IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 11, 2019, accepted December 21, 2019, date of publication December 27, 2019,
date of current version January 6, 2020.

Digital Object Identifier 10.1109/ACCESS.2019.2962387

Secure Authentication and Key Management With Blockchain in VANETs

HAOWEN TAN AND ILYONG CHUNG
Department of Computer Engineering, Chosun University, Gwangju 61452, South Korea
Corresponding author: Ilyong Chung (iyc@chosun.ac.kr)

This work was supported by Chosun University (2019).

ABSTRACT Nowadays, with rapid advancements of vehicular telematics and communication techniques, proliferation of vehicular ad hoc networks (VANETs) have been witnessed, which facilitates the construction of promising intelligent transportation system (ITS). Due to inherent wireless communicating features in open environment, secure transmission among numerous VANET entities remains crucial issues. Currently, lots of research efforts have been made, while most of which tend to allocate the universal group key to the verified devices for both vehicle-to-vehicle (V2V) and vehicle-to-RSU (V2R) communications. However, in heterogeneous VANET environment with large numbers of devices in same vehicular group, complicated and variable topologies lead to continuous key updating in every moment, causing interference to regular V2R data exchange, which is not reliable and efficient for resource-constrained VANET environment. Moreover, group membership recording and detecting mechanisms are necessary for real time vehicle revocation and participation, which has not been further studied so far. In this paper, we address the above issues by proposing a secure authentication and key management scheme. In our design, novel VANET system model with edge computing infrastructure is adopted so as to offer adequate computing and storing capacity compared to traditional VANET structure. Note that our certificateless authentication scheme applies the independent session key for each vehicle for interference avoidance. Furthermore, consortium blockchain is employed for V2V group key construction. Real time group membership arrangement with efficient group key updating is accordingly provided. Formal security proofs are presented, demonstrating that the proposed scheme can achieve desired security properties. Performance analysis is conducted as well, proving that the proposed scheme is efficient compared with the state-of-the-arts.

INDEX TERMS Vehicular ad hoc networks (VANETs), certificateless authentication, dynamic group key management, consortium blockchain.

I. INTRODUCTION

In recent years, the significant developments on information and communication technologies have triggered the explosive popularization of advanced intelligent transportation system (ITS), which is regarded as the crucial strategies for improving transportation efficiency [1]. Accordingly, emerging as the fundamental infrastructure of ITS, the vehicular ad hoc networks (VANETs) is defined as the distributed, self-organized wireless networks built by heterogeneous vehicular entities such as vehicles and rode side units (RSUs) [2]. Generally, VANET enables real-time dynamic communication with durative data exchange among participating devices, which could drastically facilitate traffic safety enhancement and driving experience [3].

Typically, a basic VANET architecture is composed of three essential components: *trusted authority (TA)*, *road-side units (RSUs)* and *vehicles*. TA performs as the top-most services provider and central trustworthy key server in charge of the whole VANET system. Therefore, pivotal system operations such as system parameters assignment, user registration, vehicular group arrangement, along with the user management and necessary verification for correlated vehicles, are performed by TA accordingly [4]. It is worth noting that massive vehicular data from all the legitimate VANET entities are aggregated and analyzed in TA side. Obviously, tremendous computation ability and storage are required [5], [6]. Nowadays, sophisticated communicating and processing techniques, including the promising

The associate editor coordinating the review of this manuscript and approving it for publication was Longxiang Gao.

5G networks and cloud computing, have been dedicated to heterogeneous IoT environment including VANETs, where sufficient computing and storing resources can be guaranteed [7], [8]. Moreover, the distributed cloud servers could manage interaction between multiple VANETs simultaneously, which accelerates the initiative formation of the worldwide Internet of vehicle (IoV).

