# A Privacy-Preserving Attribute-Based Authenticated Key Management Scheme for Accountable Vehicular Communications

Haowen Tan, Wenying Zheng, Yunguo Guan, and Rongxing Lu, *Fellow, IEEE*

***Abstract*—In recent years, the vehicular ad hoc network (VANET), recognized as the fundamental infrastructure of the intelligent transportation system (ITS), has played an increasingly momentous role in advancing real-time vehicular communications. With the purpose of achieving seamless and reliable connectivity, lots of research efforts have been witnessed. Nevertheless, the flexibility of access control and authenticated key management (AKM) has not been properly guaranteed. Particularly, exclusive V2V connections without third-party intervention or remote surveillance are crucial for privacy protection, while the non-repudiation and authenticity properties may be compromised in this case. In the proposed design, the attribute-based secret sharing scheme is adopted so that the flexible authentication mechanism with a dynamic access policy is provided. Moreover, independent V2V connections with anonymity are achieved. The vital vehicular data are autonomously stored in local storage, while the remote trusted authority (TA) maintains its ciphered form simultaneously. Therefore, repudiation on the historical transmissions can be prevented whenever a dispute occurs. The proofs and discussions regarding vital security features are presented, while the performance analysis follows. Advantages in terms of security and performance properties can be proved compared with the state-of-the-art.**

***Index Terms*—Authenticated key management, vehicular ad hoc networks (VANETs), non-repudiation, data confidentiality, privacy-preservation, secure data sharing.**

## I. Introduction

NOWADAYS, the innovative breakthroughs in networking and communicating techniques have triggered the prosperity of modern intelligent transportation systems, which gradually facilitate the improvement of transportation quality in all respects. With its groundbreaking advantages in providing effective vehicular services and functional applications, the construction of ITS paradigms has extensively received attention from both the academia and the industry. Accordingly, advanced traffic management and vehicular data interactions can be achieved, which is of particular importance to metropolitan areas with booming populations and severe traffic pressure. As a consequence, the VANETs, as the indispensable components of diverse ITS scenarios, have attracted increasing research interest [1]. Briefly speaking, the VANET is delineated as the scattered, distributed, self-organized mobile wireless network established between heterogeneous vehicle entities. The unique characteristics including spontaneous communication, flexibility, scalability, and high mobility can be achieved.

A typical VANET infrastructure is composed of three crucial types of entities with distinctive functionalities: the roadside units (RSUs), the trusted authority (TA), and vehicles. Above all, TA is the topmost service provider and data center in charge of essential systematic management and confidential data processing. Furthermore, crucial security-related operations including initial configuration, session key allocation, and group validation, are executed by TA as well [2]. It is envisaged that the consolidated vehicular data are safely preserved in the affiliated cloud facilities. In this case, the cloud-based infrastructure is able to support inter-network communications between varied VANETs simultaneously, which accelerates the establishment of a universal global internet initiative for vehicles (IoV).

Generally, the RSUs are characterized as the distributed edge deployments at the designated zones. Individual RSU takes the responsibility of carrying out real-time and dynamic data exchange with vehicles of its vicinity [3], [4]. Particularly, the requisite validation and critical verification tasks towards all the participating vehicles are carried out by nearby RSU. Meanwhile, the vehicles are recognized as the terminal users of the specific VANET so that manifold vehicular services and applications can be obtained. Each vehicle is equipped with various sensors for measuring significant driving parameters including velocity, acceleration, location, rotation speed. Correspondingly, vital driving-related vehicular data including route information and traffic characteristics, are collaboratively collected and uploaded to the remote trusted authority (TA) via secure interactions with RSUs [5], [6].

In VANETs, two main communication types, namely vehicle-to-vehicle (V2V), and vehicle-to-RSU (V2R) communication are performed. The seamless data connections between an individual vehicle and its nearby RSU are maintained through V2R communication, while spontaneous mutual communications within random vehicles are achieved through the instant V2V data sharing mechanism. Notably, both V2R and V2V interconnections operate in the public wireless environment with vulnerability to multiple attacks



H. Tan is with the School of Information Science and Technology, Zhejiang Sci-Tech University, Hangzhou 310018, China (e-mail: tan_halloween@foxmail.com).

W. Zheng is with the School of Computer Science and Technology, Zhejiang Sci-Tech University, Hangzhou 310018, China (e-mail: zhengwy0501@126.com) *(Corresponding author)*.

Y. Guan is with the Faculty of Computer Science, University of New Brunswick, Fredericton, Canada (e-mail: yguan4@unb.ca).

R. Lu is with the Faculty of Computer Science, University of New Brunswick, Fredericton, Canada (e-mail: rlu1@unb.ca).

and threats. Many existing authentication methods and key management strategies are proposed, whereas the intrinsic security flaws and weaknesses have not been fully eliminated. Moreover, as for dynamic VANET topologies with heterogeneous entities, flexible access control and authentication mechanisms are essential. In other word, the diverse practical requirements such as user privacy, authenticity, scalability, and data confidentiality, has not been properly satisfied so far [7].

Conventionally, in most of the existing studies towards secure vehicular data exchange, the V2V connections are maintained depending on the essential credentials and signatures issued from the deployed RSUs, which to some extent results in potential risks of being eavesdropped on, obstructed, or even manipulated, since the third-party RSUs are able to access all transmitted messages inevitably [8]. Apparently, with massive private sensitive vehicular information to be delivered via the spontaneous V2V channels, the necessity of an exclusive and independent data sharing and storing mechanism can be demonstrated so that the V2V vital information is accessible only between the authorized users themselves. In this case, other third-party entities, even the benign VANET insiders such as the RSU with key distribution responsibility, have no authority to thoroughly operate surveillance and monitoring towards the entire V2V data transmission process. Overall, the data confidentiality and privacy requirements of the individual vehicle can be accordingly met [9]. However, these surveillance-free exclusive V2V connections may also lead to security vulnerabilities including repudiation, denial, and forgery towards the previously delivered message. What's worse, collusion among the sender and receiver vehicles can be easily achieved during V2V data transmission scenarios. Therefore, with the aim of data security and privacy-preservation of self-organized V2V data sharing, the issues of non-repudiation and accountability should be taken into thorough consideration [10]. The tradeoff between advanced user privacy protection and data confidentiality remains to be studied properly. Notably, the accountability property is different from the traceability. The traceability refers to the effective tracking of the specific vehicular entity, whereas the accountability emphasizes on the non-repudiation and accountability of the message contents.

### A. Research Contributions

A privacy-preserving attribute-based authenticated key management scheme with accountable vehicular communication in VANETs is proposed in this paper. Our nontrivial efforts can be briefly summarized as follows:

- *Attributed-based authentication and key management providing flexible access policy:* The proposed design utilizes the attribute set for the individual vehicle for the construction of V2R dynamic access control policy. The requesting vehicles that satisfy the predefined accessing rules are able to pass the validation process. Meanwhile, certificateless cryptographic design is adopted for all VANET entities including RSUs and vehicles. Additionally, batch authentication is available, which drastically accelerates the validation process for massive vehicle verification.
- *Exclusive V2V secure communication with anonymity:* The vehicles are able to spontaneously construct the unique V2V data exchange channel with the shared credential. Notably, the sensitive V2V connectivities are accessible only between the sender and receiver themselves. The potential surveillance and interference from other third parties, even the nearby RSUs that have issued the credentials, can be largely prevented. A genuine trustworthy V2V data delivery mechanism is established in this way.
- *Accountable vehicular message delivery process with resistance to repudiation and collusion:* The tradeoff between user privacy-preserving and non-repudiation in terms of V2V data exchange is made. The decrypted vehicular contents are stored in local hash chains, while the ciphered messages are remotely monitored and updated in the TA server. Therefore, collusion between sender and receiver vehicles can be prevented. Accountable and reliable V2V data sharing is provided.

The remainder of this paper is formulated as follows. The corresponding research progress is briefly introduced in Section II. To gain a better understanding of the topic, Section III outlines the requisite preliminary works and the VANET system model. In Section IV, the proposed attribute-based authentication and key management scheme are presented in detail. The security analysis and performance discussion are presented in Section V and Section VI, respectively. The conclusion is drawn in Section VII.

## II. Related Work

In recent years, numerous studies regarding authenticated key management and reliable vehicular data exchange have been conducted. Lu *et al.* [11] developed a dynamic key updating protocol DIKE to satisfy the privacy-preserving and reliability requirements of location-based VANET services (LBS). The distributed session keys are cooperatively updated by the involved vehicles whenever the revocation process initializes. In [12], the validating process towards certificate revocation lists (CRLs) in terms of vehicular message authentication is improved with the adopted hash chains. Subsequently, a scalable group key management and message encryption scheme is proposed by Aliev *et al.* [13]. Notably, the matrix-based encryption algorithm is utilized in the distributed VANET architecture so that enhanced security characteristics and efficiency can be guaranteed. Similarly, Aman *et al.* [14] developed a robust IoV authentication scheme with unclonable functions. The approaching vehicles are verified by the gateway instead of each RSU. Cai *et al.* [15] proposed a conditional privacy protection mechanism adopting ring signcryption and identity-based cryptosystem. Identities of the misbehaving VANET nodes can be revealed with the assigned tracking marks. Recently, several VANET authentication and key management schemes are developed [16], [17], [18].

Identity-based and attributed-based cryptographic techniques have been widely adopted in the authenticated key management process. A cooperative message authentication and key management framework is developed in 2011 [1],

where decentralized message verification tasks are allocated to each legitimate vehicle. Meanwhile, with the aim to enhance the communication efficiency of VANET emergency services, Yeh *et al.* [19] proposed an attributed-based access control scheme ABACS so that data confidentiality property is provided. Afterward, the pseudonymous authentication-based conditional privacy protocol PACP [2] is presented by Huang *et al.*. The improvement in terms of computation and storage cost during the message validation process is achieved. Subsequently, He *et al.* developed an identity-based VANET authentication method without pairing [20]. Accordingly, the computational complexity of the verification session can be significantly reduced. In 2020, Feng *et al.* applied the blockchain-assisted authentication framework in [21] for privacy preservation. Dynamic revocation and conditional tracking towards the misbehaving vehicles are enabled. Another attribute-based encryption (ABE) model [22] is developed in order to meet the responding time requirement of edge intelligence-empowered IoV. The proposed ABEMPOD adopts the parallel outsourced decryption process, which is of specific usage for the tree access structure.

Specifically, many featured studies on secure V2V data sharing have been presented. Zhang *et al.* [23] proposed a decentralized authentication protocol, where each RSU is responsible for managing the ongoing spontaneous vehicular groups. In [8], the dual authentication scheme PPDAS is constructed for privacy preservation and secure access control in diverse IoV scenarios. Afterward, in 2019, another privacy-preserving mutual authentication scheme for V2V data exchange is established [24]. In the next, Hathal *et al.* [25] proposed a lightweight certificateless authentication method for secure vehicular communication. The authenticating tokens are adopted in place of digital certificates so that the computation overhead for certificate management in TA can be alleviated. Recent studies on V2V secure communication are witnessed [26], [27], where the proposed CLSS-CPPA protocol in [26] adopts a pairing-free design for efficiency concerns. Overall, the significant security characteristics including authentication flexibility, non-repudiation, have not been properly addressed in the existing VANET authentication and key management schemes. Moreover, the exclusive V2V connections satisfying both the privacy-preserving and accountability requirements should be thoroughly investigated.

## III. Model Definition and Preliminaries

The fundamental principles and knowledge are presented in this section, with the purpose of facilitating the reader's understanding on the proposed design.

### A. Bilinear Pairing

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be the cyclic additive group and multiplicative group generated with prime order $q$. The mapping $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ is defined as a bilinear pairing with the following characteristics [28]:

1) *Bilinearity:* $\forall P, Q, R \in \mathbb{G}_1$ and $\forall a, b \in \mathbb{Z}_q^*$, there is

$$\begin{cases} \hat{e}(aP, bQ) = \hat{e}(P, bQ)^a = \hat{e}(aP, Q)^b = \hat{e}(P, Q)^{ab} \\ \hat{e}(P, Q+R) = \hat{e}(Q+R, P) = \hat{e}(P, Q)\,\hat{e}(P, R) \end{cases}.$$

2) *Non-degeneracy:* $\exists P, Q \in \mathbb{G}_1$ such that $\hat{e}(P, Q) \neq 1_{\mathbb{G}_2}$, where $1_{\mathbb{G}_2}$ is the identity element of $\mathbb{G}_2$.
3) *Computability:* $\forall P, Q \in \mathbb{G}_1$, there is an efficient algorithm to calculate $\hat{e}(P, Q)$.

