. Gao, and B. Hu, "Ciphertext policy attribute-based encryption scheme supporting Boolean circuits over ideal lattices," *J. Inf. Secur. Appl.*, vol. 84, Aug. 2024, Art. no. 103822, doi: 10.1016/j.jisa.2024.103822.
[32] Y. Dodis, I. Mironov, and N. Stephens-Davidowitz, "Message transmission with reverse firewalls—Secure communication on corrupted machines," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 2016, pp. 341–372.
[33] Y. Zhou, Y. Guan, Z. Zhang, and F. Li, "Cryptographic reverse firewalls for identity-based encryption," in *Proc. 2nd Int. Conf. Frontiers Cyber Secur. (FCS)*, Xi'an, China. Singapore: Springer, Nov. 2019, pp. 36–52.
[34] N. Eltayieb, R. Elhabob, Y. Liao, F. Li, and S. Zhou, "A heterogeneous signcryption scheme with cryptographic reverse firewalls for IoT and its application," *J. Inf. Secur. Appl.*, vol. 83, Jun. 2024, Art. no. 103763, doi: 10.1016/j.jisa.2024.103763.
[35] Y. Ming, H. Liu, C. Wang, and Y. Zhao, "Generic construction: Cryptographic reverse firewalls for public key encryption with keyword search in cloud storage," *IEEE Trans. Cloud Comput.*, vol. 12, no. 2, pp. 405–418, Apr. 2024, doi: 10.1109/TCC.2024.3366435.
[36] A. Lewko et al., "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, French Riviera. Berlin, Germany: Springer, May/Jun. 2010, pp. 62–91.
[37] S. Agrawal and M. Chase, "FAME: Fast attribute-based message encryption," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, B. Thuraisingham, D. Evans, T. Malkin, and D. Xu, Eds., Dallas, TX, USA, Oct. 2017, pp. 665–682, doi: 10.1145/3133956.3134014.

Ye Lin received the B.S. degree from the University of Electronic Science and Technology of China in 2022, where he is currently pursuing the M.S. degree from the School of Information and Software Engineering. His research interests include proxy re-encryption public key cryptography.

Hu Xiong (Senior Member, IEEE) received the Ph.D. degree from the School of Computer Science and Engineering, University of Electronic Science and Technology of China (UESTC) in 2009. He is currently a Full Professor with the School of Information and Software Engineering, UESTC. His research interests include applied cryptography and cyberspace security.

Hui Su received the B.S. degree from the University of Electronic Science and Technology of China in 2024. She is currently pursuing the M.S. degree from Shanghai Jiao Tong University. Her research interests include proxy re-encryption public key cryptography.

Kuo-Hui Yeh (Senior Member, IEEE) received the M.S. and Ph.D. degrees in information management from the National Taiwan University of Science and Technology, Taipei, Taiwan, in 2005 and 2010, respectively. He is currently a Professor with the Institute of Artificial Intelligence Innovation, National Yang Ming Chiao Tung University, Hsinchu, Taiwan. Prior to this appointment, he was a Professor with the Department of Information Management, National Dong Hwa University, Hualien, Taiwan, from February 2012 to January 2024. He has contributed over 150 articles to esteemed journals and conferences, covering a wide array of research interests such as the IoT security, blockchain, NFC/RFID security, authentication, digital signatures, data privacy, and network security. Furthermore, he plays a pivotal role in the academic community, serving as an Associate Editor (or Editorial Board Member) for several journals, including the *Journal of Information Security and Applications*, *Human-Centric Computing and Information Sciences*, *Symmetry*, *Journal of Internet Technology*, and *CMC-Computers, Materials and Continua*. In the professional realm, he holds memberships with $(ISC)^2$, ISA, ISACA, CAA, and CCISA. His professional qualifications include certifications, such as CISSP, CISM, Security+, ISO 27001/27701/42001 Lead Auditor, IEC 62443-2-1 Lead Auditor, and ISA/IEC 62443 cybersecurity expert, covering fundamentals, risk assessment, design, and maintenance specialties.