The *RSUs* are defined as the distributed facilities established along the road sides at fixed intervals [9]. In order to deliver services to targeted vehicles, the effective ranges of the fix RSUs are supposed to cover the whole road sections. Each RSU is responsible for direct communication with vehicles within its vicinity. Note that the vehicles can only access the VANETs through seamless interactions with the nearby RSU [10]. As the fundamental entities of VANETs, *vehicles* perform as both the terminal users and major vehicular information source. Massive heterogenous vehicular data and real time road characteristics such as traffic congestion and accident reports, are collaboratively acquired by vehicles [11], [12]. The aggregated data are subsequently uploaded to VANET central server for further analysis and managements. Technically, each vehicle is equipped with onboard unit (OBU) [13], in which the wireless communicating modules including transceiver and transponder are implemented. The OBU of each vehicle is supposed to handle all the message transmission and reception in high-mobility environment.

In VANETs, interactions between vehicles can be guaranteed through vehicle-to-vehicle (V2V) communications [14], [15]. Therefore, self-organized wireless vehicular networks involving multiple vehicles of certain vicinity can be constructed in this way, offering opportunities for real time data exchange and aggregation. Meanwhile, the communication between vehicle and the surrounding RSU can be achieved by means of vehicle to RSU (V2R) communications [16]. Note that both the V2V and V2R communications employ dedicated short-range communications (DSRC) technique designed for reliable automotive use in ITS. Accordingly, the integrated VANET framework with high connectivity and dynamic topology is built [17].

In practical VANET scenarios, the vital data exchange of V2V and V2R connections are conducted in open wireless environment. The transmitted vehicular information may be eavesdropped or forged by malicious entities, resulting in severe vulnerabilities to various security threats and privacy risks [18], [19]. The significant keying information and user secrets may be illegally revealed to adversaries. The whole VANET system may be compromised in this way. Under this circumstance, it is necessary to deploy effective mechanisms for security preservation and privacy protection in VANETs.

Nowadays, relevant studies on secure VANET transmission have attracted lots of attention from both academia and industry [20]–[22]. Many schemes with different safe strategies and cryptographic techniques have been adopted, where mutual authentication between vehicles and RSUs are conducted, followed by the session key distribution process for verified vehicles. In this case, the individual RSU is designed to issue the shared group key to vehicles of its vicinity. Hence, the universal group communication channel is built for both V2V and V2R communications. That is, the data sharing between neighboring vehicles, and the sensitive vehicular data transmission from vehicles to central server, are all conducted within the group channel. However, due to intrinsic high mobility characteristics, the allocated group key may be updated in every moment, resulting in severe inference to regular V2R data exchange [23], [24].

As for data sharing for V2V group communications, due to the dynamic topologies of vehicular groups, timely and efficient key updating method should be provided for secure transmission [25], [26]. To be concrete, in occasions when some vehicles are revoked or disabled, the current group key should be immediately changed [27], [28]. Meanwhile, the group key should be delivered to the newly joined vehicles as well. To achieve this, VANET should be aware of the accurate group information of every moment. The existing VANET security mechanisms mainly focus on authentication and efficient key management, while the corresponding group membership monitoring methods have not been further studied. Furthermore, in V2V group communications, valid and consistent vehicle records in vehicle side are of great significance for targeted transmission with particular entities [29], [30].

Nowadays, the remarkable progress in cloud computing techniques bring new paradigms for massive data processing and storing in VANETs [31]. The uploaded heterogeneous vehicular data can be analyzed and stored in cloud server, which provides adequate computation ability and storage. On the other hand, considering the low latency and high reliability requirements in V2R communications, the edge computing architecture can be deployed [32]. In this case, the nearby RSUs are combined as the local vehicular edge cluster, where the frequently used data can be cached in edge layer instead of requesting from data center every time. Similarly, the RSU clusters are able to assist the central server with certain computation, which alleviates the bandwidth burden for data center.