With the modified Weil pairing or Tate pairing on the supersingular elliptic curve $\mathbb{G}_1$, a bilinear map $\hat{e}$ satisfying the above properties can be constructed, where the following properties are presented:

**Definition 1** (Elliptic Curve Discrete Logarithm Problem (ECDLP))**.** *Given two random points $P, Q \in \mathbb{G}_1$, where $Q = aP$. The advantage in finding the integer $a \in \mathbb{Z}_q^*$ to solve the ECDLP problem for any probabilistic polynomial-time (PPT) algorithm $\mathscr{A}$ is negligible [29], which is defined as:*

$$Succ_{\mathscr{A},\mathbb{G}_1}^{ECDLP} = \Pr\left[\mathscr{A}(P, aP) \to a | \forall a \in \mathbb{Z}_q^*\right] \leq \varepsilon$$

**Definition 2** (Computational Diffie-Hellman Problem (CDHP))**.** *Given $P, aP, bP \in \mathbb{G}_1$ for $a, b \in \mathbb{Z}_q^*$, where $P$ is the generator of $\mathbb{G}_1$, the advantage in computing $abP$ to solve the CDHP problem for any probabilistic polynomial-time (PPT) algorithm $\mathscr{A}$ is negligible [30], which is defined as:*

$$Succ_{\mathscr{A},\mathbb{G}_1}^{CDHP} = \Pr\left[\mathscr{A}(P, aP, bP) \to abP | \forall a, b \in \mathbb{Z}_q^*\right] \leq \varepsilon$$

### B. Lagrange Polynomial Interpolation

**Definition 3** (Degree of Polynomial over $\mathbb{F}_p$)**.** *Let $\mathbb{F}_p$ be a finite field, $P(x) = \sum_{i=0}^{t} \epsilon_i x^i$ be a non-zero polynomial, where $\epsilon_t \neq 0$, the arbitrary positive integer $t$ is defined as the degree of $P(x)$ such that $\deg P(x) = t$.*

Accordingly, define $\{(x_0, y_0), \ldots, (x_j, y_j), \ldots, (x_k, y_k)\}$ as a set of $k+1$ distinctive data points such that $\forall m \neq j$, $x_m \neq x_j$. The polynomial of the degree $k$ over a finite field $\mathbb{F}_p$ is built as $Q_k(x) = \sum_{i=0}^{k} a_i x^i$, where $Q_k(x_i) = y_i$ for all $i = 0, \ldots, k$. The unique Lagrange basis polynomials $\ell_j(x)$ $(0 \leq j \leq k)$ of degree at most $k$ are computed as

$$\begin{aligned} \ell_j(x) &= \frac{(x-x_0)}{(x_j-x_0)} \cdots \frac{(x-x_{j-1})}{(x_j-x_{j-1})} \frac{(x-x_{j+1})}{(x_j-x_{j+1})} \cdots \frac{(x-x_k)}{(x_j-x_k)} \\ &= \prod_{m=0, m\neq j}^{k} \frac{x-x_m}{x_j-x_m} \end{aligned}.$$

The corresponding interpolation polynomial $L_k(x)$ in the Lagrange form [31] can be defined as $L_k(x) = \sum_{j=0}^{k} y_j \ell_j(x)$. That is, $L_k(x) = \sum_{j=0}^{k} \left( \prod_{m=0, m\neq j}^{k} \frac{x-x_m}{x_j-x_m} \right) y_j$. Accordingly, for $\forall i \neq j$, $\ell_j(x_i) = \prod_{m=0, m\neq j}^{k} \frac{x_i-x_m}{x_j-x_m} = 0$, and $\ell_j(x_j) = \prod_{m=0, m\neq j}^{k} \frac{x_j-x_m}{x_j-x_m} = 1$ hold. Hence, the reconstruction of the polynomial $Q_k(x)$ can be performed with $k+1$ distinctive data points on the graph of polynomial $Q_k(x)$ and $L_k(x)$.

TABLE I: Security Notations

| Notation | Description |
|---|---|
| TA | Trusted Authority |
| RSU | Road-Side Unit |
| $\mathbb{G}_1, \mathbb{G}_2$ | Additive Cyclic Group |
| $q$ | Order of $\mathbb{G}_1$ |
| $P$ | Generator of $\mathbb{G}_1$ |
| $\{H_i\}_{i\in[1,4]}, \{h_i\}_{i\in[1,3]}$ | Secure Hash Functions |
| $\left\{\mathsf{id}^j_{\mathsf{rsu}}, \mathsf{ID}^j_{\mathsf{rsu}}\right\}$ | RSU Identities |
| $\{\mathsf{id}_i, \mathsf{ID}^i_{\mathsf{v}}, \mathsf{ID}^i_{\Delta}, \mathsf{ID}^{\mathsf{S}}_{\Delta}, \mathsf{ID}^{\mathsf{R}}_{\Delta}\}$ | Vehicle Identities |
| $\{\mathsf{t}^1_{\mathsf{rsu}}, \mathsf{t}^1_{\mathsf{v}}, \mathsf{t}_{\mathsf{ta}}, \mathsf{t}^{\mathsf{S}}_{\Delta}\}$ | Timestamps |
| $\mathcal{P}$ | Access Structure |
| $\aleph_j$ | Group Key |
| $\{\mathcal{G}_i, \hbar_i\}$ | V2V Encryption Key Pair |
| $\{\varrho_i, \varkappa_i\}$ | V2V Decryption Key Pair |
| $\mathrm{Vehicle}_{\mathsf{S}}, \mathrm{Vehicle}_{\mathsf{R}}$ | Sender and Receiver |
| $\{\mathsf{ID}^{\mathsf{S}}_{\Delta}, \mathsf{ID}^{\mathsf{R}}_{\Delta}\}$ | Identities for $\mathrm{Vehicle}_{\mathsf{S}}, \mathrm{Vehicle}_{\mathsf{R}}$ |

### C. Linear Integer Secret Sharing

In the linear integer secret sharing (LISS) design [32], the secret $s \in [-2^{\chi}, 2^{\chi}]$ is a specific integer selected from a publically known interval. Note that $\chi$ is defined as an integer constant. The recovery towards the issued secret $s$ can be conducted by calculating the linear combination with integer coefficients of the shares in a qualified set. Given $\mathcal{D}$ as the dealer, $\mathcal{P} = \{P_1, \ldots, P_n\}$ denote the $n$ shareholders. The dealer $\mathcal{D}$ is going to share the secret $s$ to the shareholders $\mathcal{P}$ over a monotone access structure $\Gamma$. The subset $\mathsf{A} \subseteq \mathcal{P}$ is recognized to be qualified if the parties of $\mathsf{A}$ jointly are allowed to reconstruct the secret $s$. In this case, every set of shareholders $\mathsf{A} \in \Gamma$ is able to reconstruct the secret $s$, while the set of shareholders $\overline{\Gamma} = \{\mathsf{B} \subseteq \mathcal{P} | \mathsf{B} \notin \Gamma\}$ get no or very little information of $s$. The definition of a monotone access structure $\Gamma$ is given as follows.

**Definition 4** (Access Structure)**.** *Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ denote a set of $n$ parties. If a non-empty collection $\Gamma$ of the subsets of $\mathcal{P}$ is closed under taking subsets and $\oslash \notin \Gamma$, $\Gamma$ is defined as a monotone access structure on $\mathcal{P}$. That is, for all $\mathsf{A} \in \Gamma$ and all $\mathsf{B} \subseteq \mathcal{P}$ fulfilling $\mathsf{A} \subseteq \mathsf{B}$, $\mathsf{B} \in \Gamma$. Likewise, if a collection $\Delta$ of the subsets of $\mathcal{P}$ is closed under taking subsets and $\oslash \in \Delta$, $\Delta$ is defined as a monotone adversary structure on $\mathcal{P}$. That is, for all $\mathsf{C} \in \Delta$ and all $\mathsf{D} \subseteq \mathcal{P}$ fulfilling $\mathsf{D} \subseteq \mathsf{C}$, $\mathsf{D} \in \Delta$ holds.*

In a LISS design, the shares consist of a collection of integers $\{s_i\}_{i\in\mathsf{I}}$. For each $i \in \mathsf{I}$, the integer $s_i$ belongs to exactly one party. Accordingly, $s_i$ is calculated as the linear integer combination of $s$ and some randomness selected by $\mathcal{D}$. Let $\{s_i\}_{i\in\mathsf{I}'}$ be a qualified subset of shares, the secret $s$ can then be constructed as $s = \sum_{i\in\mathsf{I}'} \lambda_i s_i$, where $\{\lambda_i\}_{i\in\mathsf{I}'}$ are integer coefficients determined by the index set $\mathsf{I}'$.

### D. Notations

The notations used in the proposed scheme, along with the corresponding descriptions are listed in the following Table I.

### E. System Model

The deployed VANET infrastructure is briefly illustrated in this section. As shown in Fig. 1, a typical VANET system model is composed of three types of essential components with distinctive functionalities: the vehicles as the terminal users, the trusted authority as the remote server and data center, the RSUs as the edge vehicular facilities. Respectively, the relevant descriptions of the three varieties of VANET entities are presented as follows.

- Trusted authority is the essential trustworthy authority with remote control towards the entire vehicular networks. Critical global operations, including user registration and systematic key issuance, are all performed by trusted authority (TA).
- Edge vehicular infrastructure is recognized as the distributed VANET facilities with various collaborative RSU clusters. Each RSU cluster retains stable and wired inside communication between the in-range RSUs.
- The vehicles are considered as terminal users of VANET services and applications. The transceiver and transponder units are mounted on the embedded on-board unit (OBU) for wireless message delivery.

### F. Network Assumptions

As shown in Fig. 1, in VANETs, the distinctive V2R and V2V transmission forms are conducted. The independent message delivery between the specific vehicle and its nearby RSU is organized via V2R communication, while the arbitrary data sharing among vehicles is performed through V2V communication. Both V2V and V2R interconnections are carried out in the open wireless environment so that they are vulnerable to various attacks and security risks. Therefore, to offer advanced security properties, many existing authentication methods and key management strategies have been developed, while the intrinsic security flaws and weaknesses have not been fully eliminated. Moreover, as for dynamic VANET topologies with heterogeneous entities in various frameworks, flexible access control and authentication mechanisms are essential so that the robust and adaptable VANET system can be guaranteed.

Particularly, the V2V connections are built with the valid credentials and signatures issued by the third-party RSUs, which to some extent results in potential risks of being eavesdropped on, obstructed, or even manipulated by the compromised RSUs. That is, the RSUs could easily access all transmitted information. Accordingly, an exclusive and independent data sharing mechanism is necessary such that other third-party entities can not obtain details of the V2V transmission process. However, due to lack of surveillance, the V2V data sharing may suffer from vulnerabilities such as repudiation, forgery, and collusion towards the transmission process. Therefore, the tradeoff between user privacy protection and data confidentiality is to be investigated.

## IV. Proposed Authenticated Key Management Scheme

In this section, the proposed privacy-preserving attribute-based authentication and vehicular group key management

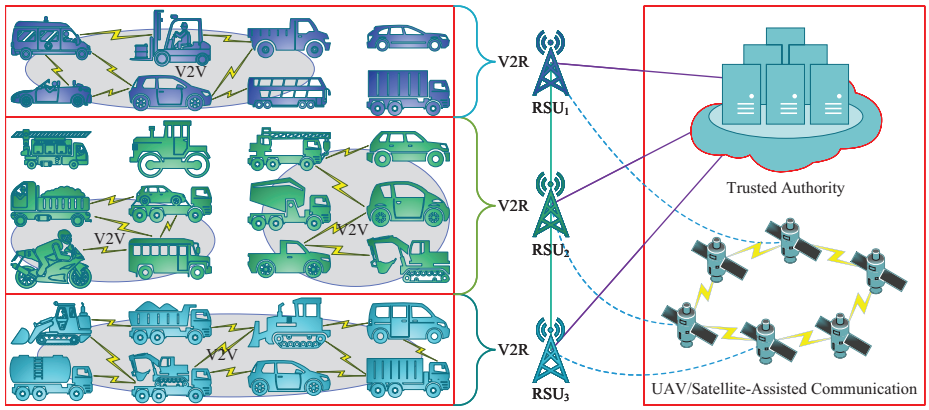


Fig. 1: VANET System Model for Vehicular Communications

scheme is introduced. Intuitively, the proposed scheme can be roughly divided into *vehicle authentication*, *attribute-based vehicular group key distribution*, and *accountable vehicular communication*. The authentication design utilizes the attribute set of each vehicle in the verification process. Upon successful validation towards the requesting vehicles, the dynamic access policy and the corresponding distribution matrix are generated according to flexible access requirements. Subsequently, the vehicular group key is distributed to all entities, while only the accessible vehicles could reveal the shared key correctly. Moreover, the exclusive V2V secure communication channel is constructed independently.

### A. Vehicle Authentication

Initially, it is mandatory for all vehicles to carry out registration prior to the authentication and data delivery process. In this case, the attribute-based registration process to TA is performed, while the corresponding secrets are distributed to each vehicle. Practically, a distinctive attribute set for the individual vehicle can be constructed based on both the vehicle data and driver information. Assuming that $n$ distinctive vehicle attributes including region, address, name, driving license number, model, vehicle identification number (VIN), are extracted and then registered to TA in the offline mode, TA allocates the original secret set $\{k_1^i, k_2^i, \ldots, k_n^i\}$ and the related identity $\mathsf{id}_i$ to the specific vehicle, where $i$ indicates the sequence number and $n$ denotes the predefind constant number of the adopted attributes.

Notably, the secret set is one-to-one mapped to the attribute set and is safely stored by TA and each vehicle. As for TA, the system initialization is conducted, where the crucial global parameters, master keys, and the deployed functions are presented. The two cyclic groups $\mathbb{G}_1$ and $\mathbb{G}_2$ are respectively defined, both are of the same prime order $q$. $P$ is defined as the generator of $\mathbb{G}_1$. The bilinear pairing function $\hat{e}$ is constructed in the form of $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. Furthermore, the cryptographic hash functions $\{H_i\}_{i\in[1,4]}$ and $\{h_i\}_{i\in[1,3]}$ that are utilized in the design, are defined. Particularly, as mentioned above, the construction of $H_2$ is related to the attributes set. For better description, we set $n = 4$. In this case, $(n+2) = 6$ inputs are needed for $H_2$. The corresponding definitions are given as follows: $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $H_2 : \underbrace{\{0,1\}^* \times \cdots \times \{0,1\}^*}_{6} \times \mathbb{G}_1 \rightarrow \mathbb{Z}_q^*$, $H_3 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $H_4 : \{0,1\}^* \times \mathbb{G}_1 \rightarrow \mathbb{Z}_q^*$, and $h_1 : \{0,1\}^* \times \{0,1\}^* \times \mathbb{G}_1 \rightarrow \mathbb{Z}_q^*$, $h_2 : \{0,1\}^* \times \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $h_3 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \rightarrow \mathbb{Z}_q^*$.