The studies on blockchain technology have attracted extensively attention so far [33], [34]. With its prominent advantages in decentralized data sharing, blockchain can be exploited in various Internet of thing (IoT) scenarios. Currently, the blockchain networks can be elaborated into four types, including the public blockchains, private blockchains, hybrid blockchains, and consortium blockchains, all of which have been applied to diverse communication circumstances [35]. Specially, the consortium blockchains allocate the preselected user group to establish decentralized paradigms for collaborative data sharing, thus have high potential for deployment in V2V group communications. The commonly shared group membership records can be dynamically managed and stored by all the legitimate vehicles. Note that the historical group communicating records can be validated and traced, which is helpful for conditional

privacy preserving [13], [36]. Moreover, effective key updating mechanism involving the currently legitimate vehicles is achievable [37], [38].

In this paper, with the purpose of offering advanced security properties for VANETs transmission, V2R mutual authentication design is developed. Specifically, the cloud-assisted VANETs infrastructure with edge computing layer for RSU clusters is deployed, which facilitates sufficient computing and storing ability compared to traditional VANETs structure. Subsequently, the group communication channel for V2V data sharing among neighboring vehicles is allocated, where consortium blockchain technique is implemented for real time group membership recording. Moreover, efficient group key updating mechanism is designed, which satisfies practical requirements for resource-limited VANETs occasions.

A. OUR RESEARCH CONTRIBUTIONS

In this paper, we develop a secure authentication and group key establishment scheme with consortium blockchain for dynamic key updating in VANETs. Our nontrivial efforts can be briefly summarized as follows: (1)

(1) **Certificateless authentication scheme for cloud-assisted VANETs with edge computing infrastructure:** Our design adopts novel VANETs infrastructure with edge computing for efficient V2R transmission. The heterogenous vehicular data are to be processed and stored in distributed cloud server. The nearby RSUs perform as the edge cluster for data caching and necessary local data processing. Consequently, certificateless cryptography is exploited so as to address the key escrow problem in identity-based encryption.
(2) **Efficient Group key distribution mechanism deploying consortium blockchain:** In the proposed scheme, vehicular group channels involving RSU and the neighboring vehicles are built for V2V data interactions. Consortium blockchain technique is employed for establishing decentralized V2V networks. Hence, the real time membership records can be shared and managed by all the existing vehicles of the same group, which facilitates accurate group management in distributed way.
(3) **Dynamic group key updating strategies for V2V vehicular group:** Reliable group key updating mechanism is designed for dynamic updating, where the Chinese remainder theorem is applied. The updating process requires comparatively small computation overhead in vehicle side, which could satisfy practical requirements for resource-limited VANETs occasions. Additionally, considering the resource limitation, complex pairing calculations are conducted in RSU and TA side, while relatively lightweight tasks for authentication and key management are conducted in vehicle side.

The remainder of this paper is organized as follows. Section II briefly introduced the related research progresses. Section III illustrated the necessary preliminary works and the designed system model for the reader to obtain a better understanding of the topic. Section IV presents the proposed V2R certificateless authentication and key management scheme in detail. Section V describes V2V group key management scheme. Section VI demonstrates the security analysis. Section VII displays the performance analysis. The conclusion is drawn in Section VIII.

II. RELATED WORKS

In recent years, the secure authentication and key management for VANETs have been widely investigated. In 2012, emphasizing on user privacy preservation and key updating efficiency, Lu *et al.* [39] proposed a dynamic key management scheme for location-based services (LBSs). The LBS session is divided into various time slots with different session keys. Subsequently, a vehicular data authenticating mechanism is described [20], where the probabilistic verification technique is deployed for malicious behavior detection. Furthermore, with the purpose of avoiding the computation delay for certificate revocation list (CRL) checking, group signature with hash message authentication code (HMAC) is utilized in [25]. Similarly, Chuang and Lee [26] developed a decentralized trust-extended authentication mechanism (TEAM) for decentralized V2V communication. Note that the transitive trust relationships frame is applied in order to improve the authenticating efficiency. Recently, multiple authentication schemes have been developed [38], [40], which emphasizes on lightweight VANET verification and privacy preserving.