At this moment, TA assigns different identity set $\{\mathsf{id}_{\mathsf{rsu}}^j, \mathsf{sk}_{\mathsf{rsu}}^j\}$ to each RSU independently, where $\mathsf{id}_{\mathsf{rsu}}^j \in \{0,1\}^*$ is the pre-configured constant identity, and $\mathsf{sk}_{\mathsf{rsu}}^j \in \mathbb{Z}_q^*$ is the master secret key particularly generated for each RSU. The identity set is safely shared between RSU itself and TA and will be utilized in the following data transmission process in an indirect way. Periodically, the RSU generates the random number $\mathsf{r}_{\mathsf{rsu}}^j$ and calculates its temporary session identity as $\mathsf{ID}_{\mathsf{rsu}}^j = h_1(\mathsf{id}_{\mathsf{rsu}}^j, \mathsf{t}_{\mathsf{rsu}}^1, \mathsf{r}_{\mathsf{rsu}}^j P)$ so that $R_{\mathsf{rsu}}^j = \mathsf{r}_{\mathsf{rsu}}^j[h_2(\mathsf{t}_{\mathsf{rsu}}^1, \mathsf{sk}_{\mathsf{rsu}}^j)]$ and $Q_{\mathsf{rsu}}^j = \mathsf{sk}_{\mathsf{rsu}}^j[h_2(\mathsf{t}_{\mathsf{rsu}}^1, \mathsf{r}_{\mathsf{rsu}}^j)]P$ are issued, which is published along with the current timestamp $\mathsf{t}_{\mathsf{rsu}}^1$ in the form of $\langle \mathsf{t}_{\mathsf{rsu}}^1, \mathsf{ID}_{\mathsf{rsu}}^j, R_{\mathsf{rsu}}^j, Q_{\mathsf{rsu}}^j \rangle$. The adopted session identity $\mathsf{ID}_{\mathsf{rsu}}^j$ is effective only within a certain time interval and will be updated afterward to achieve anonymous transmission.

Subsequently, the authentication process is conducted. The corresponding diagram is shown in Figure 2. Assuming the individual vehicle with a secret set $\{k_1^i, k_2^i, \ldots, k_n^i\}$ is approaching the effective range of RSU with an identity set $\{\mathsf{id}_{\mathsf{rsu}}^j, \mathsf{sk}_{\mathsf{rsu}}^j\}$, similar to the above RSU session identity generation, the vehicle itself generates the random number $\mathsf{r}_{\mathsf{v}}^i$ and updates its vehicle session identity as $\mathsf{ID}_{\mathsf{v}}^i = h_2\left[(\mathsf{ID}_{\mathsf{v}}^i)^*, \mathsf{t}_{\mathsf{v}}^1\right]$, where $(\mathsf{ID}_{\mathsf{v}}^i)^*$ denotes the previous session identity in the last RSU range. In the next, for each $k_{\ell\in[1,n]}^i$, the vehicle collects the published $R_{\mathsf{rsu}}^j$ and calculates its corresponding $T_i^\ell$ according to $T_i^\ell = h_2(\mathsf{id}_i, k_\ell^i)H_1(\mathsf{r}_{\mathsf{v}}^i)R_{\mathsf{rsu}}^j$.

With the acquired $\mathsf{ID}_{\mathsf{rsu}}^j$ and secret set $\{k_1^i, k_2^i, \ldots, k_n^i\}$, the vehicle calculates $\eth_i = H_2(\mathsf{t}_{\mathsf{v}}^1, \mathsf{id}_i, k_1^i, \ldots, k_n^i, \mathsf{r}_{\mathsf{v}}^i)$ and $\partial_i = H_3(\mathsf{t}_{\mathsf{v}}^1, \mathsf{ID}_{\mathsf{rsu}}^j, \mathsf{ID}_{\mathsf{v}}^i, \eth_i, \sum_{\ell=1}^n T_i^\ell)$. Therefore, the credential for mutual verification is computed as

$$U_i = h_3\left(\mathsf{t}_{\mathsf{v}}^1, \mathsf{id}_i, \prod_{\ell=1}^n k_\ell^i\right)Q_{\mathsf{rsu}}^j + \left(\partial_i H_1(\mathsf{r}_{\mathsf{v}}^i)R_{\mathsf{rsu}}^j + H_1\left(H_1(\mathsf{r}_{\mathsf{v}}^i)\left(\sum_{\ell=1}^n h_2(\mathsf{id}_i, k_\ell^i)\right)\right)\right)P, \quad (1)$$

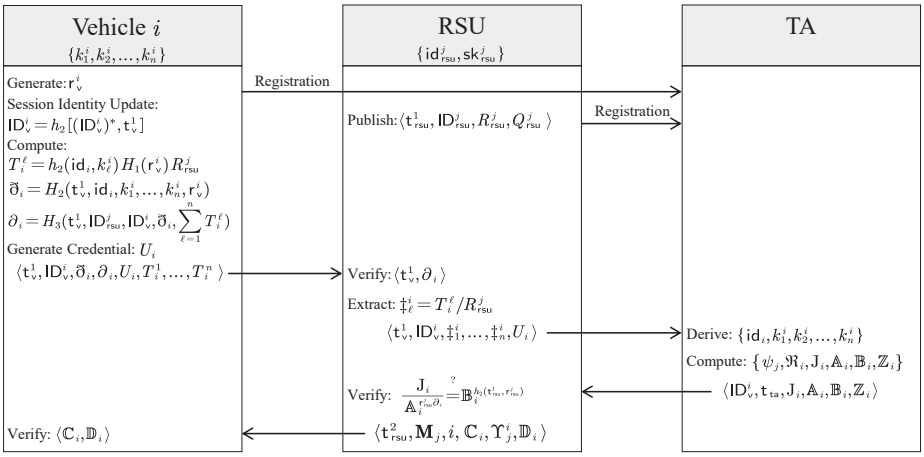


Fig. 2: Diagram for the Authentication Process

where $\mathsf{t}_{\mathsf{v}}^1$ denotes the latest timestamp. Finally, the requesting packet to be delivered is composed as $\left\langle \mathsf{Request}, \mathsf{t}_{\mathsf{v}}^1, \mathsf{ID}_{\mathsf{v}}^i, \eth_i, \partial_i, U_i, T_i^1, \ldots, T_i^n \right\rangle$.

Upon receiving the authentication request, RSU verifies the freshness of the timestamp $\mathsf{t}_{\mathsf{v}}^1$. If matches, the validity of the received $\partial_i$ is verified according to the acquired $\{\mathsf{ID}_{\mathsf{v}}^i, \eth_i, T_i^1, \ldots, T_i^n\}$. Afterward, for $\ell \in [1, n]$, RSU extracts $\ddagger_\ell^i = T_i^\ell / R_{\mathsf{rsu}}^j$ and uploads the vehicle information $\left\langle \mathsf{t}_{\mathsf{v}}^1, \mathsf{ID}_{\mathsf{v}}^i, \ddagger_1^i, \ldots, \ddagger_n^i, U_i \right\rangle$ to the remote TA for final validation.

Upon receiving the above vehicle information from RSU, TA extracts the previously updated vehicle identities from its record, which relates to the active vehicles nearby RSUs. TA then attempts to compute $h_2\left[(\mathsf{ID}_{\mathsf{v}}^i)^*, \mathsf{t}_{\mathsf{v}}^1\right] \stackrel{?}{=} \mathsf{ID}_{\mathsf{v}}^i$ to figure out the real identity. Note that the identity of the requesting vehicle have already been verified and recorded by the neighboring RSUs in the previous time, if the vehicle itself is legitimate and valid. The original identity $\mathsf{id}_i$ and the secret set $\left\{k_1^i, k_2^i, \ldots, k_n^i\right\}$ can be derived accordingly. Subsequently, TA outputs $\psi_j = \mathsf{sk}_{\mathsf{rsu}}^j P$ and $\Re_i = H_1(\mathsf{r}_{\mathsf{v}}^i) P$, as well as

$$\begin{cases} \mathrm{J}_i = \hat{e}\left(U_i - H_1\left(\sum_{\ell=1}^n \ddagger_\ell^i\right) P, P\right) \\ \mathbb{A}_i = \hat{e}\left(h_2\left(\mathsf{t}_{\mathsf{rsu}}^1, \mathsf{sk}_{\mathsf{rsu}}^j\right) P, \Re_i\right) \\ \mathbb{B}_i = \hat{e}\left(h_3\left(\mathsf{t}_{\mathsf{v}}^1, \mathsf{id}_i, \prod_{\ell=1}^n k_\ell^i\right) P, \psi_j\right) \\ \mathbb{Z}_i = h_1\left(\mathsf{t}_{\mathsf{ta}}, h_3(\mathrm{J}_i, \mathbb{A}_i, \mathbb{B}_i), h_3(\mathrm{J}_i, \mathsf{id}_{\mathsf{rsu}}^j, \mathsf{sk}_{\mathsf{rsu}}^j) P\right) \end{cases} \tag{2}$$

and forwards $\langle \mathsf{ID}_{\mathsf{v}}^i, \mathsf{t}_{\mathsf{ta}}, \mathrm{J}_i, \mathbb{A}_i, \mathbb{B}_i, \mathbb{Z}_i \rangle$ to RSU. Notably, the group key $\aleph_j$ is also attached as the shared credential for V2V communication within the current RSU range. With the acquired information, RSU checks the validity of $\mathbb{Z}_i$ for data integrity preservation and conducts the validation as $\frac{\mathrm{J}_i}{\mathbb{A}_i^{r_{\mathsf{rsu}}^j \partial_i}} \stackrel{?}{=} \mathbb{B}_i^{h_2(\mathsf{t}_{\mathsf{rsu}}^1, \mathsf{r}_{\mathsf{rsu}}^j)}$. If matches, the validity of the vehicle can be proved.

The batch validation design for the multiple-vehicles scenario is also provided. In this case, it is assumed that there are $\hbar$ vehicles to be simultaneously authenticated by a single RSU. Therefore, the TA calculates $\mathcal{S}_i = \hat{e}\left(\sum_{i=1}^{\hbar}\left(U_i - H_1\left(\sum_{\ell=1}^n \ddagger_\ell^i\right) P\right), P\right)$ and forwards it to RSU so that the RSU is able to carry out the batch verification process on $\hbar$ vehicles at a time according to $\frac{\mathcal{S}_i}{\prod_{i=1}^{\hbar} \mathbb{A}_i^{r_{\mathsf{rsu}}^j \partial_i}} \stackrel{?}{=} \left(\prod_{i=1}^{\hbar} \mathbb{B}_i\right)^{h_2(\mathsf{t}_{\mathsf{rsu}}^1, \mathsf{r}_{\mathsf{rsu}}^j)}$. Similarly, the correctness is as follows.

$$\begin{aligned} L.H.S. =& \frac{\hat{e}\left(\sum_{i=1}^{\hbar} U_i - \sum_{i=1}^{\hbar} H_1\left(\sum_{\ell=1}^n \ddagger_\ell^i\right) P, P\right)}{\prod_{i=1}^{\hbar} \hat{e}\left(\partial_i \mathsf{r}_{\mathsf{rsu}}^j h_2\left(\mathsf{t}_{\mathsf{rsu}}^1, \mathsf{sk}_{\mathsf{rsu}}^j\right) P, \Re_i\right)} \\ =& \frac{1}{\hat{e}\left(\sum_{i=1}^{\hbar} \partial_i R_{\mathsf{rsu}}^j P, \Re_i\right)} \times \hat{e}\left(\sum_{i=1}^{\hbar} \partial_i R_{\mathsf{rsu}}^j \Re_i \right. \\ & \left. + \sum_{i=1}^{\hbar} h_3\left(\mathsf{t}_{\mathsf{v}}^1, \mathsf{id}_i, \prod_{\ell=1}^n k_\ell^i\right) Q_{\mathsf{rsu}}^j, P\right) \\ =& \hat{e}\left(\sum_{i=1}^{\hbar} h_3\left(\mathsf{t}_{\mathsf{v}}^1, \mathsf{id}_i, \prod_{\ell=1}^n k_\ell^i\right) Q_{\mathsf{rsu}}^j, P\right). \end{aligned} \tag{3}$$

Meanwhile,

$$\begin{aligned} R.H.S. =& \prod_{i=1}^{\hbar} \hat{e}\left(h_2(\mathsf{t}_{\mathsf{rsu}}^1, \mathsf{r}_{\mathsf{rsu}}^j) h_3\left(\mathsf{t}_{\mathsf{v}}^1, \mathsf{id}_i, \prod_{\ell=1}^n k_\ell^i\right) P, \mathsf{sk}_{\mathsf{rsu}}^j P\right) \\ =& L.H.S.. \end{aligned} \tag{4}$$

Intuitively, because $L.H.S. = R.H.S.$, the $\hbar$ vehicles are recognized as the validated entities simultaneously. The batch authentication process is finished.

### *B. Attribute-Based Vehicular Group Key Distribution*

After successfully verify all $\hbar$ vehicles, RSU then acquires $\{T_i^1, \ldots, T_i^n\}_{i \in [1, \hbar]}$, which indicate the unique attributes and properties of each vehicle, respectively. At this moment, RSU generates the corresponding access structure using the attribute

sets that belongs to the $\hbar$ verified vehicles. Initially, the feature set $\mathbf{F}$ is defined as

$$\mathbf{F} = \begin{pmatrix} k_1^1 & \cdots & k_\ell^1 & \cdots & k_n^1 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ k_1^i & \cdots & k_\ell^i & \cdots & k_n^i \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ k_1^\hbar & \cdots & k_\ell^\hbar & \cdots & k_n^\hbar \end{pmatrix}, \tag{5}$$

which is composed of $n\hbar$ attribute-related secrets $\{k_\ell^i\}_{i\in[1,\hbar],\ell\in[1,n]}$. Accordingly, the RSU is able to construct the access structure as $\mathcal{P} = \overbrace{\left(k_1^1 \wedge \ldots k_\ell^1 \wedge \ldots k_n^1\right)}^{\mathbf{v}_1} \cdots \vee \overbrace{\left(k_1^\hbar \wedge \ldots k_\ell^\hbar \wedge \ldots k_n^\hbar\right)}^{\mathbf{v}_\hbar} = \bigvee_{i=1}^{\hbar}\left(\bigwedge_{\ell=1}^{n} k_\ell^i\right)$ Notably, the construction of $\mathcal{P}$ is subject to flexible requirements and can be organized and updated by individual RSU. Hence, the minimal access set is the values in each row of the feature set $\mathbf{F}$. The access policy matrix is generated in the next. According to linear integer secret sharing (LISS) [32], the partial matrix $\mathbb{H}^i$ for access policy $\bigwedge_{\ell=1}^{n} k_\ell^i$ is

$$\mathbb{H}^i = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ 0 & 0 & \ldots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & \ldots & 0 \end{bmatrix}_{n\times n}. \tag{6}$$

Let $(\mathbb{L}_i, \mathbb{R}_i)$ be the first and the rest columns of $\mathbb{H}^i$, respectively. For $\mathcal{P} = \bigvee_{i=1}^{\hbar}\left(\bigwedge_{\ell=1}^{n} k_\ell^i\right)$, the corresponding distribution matrix $\mathbf{M}_j$ of RSU with identity $\mathsf{id}_{\mathsf{rsu}}^j$ can be expressed as

$$\begin{aligned} \mathbf{M}_j &= \begin{bmatrix} \mathbb{L}_1 & \mathbb{R}_1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \mathbb{L}_\hbar & 0 & \ldots & \mathbb{R}_\hbar \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 & \ldots & 1 & & & & \\ 0 & 0 & \ldots & 1 & & & \mathbf{0} & \\ \vdots & \vdots & \ddots & \vdots & \ldots & & & \\ 0 & 1 & \ldots & 0 & & & & \\ \vdots & & \vdots & & \ddots & & \vdots & \\ 1 & & & & & 1 & \ldots & 1 \\ 0 & & \mathbf{0} & & & 0 & \ldots & 1 \\ \vdots & & & & \ldots & \vdots & \ddots & \vdots \\ 0 & & & & & 1 & \ldots & 0 \end{bmatrix}, \end{aligned} \tag{7}$$

which is displayed as a $[n\hbar] \times [\hbar(n-1)+1]$ matrix. Every $n$ rows are mapped to a specific vehicle according to the sequence. At this point, RSU randomly selects $\{\Psi_j^2, \ldots, \Psi_j^{\hbar(n-1)+1}\}$ and generates the vector $\rho_j = \left[\aleph_j, \Psi_j^2, \ldots, \Psi_j^{\hbar(n-1)+1}\right]^{\mathbf{T}}$, where the group key $\aleph_j$ is previously allocated by TA. The calculation for key distribution can be conducted as $\mathbf{M}_j \cdot \rho_j = \left[\Lambda_j^1, \ldots, \Lambda_j^n, \Lambda_j^{n+1}, \ldots, \Lambda_j^{2n}, \ldots, \Lambda_j^{\hbar n}\right]^{\mathbf{T}}$. In this case, RSU gets the result containing $n\hbar$ values, among which every $n$ items are related to a specific vehicle. Subsequently, for $\ell \in [1, n]$, by using the aforementioned $\ddagger_\ell^i = T_i^\ell / R_{\mathsf{rsu}}^j = h_2(\mathsf{id}_i, k_\ell^i) H_1(\mathsf{r}_{\mathsf{v}}^i)$, the final output can be generated as

$$\mathsf{output}_j = \begin{bmatrix} \Lambda_j^1 \ddagger_1^1 & \cdots & \Lambda_j^1 \ddagger_n^1 & \cdots & \Lambda_j^1 \ddagger_n^\hbar \\ \vdots & \ddots & \vdots & & \vdots \\ \Lambda_j^n \ddagger_1^1 & \cdots & \Lambda_j^n \ddagger_n^1 & \cdots & \Lambda_j^n \ddagger_n^\hbar \\ \vdots & & \vdots & \ddots & \vdots \\ \Lambda_j^{\hbar n} \ddagger_1^1 & \cdots & \Lambda_j^{\hbar n} \ddagger_n^1 & \cdots & \Lambda_j^{\hbar n} \ddagger_n^\hbar \end{bmatrix}_{[\hbar n]\times[\hbar n]}. \tag{8}$$

Notably, the diagonal elements are extracted as

$$\left\{\Lambda_j^1 \ddagger_1^1, \ldots, \Lambda_j^n \ddagger_n^1, \Lambda_j^{n+1} \ddagger_1^2, \ldots, \Lambda_j^{2n} \ddagger_n^2, \ldots, \Lambda_j^{\hbar n} \ddagger_n^\hbar\right\}, \tag{9}$$

which will be allocated to the $\hbar$ vehicles in sequence. In other words, vehicle $i \in [1, \hbar]$ will be associated with $\Upsilon_j^i = \left\{\Lambda_j^{(i-1)n+1} \ddagger_1^i, \ldots, \Lambda_j^{in} \ddagger_n^i\right\}$. At this moment, RSU computes $\mathbb{C}_i = h_1\left(\mathsf{ID}_{\mathsf{v}}^i, H_1(\mathsf{r}_{\mathsf{v}}^i), \mathsf{J}_i\right)$ and $\mathbb{D}_i = H_3\left(\mathsf{t}_{\mathsf{rsu}}^2, \mathsf{ID}_{\mathsf{rsu}}^j, \mathbf{M}_j, i, \Upsilon_j^i\right)$ and delivers the group key distribution packet $\left\langle \mathsf{t}_{\mathsf{rsu}}^2, \mathbf{M}_j, i, \mathbb{C}_i, \Upsilon_j^i, \mathbb{D}_i \right\rangle$ to each vehicle, where the access matrix $\mathbf{M}_j$, sequence number $i$, and other relevant information are attached. Overall, $\hbar$ packets are distributed to the vehicle group.

In the final vehicle validation process, the vehicle $i \in [1, \hbar]$ first checks the validity of the acquired $\mathbb{C}_i$ and $\mathbb{D}_i$. If matches, the vehicle confirms its sequence number $i$ so that the calculation on $\{\zeta_1^i, \ldots, \zeta_n^i\}$ is performed as

$$\begin{cases} \zeta_1^i = \Lambda_j^{(i-1)n+1} \ddagger_1^i \left(\ddagger_1^i\right)^{-1} = \Lambda_j^{(i-1)n+1} \\ \vdots \quad \vdots \\ \zeta_n^i = \Lambda_j^{in} \ddagger_n^i \left(\ddagger_n^i\right)^{-1} = \Lambda_j^{in} \end{cases}. \tag{10}$$

Thereafter, the vehicle extracts the $[in+1, \ldots, (i+1)n]$ rows so that a new $[n] \times [\hbar(n-1)+1]$ matrix $\mathbf{N}_i$ is generated. Given $\varphi = \underbrace{[1, 0, \ldots, 0]}_{\hbar(n-1)+1}^{\mathbf{T}}$, the vehicle is able to calculate $\xi_i$ according to $\mathbf{N}_i^{\mathbf{T}} \cdot \xi_i = \varphi$. Assuming that $\xi_i = \left[\Gamma_1^i, \ldots, \Gamma_n^i\right]^{\mathbf{T}}$, the vehicle then reconstructs the group key $\aleph_j$ as $\zeta_1^i \Gamma_1^i + \cdots + \zeta_n^i \Gamma_n^i = \sum_{\ell=1}^{n}\left(\zeta_\ell^i \Gamma_\ell^i\right) = \Lambda_j^{(i-1)n+1} + \cdots + \Lambda_j^{in} = \aleph_j$. The group key $\aleph_j$ is successfully delivered to the $\hbar$ validated vehicles. The mutual authentication and vehicular group key distribution process are finished.

In the next, a concrete example with $n = 4$ and $\hbar = 2$ is presented: Assuming the two vehicles have passed the authentication process, RSU then acquires $\{T_1^1, \ldots, T_1^4\}$ and $\{T_2^1, \ldots, T_2^4\}$. Therefore, the feature set is generated as $\mathbf{F} = \begin{pmatrix} k_1^1 & k_2^1 & k_3^1 & k_4^1 \\ k_1^2 & k_2^2 & k_3^2 & k_4^2 \end{pmatrix}$. Accordingly, the access structure is extracted as $\mathcal{P} = \bigvee_{i=1}^{2}\left(\bigwedge_{\ell=1}^{4} k_\ell^i\right)$. The corresponding

distribution matrix $\mathbf{M}_j$ can be calculated as

$$\mathbf{M}_j = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}. \tag{11}$$

Notably, the diagonal elements are extracted as $\left\{\Lambda_j^{1\ddagger 1}, \Lambda_j^{2\ddagger 2}, \Lambda_j^{3\ddagger 1}, \Lambda_j^{4\ddagger 1}, \Lambda_j^{5\ddagger 2}, \Lambda_j^{6\ddagger 2}, \Lambda_j^{7\ddagger 2}, \Lambda_j^{8\ddagger 2}\right\}$, which will be allocated to the 2 vehicles in sequence. That is, RSU computes and delivers $\left\langle \mathsf{t}_{\mathsf{rsu}}^2, \mathbf{M}_j, 1, \mathbb{C}_1, \Upsilon_j^1, \mathbb{D}_1 \right\rangle$ and $\left\langle \mathsf{t}_{\mathsf{rsu}}^2, \mathbf{M}_j, 2, \mathbb{C}_2, \Upsilon_j^2, \mathbb{D}_2 \right\rangle$ to the vehicle group. Following this way, the two vehicles reconstruct the group key $\aleph_j$ as $\zeta_1^1\Gamma_1^1 + \cdots + \zeta_4^1\Gamma_4^1 = \Lambda_j^1 + \cdots + \Lambda_j^4 = \zeta_1^2\Gamma_1^2 + \cdots + \zeta_4^2\Gamma_4^2 = \Lambda_j^5 + \cdots + \Lambda_j^8 = \aleph_j$. The group key $\aleph_j$ is successfully delivered. The mutual authentication and vehicular group key distribution process are finished.

### C. Accountable Vehicular Communication

In this section, the accountable V2V data sharing is executed, where an exclusive chain-based message delivery mechanism is constructed independently. For privacy-preserving, the crucial vehicular data is locally stored in the participant storage, while the metadata packet is uploaded to the remote cloud server via RSU surveillance. As introduced above, the legitimate vehicles that approach the RSU range have successfully passed the verification process. The group key $\aleph_j$ for vehicular communication is issued and shared among all participants so that the V2V data exchange among the $\hbar$ vehicles can be achieved.

Upon successful extraction of the group key, the verified vehicles update their identities as $\mathsf{ID}_\Delta^i = H_4\left(\mathbb{C}_i, \mathbb{A}_i\right)_{i\in[1,\hbar]}$. The V2V exclusive communication mechanism is constructed based on the homomorphic encryption infrastructure. That is, $\mathcal{R}_i$ and $\mathcal{Q}_i$ denote the prime values with $\gcd\left(\mathcal{R}_i\mathcal{Q}_i, (\mathcal{R}_i-1)(\mathcal{Q}_i-1)\right) = 1$. Subsequently, the vehicle computes $\mathcal{G}_i = \mathcal{R}_i\mathcal{Q}_i$ and randomly chooses $\hbar_i \in \mathbb{Z}_{\mathcal{G}_i^2}^*$. Afterwards, the vehicle computes $\mathbb{E}_i = H_3\left(\mathsf{t}_\Delta^i, \mathsf{ID}_\Delta^i, \mathcal{G}_i, \hbar_i, \aleph_j\right)$, $\varrho_i = \mathrm{lcm}\left(\mathcal{R}_i - 1, \mathcal{Q}_i - 1\right)$, $\varkappa_i = \ell_i\left(\hbar_i^{\varrho_i} \bmod \mathcal{G}_i^2\right) \bmod \mathcal{G}_i$, where $\ell_i(x) = (x-1)/\mathcal{G}_i$ and $\mathsf{t}_\Delta^i$ denotes the current timestamp. At this point, the V2V encryption key pair $\{\mathcal{G}_i, \hbar_i\}$ and decryption key pair $\{\varrho_i, \varkappa_i\}$ are generated. Each vehicle then publishes $\left\langle \mathsf{t}_\Delta^i, \mathsf{ID}_\Delta^i, \mathcal{G}_i, \hbar_i, \mathbb{E}_i \right\rangle$, which will be used during the construction of the specific one-to-one data sharing channel.