Particularly, identity-based public key cryptography (ID-PKC) [41] has been widely applied for secure certificate management in VANETs. Initially, Zhang *et al.* [11] proposed the batch signature verification scheme for V2R communications. Nevertheless, this scheme is vulnerable to replay attack [30]. Meanwhile, Jung *et al.* [5] developed the universal re-encryption scheme with identity-based key establishment. Subsequently, the VANETs authentication framework with preservation and repudiation (ACPN) is presented [23]. In their design, self-generated PKC-based pseudo identities are applied. Thereafter, He *et al.* [18] developed an efficient identity-based CPPA scheme for VANETs. Note that bilinear pairing operations are not used, resulting in comparatively low computation cost. Similarly, another two CPPA schemes for VANETs are respectively developed [1], [17]. Furthermore, Gao *et al.* [16] developed a message authentication scheme for PMIPv6 in VANETs (PAAS), where mutual authentication is achieved with hierarchical identity-based signatures.

With the purposed of addressing the key escrow problem of ID-PKC, certificateless public key cryptography (CL-PKC) was introduced [42]. In CL-PKC, the private partial keys are respectively generated by the semi-trusted key generation center (KGC) and the user itself. Multiple certificateless authentication schemes for VANETs have been proposed so far. In 2014, Malip *et al.* [21] developed a privacy preserving authentication protocol based on certificateless signature

and reputation system. Thereafter, Song *et al.* [10] proposed a lightweight VANET certificateless key agreement scheme without pairing. Note that the proposed scheme can be conducted for secure V2V communications without available RSU. Afterwards, emphasizing on secure V2R communication, Horng *et al.* [2] developed a certificateless aggregate signature (CLAS) scheme in VANETs, where both CL-PKC and aggregate signature are used. After that, several VANETs authentication schemes with CL-PKC are developed recently [13], [27], [43].

As mentioned above, with conspicuous advantages in massive data processing and storing, emerging cloud computing techniques have been extensively exploited in various VANET applications. The integrated fog computing infrastructure with VANETs is clarified by Khattak *et al.* [31], which facilitates heterogeneous data interaction, lower latency, and location-aware service provision. In 2017, Soleymani *et al.* [44] constructed a fuzzy VANET trust model based on experience and plausibility. Meanwhile, the safety message dissemination in VANETs has been investigated in [4], where the particular gateways combing both cellular networks and VANETs deliver safety messages from cloud server to neighboring vehicles through V2V communications. Subsequently, Khan *et al.* [7] proposed a hierarchical 5G-based VANETs framework, which integrates centralized software defined networks (SDN) and cloud radio access network (C-RAN). Similarly, another vehicular content distribution scheme with edge computing for 5G-VANETs is presented [32]. The legitimate vehicles are responsible for handling content requests from neighboring devices, resuling in less communication burden for the vehicular networks. Thereafter, another vehicular message dissemination scheme is proposed by Ullah *et al.* [8], where message congestion avoidance is provided.

The development of blockchain techniques facilitate decentralized trust management in VANETs. The relevant privacy-preserving VANETs trust model is proposed in [37]. Note that the extended blockchain-based anonymous reputation system (BARS) is developed, which simultaneously adopts direct historical interactions and indirect opinions about vehicles. Thereafter, Butt *et al.* discussed the challenges and issues on blockchain-based privacy management in social internet of vehicle (SIoV) [35]. As for SDN-enabled 5G-VANETs in promising ITS environment, decentralized blockchain framework [33] is exploited for real time cloud-based trust management. Hence, the malicious entities and messages can be well detected with acceptable overhead, which is crucial for large-scale VANET scenarios. Subsequently, a traceable Internet of vehicle (IoV) system model is constructed [14]. The vehicle transparency and announcement are conducted by the adopted blockchain design. As one of the important paradigms of blockchain, employing consortium blockchain into cloud-assisted VANETs is able to provide secure data sharing among validated entities. Accordingly, an effective traffic signal verification mechanism is proposed [34]. Note that smart contract is employed so as to coordinately optimize the signal management and decision-making process. Hence, synergistic optimization can be provided.