The V2V data sharing frame is briefly illustrated in Fig. 3. $\mathrm{Vehicle}_\mathsf{S}$ and $\mathrm{Vehicle}_\mathsf{R}$ represent the message sender and receiver, respectively. $\left\{\mathsf{ID}_\Delta^\mathsf{S}, \mathsf{ID}_\Delta^\mathsf{R}\right\}$ denotes the updated identities for $\mathrm{Vehicle}_\mathsf{S}$ and $\mathrm{Vehicle}_\mathsf{R}$. In the assumption, $\mathrm{Vehicle}_\mathsf{S}$ sends the vehicular data $M$ to the receiver $\mathrm{Vehicle}_\mathsf{R}$ with $\mathsf{ID}_\Delta^\mathsf{R}$. $\mathrm{Vehicle}_\mathsf{S}$ then first verifies the published $\mathbb{E}_i$ from $\mathrm{Vehicle}_\mathsf{R}$. Since the previously distributed group key $\aleph_j$ is involved, the validity of $\mathbb{E}_i$ is guaranteed, indicating that $\mathrm{Vehicle}_\mathsf{R}$ is in the vehicular group. $\mathrm{Vehicle}_\mathsf{S}$ then calculates $\wp_i = Enc_{\langle \mathcal{G}_i, \hbar_i\rangle}^{\mathsf{r}_\mathsf{v}^i}(\mathsf{ID}_\Delta^\mathsf{S} || M)$ and $\Im_i = h_3(\aleph_j, \mathsf{ID}_\Delta^\mathsf{R}, \wp_i)$. The vehicle

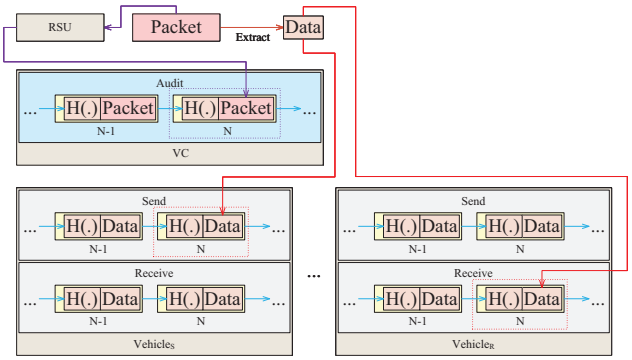


Fig. 3: Accountable Vehicular Communication Frame

identity is updated as $\mathsf{ID}_\Delta^\mathsf{R} \leftarrow h_2\left(\mathsf{ID}_\Delta^\mathsf{R}, \aleph_j\right)$ such that the packet $\left\langle \mathsf{t}_\Delta^\mathsf{S}, \mathsf{ID}_\Delta^\mathsf{R}, \wp_i, \Im_i \right\rangle$ is issued and sent. Notably, the $\mathrm{Vehicles}_\mathsf{S}$ maintains two distinctive hash chains for recording the sent and received messages. The metadata regarding the message delivery process is safely stored whenever a message is sent or received. As shown in Fig. 3, the vehicular data $M$ sent to $\mathrm{Vehicle}_\mathsf{R}$ is preserved in a block of the chain, where the detailed timestamp, receiver identity are also attached. The sending chain of $\mathrm{Vehicles}_\mathsf{S}$ is updated accordingly.

$\mathrm{Vehicle}_\mathsf{R}$ validates the freshness and the integrity via $\left\{\mathsf{t}_\Delta^\mathsf{S}, \Im_i\right\}$ upon receiving the packet. The homomorphic decryption key pair $\{\varrho_i, \varkappa_i\}$ is adopted to $\wp_i$ such that the original data $\left\{\mathsf{ID}_\Delta^\mathsf{S}, M\right\}$ is extracted. At this moment, the exclusive V2V data delivery process is completed. The vehicular data $M$ is transmitted. Similarly, $\mathrm{Vehicle}_\mathsf{R}$ updates the received hash chain with the decrypted $M$ and other metadata including the sender identity $\mathsf{ID}_\Delta^\mathsf{S}$ and timestamp $\mathsf{t}_\Delta^\mathsf{S}$. Furthermore, the RSU also observes the sending packet $\left\langle \mathsf{t}_\Delta^\mathsf{S}, \mathsf{ID}_\Delta^\mathsf{R}, \wp_i, \Im_i \right\rangle$ so that the packet is uploaded to TA in the original form. That is, TA and RSU are unable to decrypt but only record the packet itself for future auditing. The transmitted data $M$ is recorded in the sending chain of the sender, the receiving chain of the receiver, while the raw packet is managed in the auditing chain of TA. In this case, the exclusive and private V2V communication channel is built. As for possible disputes and malicious behaviors, for instance, some users may take advantage of the above private V2V data sharing channel and send fraud messages. In this case, the TA is able to check the auditing chain and compares the information with a certain block on both the sender and receiver sides. The non-repudiation property can be provided.

## V. Security Analysis

In this section, the vital security properties are analyzed with the purpose of demonstrating the proposed design is provably secure. The security comparisons with the state-of-the-arts regarding significant characteristics are shown as well.

### A. Security Analysis

**Proposition 1** (Message Unforgeability)**.** *The proposed scheme is provably unforgeable towards chosen message at-*

*tack (CMA) under the random oracle model, if the CDHP is intractable.*

*Proof.* In the formal way, the unforgeability in terms of the proposed design can be demonstrated with the following game $\mathscr{G}_1$. $\mathscr{A}_1$ is defined as a probabilistic polynomial time (PPT) adversary with the capability of violating the AKM scheme. The utilized hash functions in $\mathscr{G}_1$ are assumed to be random oracles. A challenger $\mathscr{C}_1$ is constructed in order to address the CDHP with a non-negligible probability by executing the corresponding queries from the subroutine $\mathscr{A}_1$. Notably, $\mathscr{C}_1$ has the ability to simulate all the following oracles and maintains the related hash recording lists as well. The queries of $\mathscr{C}_1$ can be adaptively issued by the adversary $\mathscr{A}_1$ in the following form:

- *Setup-Oracle:* With an instance $\left(R^j_{\mathsf{rsu}}P, \Re_i\right) = (aP, bP)$ for some $a, b \in \mathbb{Z}^*_q$, $\mathscr{C}_1$ returns the system parameters set $\{\hat{e}, \mathbb{G}_1, \mathbb{G}_2, P, q\}$ to the adversary $\mathscr{A}_1$.
- $h_1$*-Oracle:* It's assumed that $\mathscr{A}_1$ is not capable of calculating the hash function $h_1(\cdot)$. In order to give response to the query, $\mathscr{C}_1$ organizes a hash recording list $h^1_{list}$ in the form of $\langle \circledast_i, \tau_i \rangle$, which is initialized to be empty. Note that $\circledast_i$ denotes the tuple $\left\langle \mathsf{id}^j_{\mathsf{rsu}}, \mathsf{t}^1_{\mathsf{rsu}}, \mathsf{r}^j_{\mathsf{rsu}}P \right\rangle$, where $\mathsf{r}^j_{\mathsf{rsu}}P \in \mathbb{G}_1$. In this case, when the adversary $\mathscr{A}_1$ invokes the query with a particular input value set $\circledast_i$, $\mathscr{C}_1$ verifies whether the parameter $\circledast_i$ exists in $h^1_{list}$, and carried out as follows:
  - Assuming the value pair $\circledast_i$ exists in $h^1_{list}$, $\mathscr{C}_1$ outputs $\tau_i = h_1(\mathsf{id}^j_{\mathsf{rsu}}, \mathsf{t}^1_{\mathsf{rsu}}, \mathsf{r}^j_{\mathsf{rsu}}P)$ to $\mathscr{A}_1$.
  - Otherwise, $\mathscr{C}_1$ randomly selects $\tau_i \in \mathbb{Z}^*_q$ and delivers it to $\mathscr{A}_1$. Meanwhile, $\langle \circledast_i, \tau_i \rangle$ will be added to $h^1_{list}$ subsequently.
- $H_1$*-Oracle:* It's assumed that $\mathscr{A}_1$ is not capable of calculating the hash function $H_1(\cdot)$. In order to give response to the query, $\mathscr{C}_1$ organizes a hash recording list $H^1_{list}$ in the form of $\langle \odot_i, \tau_i \rangle$, which is initialized to be empty. $\odot_i$ denotes the tuple $\left\langle \mathsf{r}^i_{\mathsf{v}} \right\rangle$. In this case, when the adversary $\mathscr{A}_1$ invokes the query with a particular input value set $\odot_i$, $\mathscr{C}_1$ checks whether the parameter $\odot_i$ exists in $H^1_{list}$, and performs as follows:
  - Assuming the value pair $\odot_i$ exists in $H^1_{list}$, $\mathscr{C}_1$ outputs $\tau_i = H_1\left(\mathsf{r}^i_{\mathsf{v}}\right)$ to $\mathscr{A}_1$.
  - Otherwise, $\mathscr{C}_1$ randomly selects $\tau_i \in \mathbb{Z}^*_q$ and delivers it to $\mathscr{A}_1$. Meanwhile, $\langle \odot_i, \tau_i \rangle$ will be added to $H^1_{list}$ subsequently.
- $h_3$*-Oracle:* It's assumed that $\mathscr{A}_1$ is not capable of calculating the hash function $h_3(\cdot)$. In order to give response to the query, $\mathscr{C}_1$ organizes a hash recording list $h^3_{list}$ in the form of $\langle \ominus_i, \tau_i \rangle$, which is initialized to be empty. $\ominus_i$ denotes the tuple $\left\langle \mathsf{t}^1_{\mathsf{v}}, \mathsf{id}_i, \prod^n_{\ell=1} k^i_\ell \right\rangle$. In this case, when the adversary $\mathscr{A}_1$ invokes the query with a particular input value set $\ominus_i$, $\mathscr{C}_1$ checks whether the parameter $\ominus_i$ exists in $h^3_{list}$, and performs as follows:
  - Assuming the value pair $\ominus_i$ exists in $h^3_{list}$, $\mathscr{C}_1$ outputs $\tau_i = h_3\left(\mathsf{t}^1_{\mathsf{v}}, \mathsf{id}_i, \prod^n_{\ell=1} k^i_\ell\right)$ to $\mathscr{A}_1$.
  - Otherwise, $\mathscr{C}_1$ randomly selects $\tau_i \in \mathbb{Z}^*_q$ and delivers it to $\mathscr{A}_1$. Meanwhile, $\langle \ominus_i, \tau_i \rangle$ will be added to $h^3_{list}$ subsequently.
- $H_3$*-Oracle:* It's assumed that $\mathscr{A}_1$ is not capable of calculating the hash function $H_3(\cdot)$. In order to give response to the query, $\mathscr{C}_1$ organizes a hash recording list $H^3_{list}$ in the form of $\langle \circledcirc_i, \tau_i \rangle$, which is initialized to be empty. $\circledcirc_i$ denotes the tuple $\left\langle \mathsf{t}^1_{\mathsf{v}}, \mathsf{ID}^j_{\mathsf{rsu}}, \mathsf{ID}^i_{\mathsf{v}}, \eth_i, \sum^n_{\ell=1} T^\ell_i \right\rangle$. In this case, when the adversary $\mathscr{A}_1$ invokes the query with a particular input value set $\circledcirc_i$, $\mathscr{C}_1$ checks whether the parameter $\circledcirc_i$ exists in $H^3_{list}$, and performs as follows:
  - Assuming the value pair $\circledcirc_i$ exists in $H^3_{list}$, $\mathscr{C}_1$ outputs $\tau_i = H_3(\mathsf{t}^1_{\mathsf{v}}, \mathsf{ID}^j_{\mathsf{rsu}}, \mathsf{ID}^i_{\mathsf{v}}, \eth_i, \sum^n_{\ell=1} T^\ell_i)$ to $\mathscr{A}_1$.
  - Otherwise, $\mathscr{C}_1$ randomly selects $\tau_i \in \mathbb{Z}^*_q$ and delivers it to $\mathscr{A}_1$. Meanwhile, $\langle \circledcirc_i, \tau_i \rangle$ will be added to $H^3_{list}$ subsequently.
- *Extracting-Oracle:* Upon receiving the query with the message $\circledast_i$, by using $\circledast_i$ as input, $\mathscr{C}_1$ conducts $h_1$ query and then outputs the relevant tuple $\langle \circledast_i, \tau_i \rangle$. $\langle \circledast_i, \tau_i \rangle$ is recorded in $h^1_{list}$. Similarly, with the input value set $\langle \odot_i, \tau_i \rangle$, $\langle \ominus_i, \tau_i \rangle$, and $\langle \circledcirc_i, \tau_i \rangle$, $H_1$ query, $h_3$ query, and $H_3$ query are performed by $\mathscr{C}_1$, respectively. $\mathscr{C}_1$ generates the random values $\mathsf{r}^j_{\mathsf{rsu}}, \mathsf{t}^1_{\mathsf{rsu}} \in \mathbb{Z}^*_q$ and computes $\langle \partial_i, U_i, \mathrm{J}_i, \mathbb{A}_i, \mathbb{B}_i \rangle$, where $\frac{\mathrm{J}_i}{\mathbb{A}_i^{\mathsf{r}^j_{\mathsf{rsu}}\partial_i}} = \mathbb{B}_i^{h_2(\mathsf{t}^1_{\mathsf{rsu}}, \mathsf{r}^j_{\mathsf{rsu}})}$ holds. The calculated tuple $\langle \partial_i, U_i, \mathrm{J}_i, \mathbb{A}_i, \mathbb{B}_i \rangle$ will be sent to $\mathscr{A}_1$. All the signatures that are generated by $\mathscr{C}_1$ are considered to be indistinguishable from those generated by legal entities.