III. MODEL DEFINITION AND PRELIMINARIES

In order to facilitate the reader's understanding of our design, some necessary preliminaries are described in this section, which includes the definitions of elliptic curve cryptosystem (ECC), bilinear pairing, hash function, and Chinese remainder theorem. Thereafter, the corresponding notations, system model, and network assumptions are respectively illustrated.

A. ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

Let $p > 3$ be a large prime, and $\mathbb{F}_p$ be the finite field of order p, where $a, b \in \mathbb{F}_p$ satisfy $4a^3 + 27b^2 \pmod p \neq 0$. An elliptic curve $E_p(a, b)$ over the finite field $\mathbb{F}_p$ is defined with the following equation:

$$y^2 = x^3 + ax + b \bmod p,$$

where $(x, y) \in \mathbb{F}_p$. The addition operation on the curve is called point doubling when the two points are identical. Otherwise, it is called point addition. All the points on the curve, as well as the point at infinity ∞ form an additive Abelian group $E(\mathbb{F}_p)$. Note that $\infty = (-\infty)$ serves as the identity element.

B. BILINEAR PAIRING

Let $\mathbb{G}_1$ be a cyclic additive group generated by a large prime order q and $\mathbb{G}_2$ be a cyclic multiplicative group with the same prime order. A map function $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ is defined as a bilinear pairing if all of the following three properties are satisfied:

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 compute $\hat{e}(P, Q)$.

Such a bilinear map $\hat{e}$ satisfying the above properties can be constructed with the modified Weil pairing or Tate pairing [45], [46] on the supersingular elliptic curve $\mathbb{G}_1$, where the following characteristics are presented.

Definition 1: (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 $\mathcal{A}$ is negligible as defined:

$$Adv_{\mathcal{A},\mathbb{G}_1}^{CDHP} = \Pr\left[\mathcal{A}(P, aP, bP) \to abP : a, b \in \mathbb{Z}_q^*\right].$$

Definition 2: (Elliptic Curve Discrete Logarithm Problem (ECDLP)): Given $P, Q \in \mathbb{G}_1$, 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 $\mathcal{A}$ is negligible as defined:

$$Adv_{\mathcal{A},\mathbb{G}_1}^{ECDLP} = \Pr\left[\mathcal{A}\left(P, aP\right) \rightarrow a : a \in \mathbb{Z}_q^*\right].$$

C. HASH FUNCTION

A one-way hash function $h(\cdot)$ is defined to be secure if the following properties can be achieved [47]:

1) Input a message x of arbitrary length, it is easy to compute a message digest of a fixed length output $h(x)$.
2) Given y, it is hard to compute $x = h^{-1}(y)$.
3) Given x, it is computationally infeasible to find $x' = x$ such that $h(x') = h(x)$.

D. CHINESE REMAINDER THEOREM (CRT)

Let $\{n_1, n_2, \ldots, n_k\}$ be the pairwise co-prime positive integers. For arbitrary sequence of integers $\{a_1, a_2, \ldots, a_k\}$, the system congruences defined as

$$\begin{cases} x \equiv a_1 \bmod n_1 \\ x \equiv a_2 \bmod n_2 \\ \quad \vdots \\ x \equiv a_k \bmod n_k \end{cases}$$

has a unique solution modulo $N = \prod_{i=1}^{k} n_i$. For $i = 1, 2, \ldots, k$, compute

$$\begin{cases} y_i = \dfrac{N}{n_i} = n_1 n_2 \ldots n_{i-1} n_{i+1} \ldots n_k \\ z_i \equiv y_i^{-1} \bmod n_i. \end{cases}$$