In this way, the adversary $\mathscr{A}_1$ outputs a message $\left\{\mathsf{ID}^i_{\mathsf{v}}, \partial_i, U_i, \mathrm{J}_i, \mathbb{A}_i, \mathbb{B}_i\right\}$. $\mathscr{C}_1$ then checks whether the equation $\frac{\mathrm{J}_i}{\mathbb{A}_i^{\mathsf{r}^j_{\mathsf{rsu}}\partial_i}} \stackrel{?}{=} \mathbb{B}_i^{h_2(\mathsf{t}^1_{\mathsf{rsu}}, \mathsf{r}^j_{\mathsf{rsu}})}$ holds. If it does not hold, $\mathscr{C}_1$ terminates the process. Within a polynomial time, by using Forking Lemma [33], $\mathscr{A}_1$ is capable of getting another valid signature $\left\{\mathsf{ID}^i_{\mathsf{v}}, \partial_i, U^*_i, \mathrm{J}^*_i, \mathbb{A}_i, \mathbb{B}^*_i\right\}$ after querying $\mathscr{C}_1$, if the process is executed again with a different choice of $h_3(\cdot)$. Notably, both tuples can pass the authentication process such that $\frac{\mathrm{J}_i}{\mathbb{A}_i^{\mathsf{r}^j_{\mathsf{rsu}}\partial_i}} = (\mathbb{B}_i)^{h_2(\mathsf{t}^1_{\mathsf{rsu}}, \mathsf{r}^j_{\mathsf{rsu}})}$ and $\frac{\mathrm{J}^*_i}{\mathbb{A}_i^{\mathsf{r}^j_{\mathsf{rsu}}\partial_i}} = (\mathbb{B}^*_i)^{h_2(\mathsf{t}^1_{\mathsf{rsu}}, \mathsf{r}^j_{\mathsf{rsu}})}$ hold. For brief description, let $h^*_3 = h^*_3\left(\mathsf{t}^1_{\mathsf{v}}, \mathsf{id}_i, \prod^n_{\ell=1} k^i_\ell\right)$ and $h_3 = h_3\left(\mathsf{t}^1_{\mathsf{v}}, \mathsf{id}_i, \prod^n_{\ell=1} k^i_\ell\right)$ such that

$$\begin{cases} \left(\frac{\mathrm{J}_i}{\mathbb{A}_i^{\mathsf{r}^j_{\mathsf{rsu}}\partial_i}}\right)^{h^*_3} = \hat{e}\left(h_3 P, \psi_j\right)^{h^*_3 h_2(\mathsf{t}^1_{\mathsf{rsu}}, \mathsf{r}^j_{\mathsf{rsu}})} \\ \left(\frac{\mathrm{J}^*_i}{\mathbb{A}_i^{\mathsf{r}^j_{\mathsf{rsu}}\partial_i}}\right)^{h_3} = \hat{e}\left(h^*_3 P, \psi_j\right)^{h_3 h_2(\mathsf{t}^1_{\mathsf{rsu}}, \mathsf{r}^j_{\mathsf{rsu}})} \end{cases}. \tag{12}$$

In this case, $\frac{(\mathrm{J}_i)^{h^*_3}}{\mathbb{A}_i^{\mathsf{r}^j_{\mathsf{rsu}}\partial_i h^*_3}} = \frac{(\mathrm{J}^*_i)^{h_3}}{\mathbb{A}_i^{\mathsf{r}^j_{\mathsf{rsu}}\partial_i h_3}}$ holds. Let $H_1 = H_1\left(\sum^n_{\ell=1} \ddagger^i_\ell\right) P$ so that

$$\begin{aligned} \frac{(\mathrm{J}_i)^{h^*_3}}{(\mathrm{J}^*_i)^{h_3}} &= \frac{\hat{e}\left(R^j_{\mathsf{rsu}}P, \Re_i\right)^{\partial_i h^*_3}}{\hat{e}\left(R^j_{\mathsf{rsu}}P, \Re_i\right)^{\partial_i h_3}} \\ &= \hat{e}\left(\partial_i h^*_3 R^j_{\mathsf{rsu}}P - \partial_i h_3 R^j_{\mathsf{rsu}}P, \Re_i\right) \\ &= \hat{e}\left(\left(\partial_i h^*_3 - \partial_i h_3\right) aP, bP\right) \\ &= \hat{e}\left(ab\left(\partial_i h^*_3 - \partial_i h_3\right) P, P\right) \\ &= \frac{\hat{e}\left(h^*_3 U_i - h^*_3 H_1, P\right)}{\hat{e}\left(h_3 U^*_i - h_3 H_1, P\right)} \\ &= \hat{e}\left(h^*_3 U_i - h^*_3 H_1 - h_3 U^*_i + h_3 H_1, P\right) \end{aligned} \tag{13}$$

Thereafter, due to $h_3 \neq h_3^*$, $\mathscr{C}_1$ extracts $ab\left(\partial_i h_3^* - \partial_i h_3\right) P = h_3^* U_i - h_3 U_i^* + (h_3 - h_3^*) H_1$ and calculates $abP = \frac{h_3^* U_i - h_3 U_i^*}{\partial_i (h_3^* - h_3)} - \frac{H_1}{\partial_i}$. $\mathscr{C}_1$ then outputs $\frac{h_3^* U_i - h_3 U_i^*}{\partial_i (h_3^* - h_3)} - \frac{H_1}{\partial_i}$ as the solution to the CDHP instance $\left(R_{\mathsf{rsu}}^j P, \Re_i\right) = (aP, bP)$.

At this point, it's shown that $\mathscr{C}_1$ is able to use $\mathscr{A}_1$ to address the given CDHP instance. However, the ability of addressing the CDHP problem contradicts with its hardness. The advantage for $\mathscr{C}_1$ to win $\mathscr{G}_1$ is negligible. Therefore, under the random oracle model, the proposed design is provably secure against forgery with CMA. □

**Proposition 2** (User Anonymity and Message Unlinkability)**.** *Anonymous identities for all legitimate vehicles and RSUs are adopted upon each communication session. The transmitted messages originated from or destined to the same vehicle can not be associated so that unlinkability for the specific vehicle is guaranteed.*

*Proof.* Initially, the pre-configured $\left\{\mathsf{id}_{\mathsf{rsu}}^j, \mathsf{sk}_{\mathsf{rsu}}^j\right\}$ is independently generated by TA and then issued to each RSU. Thereafter, the dynamic session identity $\mathsf{ID}_{\mathsf{rsu}}^j$ is constructed as $\mathsf{ID}_{\mathsf{rsu}}^j = h_1(\mathsf{id}_{\mathsf{rsu}}^j, \mathsf{t}_{\mathsf{rsu}}^1, \mathsf{r}_{\mathsf{rsu}}^j P)$, where the random value $\mathsf{r}_{\mathsf{rsu}}^j$ and latest timestamp $\mathsf{t}_{\mathsf{rsu}}^1$ are utilized. Notably, the adopted session identity $\mathsf{ID}_{\mathsf{rsu}}^j$ is effective within a single communication session and will expire at a certain timepoint. In this case, the previous session identity $\mathsf{ID}_{\mathsf{rsu}}^j$ will be updated using the newly generated values so that message unlinkability in terms of different communication sessions is achieved. Similarly, the periodically updating over the vehicle $(\mathsf{ID}_{\mathsf{v}}^i)^*$ is conducted as $\mathsf{ID}_{\mathsf{v}}^i = h_2\left[(\mathsf{ID}_{\mathsf{v}}^i)^*, \mathsf{t}_{\mathsf{v}}^1\right]$ whenever the new session starts. Intuitively, the anonymous identities for all the vehicles and RSUs are adopted. In this way, the distinctive user identity patterns are hidden from eavesdroppers such that illegal tracing towards the particular vehicular entity is prevented. The linkage of the vehicular messages that are related to the same vehicle during various communication sessions is not revealed at all. □

**Proposition 3** (Replay Attack Resistance)**.** *The proposed scheme provides replay attack resistance all the time. The reuse on the acquired previous messages, as well as the information extracted, cannot pass the validation process of current session.*

*Proof.* As for the whole authenticated key management scheme including vehicle authentication, group key distribution, and V2V data sharing, the freshness of the vehicular message is guaranteed by the adopted latest timestamp, which is accordingly bound to the certain occurring time point so that all the interactions are time-related. In this case, the valid packets that exceed the assumed period are no longer valid. The fresh timestamps $\left\{\mathsf{t}_{\mathsf{rsu}}^1, \mathsf{t}_{\mathsf{v}}^1, \mathsf{t}_{\mathsf{rsu}}^2, \mathsf{t}_{\Delta}^i\right\}$ are adopted in the generation of temporary session identities and crucial credentials including $\left\langle \mathsf{ID}_{\mathsf{rsu}}^j, R_{\mathsf{rsu}}^j, Q_{\mathsf{rsu}}^j, \mathsf{ID}_{\mathsf{v}}^i, \eth_i, \partial_i, U_i \right\rangle$. Consequently, the signature constructed with the above parameters is mapped to an accurate time interval and will be verified in each validation process. Hence, the previous messages from the past sessions cannot be accepted by the current RSU. Moreover, due to the characteristic of the utilized one-way hash functions, the modification on the acquired historical message will also result in verification failure on the RSU side. □

**Proposition 4** (Conditional Privacy-Preserving)**.** *The conditional privacy preservation is provided for all legitimate vehicles during the whole authenticated key management and data delivery process. Anonymous data exchange is enabled, while the VANET system is able to reveal the true identity of malicious or compromised units if necessary.*

*Proof.* In the proposed scheme, the anonymous session identities are adopted in each session, while the confidential original vehicle identity $\mathsf{id}_i \in \{0,1\}^*$ and RSU identity $\mathsf{id}_{\mathsf{rsu}}^j \in \{0,1\}^*$ are hidden all the time. The certificateless authentication is adopted, where the attribute-based vehicle secret set $\left\{k_1^i, k_2^i, \ldots, k_n^i\right\}$ is determined by the TA. The vehicle itself also generates the random number $\mathsf{r}_{\mathsf{v}}^i$ as the partial key that is valid within the current session. Notably, $\mathsf{r}_{\mathsf{v}}^i$ is involved in vital computation including $\left\{T_i^1, \ldots, T_i^n, U_i, \mathbb{A}_i\right\}$. Impersonation and forgery on the specific vehicle can not pass the final verification in TA such that user privacy is preserved. Moreover, the vehicular communication metadata is aggregated and recorded in a decentralized way. The transmitted packet $\left\langle \mathsf{t}_{\Delta}^{\mathsf{S}}, \mathsf{ID}_{\Delta}^{\mathsf{R}}, \wp_i, \Im_i \right\rangle$ is observed and stored in the auditing chain of the remote server, while the decrypted data is preserved locally. In this case, message retrieval and identity tracing can be achieved for the targeted vehicles such that the malicious user behaviors and patterns can be exposed. Overall, effective authentication and key management design, along with exclusive vehicular communication strategy are adopted for enhancing the privacy-preserving property to the utmost extent. The true identity for each vehicle can also be efficiently revealed by TA whenever necessary. Therefore, conditional privacy-preserving is achieved. □

**Proposition 5** (Session Key Establishment)**.** *Upon authentication, the session key establishment is executed for all the legitimate vehicles. Secure V2R interactions and V2V data sharing can be ensured accordingly.*

*Proof.* The confidential session key $\aleph_j$ is established for V2R data exchange. The efficient attributed-based key distribution method is deployed so that the flexibility access control is guaranteed. For each successful authentication, the vehicle exploits the credential $\{\mathbb{A}_i, \mathbb{C}_i\}$ to update their identities as $\mathsf{ID}_{\Delta}^i = H_4\left(\mathbb{C}_i, \mathbb{A}_i\right)_{i \in [1,\hbar]}$. Meanwhile, the homomorphic encryption infrastructure is adopted for exclusive V2V data exchange. Each validated vehicle outputs its encryption key pair $\langle \mathcal{G}_i, \hbar_i \rangle$, while the corresponding private key pair $\{\varrho_i, \varkappa_i\}$ is determined by the vehicle individually. Moreover, the previously extracted $\aleph_j$ is also adopted in the identity updating process $\mathsf{ID}_{\Delta}^{\mathsf{R}} \leftarrow h_2\left(\mathsf{ID}_{\Delta}^{\mathsf{R}}, \aleph_j\right)$ so that only the legitimate vehicles that have been verified by the RSU could acquire the latest identity of the destined vehicle. The vehicular packet $\left\langle \mathsf{t}_{\Delta}^{\mathsf{S}}, \mathsf{ID}_{\Delta}^{\mathsf{R}}, \wp_i, \Im_i \right\rangle$ could be correctly decrypted by the targeted vehicle, while other VANET entities can not trace the specific identity or the message contents. □

TABLE II: Comparison Result on Security Properties

| Scheme | Kumar *et al.* [3] | Bayat *et al.* [5] | He *et al.* [20] | Tsai *et al.* [34] | Mei *et al.* [35] | Xue *et al.* [36] | The proposed scheme |
|---|---|---|---|---|---|---|---|
| Unforgeability | √ | √ | √ | √ | √ | √ | √ |
| Conditional Privacy | √ | √ | √ | √ | √ | √ | √ |
| Session Key Establishment | √ | √ | √ | √ | √ | √ | √ |
| Scalability | √ | × | √ | × | × | √ | √ |
| Dynamic Identity Updating | × | √ | × | × | √ | × | √ |
| Unlinkability | √ | √ | √ | √ | √ | √ | √ |
| Replay Attack Resilience | √ | √ | √ | √ | √ | √ | √ |
| Message Non-repudiation | × | √ | × | √ | × | √ | √ |

TABLE III: Execution Time of Cryptographic Operations

| Cryptographic Operations | $T_{\mathsf{P}}$ | $T_{\mathsf{SM\cdot P}}$ | $T_{\mathsf{SSM\cdot P}}$ | $T_{\mathsf{PA\cdot P}}$ | $T_{\mathsf{H\cdot MP\cdot P}}$ | $T_{\mathsf{SM\cdot E}}$ | $T_{\mathsf{SSM\cdot E}}$ | $T_{\mathsf{PA\cdot E}}$ | $T_{\mathsf{SH}}$ |
|---|---|---|---|---|---|---|---|---|---|
| Execution Time (ms) | 4.2110 | 1.7090 | 0.0535 | 0.0071 | 4.406 | 0.4420 | 0.0138 | 0.0018 | 0.0001 |

**Proposition 6** (Exclusive V2V Data Sharing Providing Non-repudiation)**.** *The exclusive V2V data exchange is enabled in the proposed scheme. Privacy-preservation, accountability, and non-repudiation can be provided.*

*Proof.* In the proposed accountable vehicular communication strategy, the exclusive chain-based message delivery mechanism is built for each communication session. The encrypted output $\wp_i = Enc^{\mathsf{r}_{\mathsf{v}}^i}_{\langle \mathcal{G}_i, \hbar_i \rangle}(\mathsf{ID}^{\mathsf{S}}_{\Delta} || M)$ on the vehicular data $M$ is sent with the updated receiver identity $\mathsf{ID}^{\mathsf{R}}_{\Delta}$. Notably, both the sender and receiver manage the local chains so that$M$is locally stored. Furthermore, the packet $\left\langle \mathsf{t}^{\mathsf{S}}_{\Delta}, \mathsf{ID}^{\mathsf{R}}_{\Delta}, \wp_i, \Im_i \right\rangle$ is observed and stored in the auditing chain of TA. Non-repudiation on the contents of the vehicular communication is guaranteed. At future moments, the TA is able to audit the V2V data sharing process by checking the recorded chain values of the involved vehicles and cloud servers. In this case, non-repudiation on not only the communication process but also the vehicular contents can be guaranteed. Therefore, accountable V2V data exchange is achieved under the exclusive communication channel. □

### B. Security Comparison

The comparisons between the proposed design and the state-of-the-arts are conducted in terms of the crucial security properties in VANETs. The comparison results are briefly illustrated in Table II, where the schemes [3], [5], [20], [34], [35], [36] are involved. Intuitively, the proposed design is able to meet the desired security requirements.

## VI. Performance Evaluation

In this section, the performance analysis of the proposed scheme is conducted. The evaluation in terms of computational cost and communication overhead for the signing and verification process is presented, respectively. Meanwhile, the performance comparisons between the proposed design and the existing schemes [3], [5], [20], [34], [35] are presented.

For evaluation on the crypto-operations, the adopted bilinear pairing function $\hat{e}$ is constructed in the form of $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ so as to achieve the security level of 80 bits. $\mathbb{G}_1$ is defined as an additive group that is generated by a point $\bar{P}$ with the order $\bar{q}$ over a super singular elliptic curve $\bar{E} : y^2 = x^3 + x \bmod \bar{p}$ with embedding degree 2. Notably, $\bar{q}$ denotes a 160-bit Solinas prime number, while $\bar{p}$ denotes a 512-bit prime number satisfying $\bar{p} + 1 = 12\bar{q}\bar{r}$. As for the construction of the elliptic curve on 80-bits security level, the additive group $\mathbb{G}$ is generated by a point $P$ with the order $q$ on a non-singular elliptic curve $E : y^2 = x^3 + ax + b \bmod p$, where $a, b \in \mathbb{Z}^*_p$ and $q, p$ denotes two 160-bit prime numbers.

### A. Analysis on Computational Cost

The computation cost of the proposed scheme is evaluated in this subsection. The experiment and the evaluation method in [20] are adopted, where the time cost for basic cryptographic functions are evaluated using the MIRACL [37] library. The execution time of relevant cryptographic operations is given in Table III, while the corresponding notations are defined as follows:

- $T_{\mathsf{P}}$*:* The time to conduct the bilinear pairing operation $\hat{e}(M, N)$ with $\bar{M}, \bar{N} \in \mathbb{G}_1$.
- $T_{\mathsf{SM\cdot P}}$*:* The time to conduct the scale multiplication operation $\alpha \cdot \bar{P}$ related to bilinear pairing with $\bar{P} \in \mathbb{G}_1$ and $\alpha \in \mathbb{Z}^*_{\bar{q}}$.
- $T_{\mathsf{SSM\cdot P}}$*:* The time to conduct the small scale multiplication operation $\varsigma_i \cdot \bar{P}$ related to bilinear pairing with $\bar{P} \in \mathbb{G}_1$. Specifically, $\varsigma_i$ is defined as a small random integer satisfying $\varsigma_i \in [1, 2^t]$, where $t$ is a small integer.
- $T_{\mathsf{PA\cdot P}}$*:* The time to conduct the point addition operation $\bar{M} + \bar{N}$ related to bilinear pairing with $\bar{M}, \bar{N} \in \mathbb{G}_1$.
- $T_{\mathsf{H\cdot MP\cdot P}}$*:* The time to conduct a MapToPoint hash function related to bilinear pairing.
- $T_{\mathsf{SM\cdot E}}$*:* The time to conduct the scale multiplication operation $\alpha \cdot P$ related to elliptic curve with $P \in \mathbb{G}$ and $\alpha \in \mathbb{Z}^*_q$.
- $T_{\mathsf{SSM\cdot E}}$*:* The time to conduct the small scale multiplication operation $\varsigma_i \cdot P$ related to elliptic curve with $P \in \mathbb{G}_1$ using the small exponent test technology. Specifically, $\varsigma_i$ is defined as a small random integer satisfying $\varsigma_i \in [1, 2^t]$, where $t$ is a small integer.
- $T_{\mathsf{PA\cdot E}}$*:* The time to conduct the point addition operation $M + N$ related to elliptic curve with $M, N \in \mathbb{G}$.
- $T_{\mathsf{SH}}$: The time to conduct a secure hash function.

For a better description, let AIGVS denote the process of anonymous vehicle identity generation and vehicle signing, SAIV denote the process of single authentication verification

TABLE IV: Comparison Results of Computational Cost

| Scheme | AIGVS | SAIV | BAMV |
|---|---|---|---|
| Kumar *et al.* [3] | $4T_{\mathsf{SM\cdot P}} + 2T_{\mathsf{PA\cdot P}} + 1T_{\mathsf{H\cdot MP\cdot P}}$ $\approx 11.2562$ ms | $4T_{\mathsf{P}} + 3T_{\mathsf{SM\cdot P}} + 1T_{\mathsf{H\cdot MP\cdot P}}$ $\approx 26.377$ ms | $4T_{\mathsf{P}} + 3nT_{\mathsf{SM\cdot P}} + (n+1)T_{\mathsf{H\cdot MP\cdot P}}$ $\approx 9.533n + 21.25$ ms |
| Bayat *et al.* [5] | $5T_{\mathsf{SM\cdot P}} + 1T_{\mathsf{PA\cdot P}} + 1T_{\mathsf{H\cdot MP\cdot P}} + 2T_{\mathsf{SH}}$ $\approx 12.9583$ ms | $3T_{\mathsf{P}} + 1T_{\mathsf{SM\cdot P}} + 1T_{\mathsf{H\cdot MP\cdot P}} + T_{\mathsf{SH}}$ $\approx 18.7481$ ms | $3T_{\mathsf{P}} + nT_{\mathsf{SSM\cdot P}} + (3n-3)T_{\mathsf{PA\cdot P}} + nT_{\mathsf{H\cdot MP\cdot P}} + nT_{\mathsf{SH}}$ $\approx 6.1364n + 12.6117$ ms |
| He *et al.* [20] | $3T_{\mathsf{SM\cdot E}} + 3T_{\mathsf{SH}}$ $\approx 1.3263$ ms | $3T_{\mathsf{SM\cdot E}} + 2T_{\mathsf{PA\cdot E}} + 2T_{\mathsf{SH}}$ $\approx 1.3298$ ms | $(n+2)T_{\mathsf{SM\cdot E}} + 2nT_{\mathsf{SSM\cdot E}} + (3n-1)T_{\mathsf{PA\cdot E}} + 2nT_{\mathsf{SH}}$ $\approx 0.4752n + 0.8822$ ms |
| Tsai *et al.* [34] | $1T_{\mathsf{SM\cdot P}}$ $\approx 1.709$ ms | $1T_{\mathsf{P}} + 2T_{\mathsf{SM\cdot P}} + 2T_{\mathsf{PA\cdot P}}$ $\approx 7.6432$ ms | $1T_{\mathsf{P}} + 2nT_{\mathsf{SM\cdot P}} + 2nT_{\mathsf{PA\cdot P}}$ $\approx 3.4322n + 4.211$ ms |
| Mei *et al.* [35] | $4T_{\mathsf{SM\cdot P}} + 2T_{\mathsf{PA\cdot P}} + 2T_{\mathsf{H\cdot MP\cdot P}}$ $\approx 15.6622$ ms | $4T_{\mathsf{P}} + 2T_{\mathsf{SM\cdot P}} + 2T_{\mathsf{H\cdot MP\cdot P}}$ $\approx 29.074$ ms | $4T_{\mathsf{P}} + 2nT_{\mathsf{SM\cdot P}} + (2n-2)T_{\mathsf{PA\cdot P}} + 2T_{\mathsf{H\cdot MP\cdot P}}$ $\approx 3.4322n + 25.6418$ ms |
| The proposed scheme | $2T_{\mathsf{SM\cdot E}} + 1T_{\mathsf{PA\cdot E}} + 11T_{\mathsf{SH}}$ $\approx 0.8869$ ms | $1T_{\mathsf{SM\cdot E}} + 4T_{\mathsf{SH}}$ $\approx 0.4424$ ms | $nT_{\mathsf{SM\cdot E}} + (2n+2)T_{\mathsf{SH}}$ $\approx 0.4422n + 0.0002$ ms |

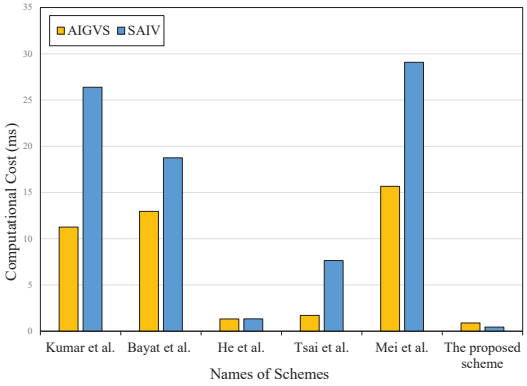


Fig. 4: Computational Cost on AIGVS and SAIV

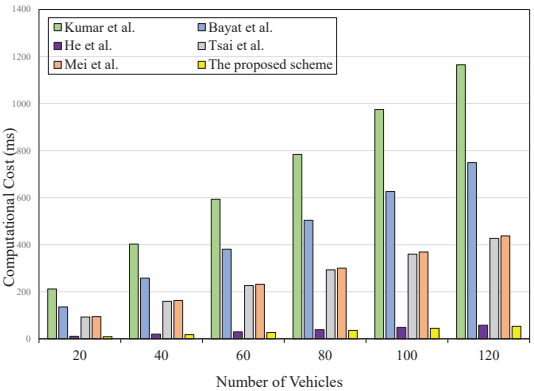


Fig. 5: Computational Cost on BAMV

of individual vehicle, BAMV denote the batch authentication process involving multiple vehicles. The detailed analysis of the proposed scheme, along with other related schemes including [3], [5], [20], [34], [35] are presented. The comparison results on computational cost for each step are shown in Table IV. In the analysis on the proposed scheme, the number of attributes for each vehicle is set to five such that the original secret set is $\left\{k_1^i, k_2^i, k_3^i, k_4^i, k_5^i\right\}$. In this case, the AIGVS phase requires one point addition operation related to elliptic curve, two scale multiplication operations related to elliptic curve, and eleven general secure hash operations. The time consumption of AIGVS is $2T_{\mathsf{SM\cdot E}} + 1T_{\mathsf{PA\cdot E}} + 11T_{\mathsf{SH}} \approx 0.8869$ ms. In the successive SAIV phase, four general secure hash

TABLE V: Percentage Improvement on Computational Cost

| Scheme | AIGVS | SAIV | BAMV |
|---|---|---|---|
| Kumar *et al.* [3] | 92.12% | 98.32% | 95.45% |
| Bayat *et al.* [5] | 93.16% | 97.64% | 92.92% |
| He *et al.* [20] | 33.13% | 66.73% | 8.36% |
| Tsai *et al.* [34] | 48.10% | 94.21% | 87.25% |
| Mei *et al.* [35] | 94.34% | 98.48% | 87.87% |

operations and one scale multiplication operation related to elliptic curve are conducted. The time consumption for SAIV is $1T_{\mathsf{SM\cdot E}} + 4T_{\mathsf{SH}} \approx 0.4424$ ms. As for the BAMV phase, $n$ scale multiplication operations related to elliptic curve, and $(2n+2)$ general secure hash operations are executed by RSU. Notably, since the complicated pairing calculation tasks are conducted by TA prior to the verification, the computation overhead on the RSU side is taken into account. Therefore, the execution time for BAMV is $nT_{\mathsf{SM\cdot E}} + (2n+2)T_{\mathsf{SH}} \approx 0.4422n + 0.0002$ ms.

The proposed design is compared with the relevant schemes including [3], [5], [20], [34], [35] graphically. The comparison results with respect to AIGVS and SAIV phase are given in Fig. 4. Moreover, the comparison results on the execution time of BAMV are illustrated in Fig. 5. The proposed design is more efficient in computational cost than the other schemes with regard to AIGVS, SAIV, and BAMV. In addition, the improvement of the proposed scheme in execution time can be demonstrated in Table V. Accordingly, the percentage improvements of the proposed scheme for AIGVS can be calculated as $\frac{11.2562-0.8869}{11.2562} \approx 92.12\%$, $\frac{12.9583-0.8869}{12.9583} \approx 93.16\%$, $\frac{1.3263-0.8869}{1.3263} \approx 33.13\%$, $\frac{1.709-0.8869}{1.709} \approx 48.10\%$, $\frac{15.6622-0.8869}{15.6622} \approx 94.34\%$, respectively. Similarly, the percentage improvements for SAIV are $98.32\%$, $97.64\%$, $66.73\%$, $94.21\%$, $98.48\%$, respectively. Moreover, the execution time for BAMV phase is $53.0642$ ms, where the total number of vehicles is set as $n = 120$. In this case, the percentage improvements are $95.45\%$, $92.92\%$, $8.36\%$, $87.25\%$, $87.87\%$, respectively.

### *B. Analysis on Communication Overhead*

The communication cost of the proposed scheme is analyzed and compared with the related schemes [3], [5], [20], [34], [35]. As mentioned above, the size of $\bar{p}$ is set as $64$ bytes ($512$ bits), and the size of $p$ is set as $20$ bytes ($160$ bits). Therefore, the elements size in the additive group $\mathbb{G}_1$ is set to be $64 \times 2 = 128$ bytes, and the size of the elements in the additive group

TABLE VI: Comparison Results of Communication Overhead

| Scheme | Single Verification | Multiple Verification |
|---|---|---|
| Kumar *et al.* [3] | 536 | $536n$ |
| Bayat *et al.* [5] | 388 | $388n$ |
| He *et al.* [20] | 144 | $144n$ |
| Tsai *et al.* [34] | 680 | $680n$ |
| Mei *et al.* [35] | 680 | $680n$ |
| The proposed scheme | 124 | $124n$ |

$\mathbb{G}$ is $20 \times 2 = 40$ bytes. Meanwhile, the size of the timestamp, and the general secure hash function are $4$ bytes and $20$ byte, respectively. In [5], the signature $\langle AID_i^1, AID_i^2, T_i, U_i \rangle$ is delivered. With $U_i \in \mathbb{G}_1$ and $AID_i^1, AID_i^2 \in \mathbb{G}_1$, the communication cost for single verification process is $128 \times 3 + 4 = 388$ bytes. Notably, $T_i$ denotes the timestamp. In [20], the packet $\langle m_i, T_i, \sigma_i, R_i, PID_i^1, PID_i^2 \rangle$ is involved. With $R_i \in \mathbb{G}$ and $PID_i^1 \in \mathbb{G}$, the communication cost for single verification process is $40 \times 2 + 20 \times 3 + 4 = 144$ bytes. As for the proposed scheme, with $\{\mathsf{ID}_{\mathsf{v}}^i, \eth_i, \partial_i\} \in \mathbb{Z}_q^*$, $U_i \in \mathbb{G}_1$, the communication cost for single verification process is $40 + 20 \times 3 + 20 + 4 = 124$ bytes, Notably, $\mathsf{t}_{\mathsf{v}}^1$ denotes the timestamp. Similarly, the communication cost discussions of [3], [34], [35] are also shown in Table VI. Intuitively, the proposed scheme provides lower communication cost compared with other related schemes.

## VII. Conclusion

Emphasizing on achieving mutual authentication and privacy preservation in practical vehicular wireless networks, an attribute-based authenticated key management is proposed such that a flexible access control mechanism is enabled for the participating vehicles. Independent and exclusive V2V communication is established for spontaneous vehicular data exchange beyond third-party surveillance. Furthermore, accountable vehicular communication is enabled with the utilized chain-based data preservation infrastructure, where the transmitted packets are simultaneously recorded by TA and related vehicles. Therefore, crucial security requirements including non-repudiation can be satisfied. Conditional privacy preservation in terms of the entire authentication and transmission is guaranteed, while the true identities of the malicious or compromised entities could be revealed whenever a dispute occurs. The proposed scheme can provide vital security properties and resist various attacks. Significant improvements compared to other related schemes can be demonstrated regarding computational cost and communication overhead.

## Acknowledgment

This work is supported by the National Natural Science Foundation of China under Grants No. 61922045, No. U21A20465, No. 62172292, and Science Foundation of Zhejiang Sci-Tech University (ZSTU) under Grants No. 22222266-Y.

## References

[1] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in vanets," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 616–629, 2011.

[2] D. Huang, S. Misra, M. Verma, and G. Xue, "PACP: an efficient pseudonymous authentication-based conditional privacy protocol for vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 3, pp. 736–746, 2011.

[3] P. Kumar, S. Kumari, V. Sharma, X. Li, A. K. Sangaiah, and S. H. Islam, "Secure cls and cl-as schemes designed for vanets," *The Journal of Supercomputing*, vol. 75, pp. 3076–3098, 2019.

[4] C. Wang, R. Huang, J. Shen, J. Liu, P. Vijayakumar, and N. Kumar, "A novel lightweight authentication protocol for emergency vehicle avoidance in vanets," *IEEE Internet of Things Journal*, vol. 8, no. 18, pp. 14 248–14 257, 2021.

[5] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for vanets with batch verification," *Wireless Networks*, vol. 21, pp. 1733–1743, 2015.

[6] J. Shen, H. Yang, P. Vijayakumar, and N. Kumar, "A privacy-preserving and untraceable group data sharing scheme in cloud computing," *IEEE Transactions on Dependable and Secure Computing*, 2021, DOI: 10.1109/TDSC.2021.3050517.

[7] H. Tan, "An efficient iot group association and data sharing mechanism in edge computing paradigm," *Cyber Security and Applications*, vol. 1, 2023, DOI: 10.1016/j.csa.2022.100003.

[8] Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure v2v communications in an iov paradigm," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2740–2749, 2017.

[9] J. Shen, Z. Gui, X. Chen, J. Zhang, and Y. Xiang, "Lightweight and certificateless multi-receiver secure data transmission protocol for wireless body area networks," *IEEE Transactions on Dependable and Secure Computing*, 2020, DOI: 10.1109/TDSC.2020.3025288.

[10] D. He, S. Chan, and M. Guizani, "An accountable, privacy-preserving, and efficient authentication framework for wireless access networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1605–1614, 2016.

[11] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, no. 1, pp. 127–139, 2012.

[12] A. Wasef and X. Shen, "EMAP: expedite message authentication protocol for vehicular ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 1, pp. 78–89, 2013.

[13] H. Aliev, H. Kim, and S. Choi, "A scalable and secure group key management method for secure v2v communication," *Sensors*, vol. 20, no. 21, p. 6137, 2020.

[14] M. N. Aman, U. Javaid, and B. Sikdar, "A privacy-preserving and scalable authentication protocol for the internet of vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 1123–1139, 2021.

[15] Y. Cai, H. Zhang, and Y. Fang, "A conditional privacy protection scheme based on ring signcryption for vehicular ad hoc networks," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 647–656, 2021.

[16] T. Miao, J. Shen, C.-F. Lai, S. Ji, and H. Wang, "Fuzzy-based trustworthiness evaluation scheme for privilege management in vehicular ad hoc networks," *IEEE Transactions on Fuzzy Systems*, vol. 29, no. 1, pp. 137–147, 2021.

[17] H. Yang, J. Shen, T. Zhou, S. Ji, and P. Vijayakumar, "A flexible and privacy-preserving collaborative filtering scheme in cloud computing for vanets," *ACM Transactions on Internet Technology (TOIT)*, vol. 22, no. 2, pp. 1–19, 2021.

[18] H. Tan, W. Zheng, P. Vijayakumar, K. Sakurai, and N. Kumar, "An efficient vehicle-assisted aggregate authentication scheme for infrastructureless vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, 2022, DOI: 10.1109/TITS.2022.3176406.

[19] L.-Y. Yeh, Y.-C. Chen, and J.-L. Huang, "ABACS: an attribute-based access control system for emergency services over vehicular ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 630–643, 2011.

[20] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[21] Q. Feng, D. He, S. Zeadally, and K. Liang, "BPAS: blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4146–4155, 2020.

[22] C. Feng, K. Yu, M. Aloqaily, M. Alazab, Z. Lv, and S. Mumtaz, "Attribute-based encryption with parallel outsourced decryption for edge intelligent iov," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13 784–13 795, 2020.

[23] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 4, pp. 1606–1617, 2010.
[24] L. Wu, Q. Sun, X. Wang, J. Wang, S. Yu, Y. Zou, B. Liu, and Z. Zhu, "An efficient privacy-preserving mutual authentication scheme for secure v2v communication in vehicular ad hoc network," *IEEE Access*, vol. 7, pp. 55 050–55 063, 2019.
[25] W. Hathal, H. Cruickshank, Z. Sun, and C. Maple, "Certificateless and lightweight authentication scheme for vehicular communication networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 16 110–16 125, 2020.
[26] I. Ali, Y. Chen, N. Ullah, R. Kumar, and W. He, "An efficient and provably secure ecc-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in vanets," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1278–1291, 2021.
[27] T. Zhou, H. Yang, and J. Shen, "Key agreement protocol with dynamic property for vanets," *Journal of Cryptologic Research*, vol. 7, pp. 375–388, 2020.
[28] N. Koblitz and A. Menezes, "Pairing-based cryptography at high security levels," in *Proceedings of the 10th International Conference on Cryptography and Coding*, ser. IMA'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 13–36.
[29] J. H. Silverman and J. Suzuki, "Elliptic curve discrete logarithms and the index calculus," in *Advances in Cryptology — ASIACRYPT'98*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 110–125.
[30] D. Boneh, "The decision diffie-hellman problem," in *Algorithmic Number Theory*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 48–63.
[31] F. Pignol, F. Colone, and T. Martelli, "Lagrange-polynomial-interpolation-based keystone transform for a passive radar," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, no. 3, pp. 1151–1167, 2018.
[32] A. Balu and K. Kuppusamy, "An expressive and provably secure ciphertext-policy attribute-based encryption," *Information Sciences*, vol. 276, pp. 354–362, 2014.
[33] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13, no. 3, pp. 361–396, 2000.
[34] J.-L. Tsai, "A new efficient certificateless short signature scheme using bilinear pairings," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2395–2402, 2017.
[35] Q. Mei, H. Xiong, J. Chen, M. Yang, S. Kumari, and M. K. Khan, "Efficient certificateless aggregate signature with conditional privacy preservation in iov," *IEEE Systems Journal*, vol. 15, no. 1, pp. 245–256, 2021.
[36] K. Xue, X. Luo, Y. Ma, J. Li, J. Liu, and D. S. L. Wei, "A distributed authentication scheme based on smart contract for roaming service in mobile vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 5, pp. 5284–5297, 2022.
[37] E. Wenger and M. Werner, "Evaluating 16-bit processors for elliptic curve cryptography," in *Smart Card Research and Advanced Applications*, E. Prouff, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 166–181.

**Haowen Tan** received the the B.S. and M.S. degrees from Nanjing University of Information Science and Technology, Nanjing, China, in 2013 and 2016, respectively, and the Ph.D. degree from the Department of Computer Engineering, Chosun University, Gwangju, Korea, in 2020. From 2021 to 2022, he was a Post-doctoral Fellow with the Cyber Security Center, Kyushu University, Fukuoka, Japan. He is currently working with the School of Information Science and Technology, Zhejiang Sci-Tech University, Hangzhou, China. His research interests include network security, ubiquitous sensor networks, blockchain, and vehicular ad-hoc networks.

**Wenying Zheng** received the M.E. degree in Electronic Engineering from Chosun University, Gwangju, Korea, in 2009, and the Ph.D. degree in Computer Science from Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2022, respectively. She is currently working with the School of Computer Science and Technology, Zhejiang Sci-Tech University, Hangzhou, China. Her research interests include cloud storage security, security systems and network security.

**Yunguo Guan** is a PhD student of the Faculty of Computer Science, University of New Brunswick, Canada. His research interests include applied cryptography and game theory.

**Rongxing Lu** (S'09-M'11-SM'15-F'21) is an associate professor at the Faculty of Computer Science (FCS), University of New Brunswick (UNB), Canada. Before that, he worked as an assistant professor at the School of Electrical and Electronic Engineering, Nanyang Technological University (NTU), Singapore from April 2013 to August 2016. Rongxing Lu worked as a Postdoctoral Fellow at the University of Waterloo from May 2012 to April 2013. He was awarded the most prestigious "Governor General's Gold Medal", when he received his PhD degree from the Department of Electrical & Computer Engineering, University of Waterloo, Canada, in 2012; and won the 8th IEEE Communications Society (ComSoc) Asia Pacific (AP) Outstanding Young Researcher Award, in 2013. Also, Dr. Lu received his first PhD degree at Shanghai Jiao Tong University, China, in 2006. Dr. Lu is an IEEE Fellow. His research interests include applied cryptography, privacy enhancing technologies, and IoT-Big Data security and privacy. He has published extensively in his areas of expertise (with H-index 72 from Google Scholar as of November 2020), and was the recipient of 9 best (student) paper awards from some reputable journals and conferences. Currently, Dr. Lu serves as the Vice-Chair (Conferences) of IEEE ComSoc CIS-TC (Communications and Information Security Technical Committee). Dr. Lu is the Winner of 2016-17 Excellence in Teaching Award, FCS, UNB.