Hence, $y_i z_i \equiv 1 \bmod n_i$ and $y_j \equiv 0 \bmod n_i$ for $i \neq j$. The solution can be computed as

$$\begin{aligned} x &= (a_1\, y_1\, z_1 + a_2\, y_2\, z_2 + \cdots + a_k y_k z_k) \bmod n_i \\ &= \left(\sum_{i=1}^{k} a_i y_i z_i\right) \bmod n_i \end{aligned}$$

E. NOTATIONS

As shown in Table 1, the notations used in our scheme are listed, respectively with the corresponding description.

F. SYSTEM MODEL

In our design, the novel VANETs system model employing cloud server and edge computing RSU infrastructure are constructed. As shown in Fig. 1, the entire VANETs system model consists of three different layers with distinctive functionalities: the cloud layer, edge layer, and user layer. The relevant description of the three layers are respectively illustrated below.

Cloud layer are defined as the core cloud server in charge of the whole VANETs system. With the utilization of cloud computing architecture, adequate computation and storing capacities are enabled. Respectively, cloud server takes the responsibilities of trusted authority (TA) for system management, and remote database for massive data storing. Note that

TABLE 1. Notations.

Symbol	Description
TA, RSU	Trusted Authority, Road-Side Units
$\mathbb{G}_1, \mathbb{G}_2$	Cyclic Groups
P	Generator of $\mathbb{G}_1$
$\hat{e}$	Bilinear Pairing
ID_T, ID_{RSU}	RSU Identity
$\langle s_{RSU}, r_{RSU} \rangle$	Partial Secret Key Pair of RSU
ID_V^i, ID_i	Vehicle Identity
sk_i	Vehicle Session Key
$\{vsk_i\}_{i\in[1,m]}$	Vehicle Private Key Set
gk	Group Key for V2V Communication
$\{\partial_i\}_{i\in[0,m]}$	Coefficients Set of $\Upsilon(x)$
$\langle k_i, r_i \rangle$	Partial Secret Key Pair of Vehicle
$\{H_i\}_{i\in[1,4]}, \{h_i\}_{i\in[1,2]}$	Secure Hash Functions

TA is assumed to be valid and trustworthy anytime. With full authority, TA handles vital VANETs tasks including vehicle registration, key distribution, and identification, while confidential system parameters and vehicle secret keys are preserved in the remote database. Note that the cloud layer is able to simultaneously supervise substantial vehicular networks from different areas, which facilitates the development of global Internet of vehicle (IoV). For better description, we consider the TA and remote database to be one entity in the proposed scheme.

Edge layer refers to the distributed local RSUs facilities, where the computation and data storage are collaboratively conducted by the local RSU cluster in edge network, leading to decentralized data and service provision. The RSU edge cluster consumes data coming from both cloud server and vehicles, leveraging physical proximity to terminal user. Consequently, the VANETs can be drastically improved with lower latency, better response time and transfer rates. In our design, individual RSUs are established along the road sides at fix intervals. Hence, the effective range of VANETs could cover the whole road sections. Practically, some RSUs are located in severe natural environment far away from the central server. Hence, it is possible that the RSUs may be compromised or disabled. In this way, for privacy preserving consideration, the crucial vehicles secret information, along with the specific vehicle identity, should not be fully revealed to RSUs.

User layer is composed of the vehicle networks built with V2V and V2R communication. The on-board units (OBUs) with wireless communication modules including transceiver and transponder are implemented in each vehicle. Hence, longitudinal data transmission and reception with the neighboring RSU are enabled in mobile environment, while data sharing among nearby legitimate vehicles is available as well. Moreover, each vehicle is equipped with tamper-proof device (TPD) for confidential information preservation. Note that the driver and vehicle are considered as one entity in our system model. Due to resource restriction, complex computation and massive data storage are not supported in

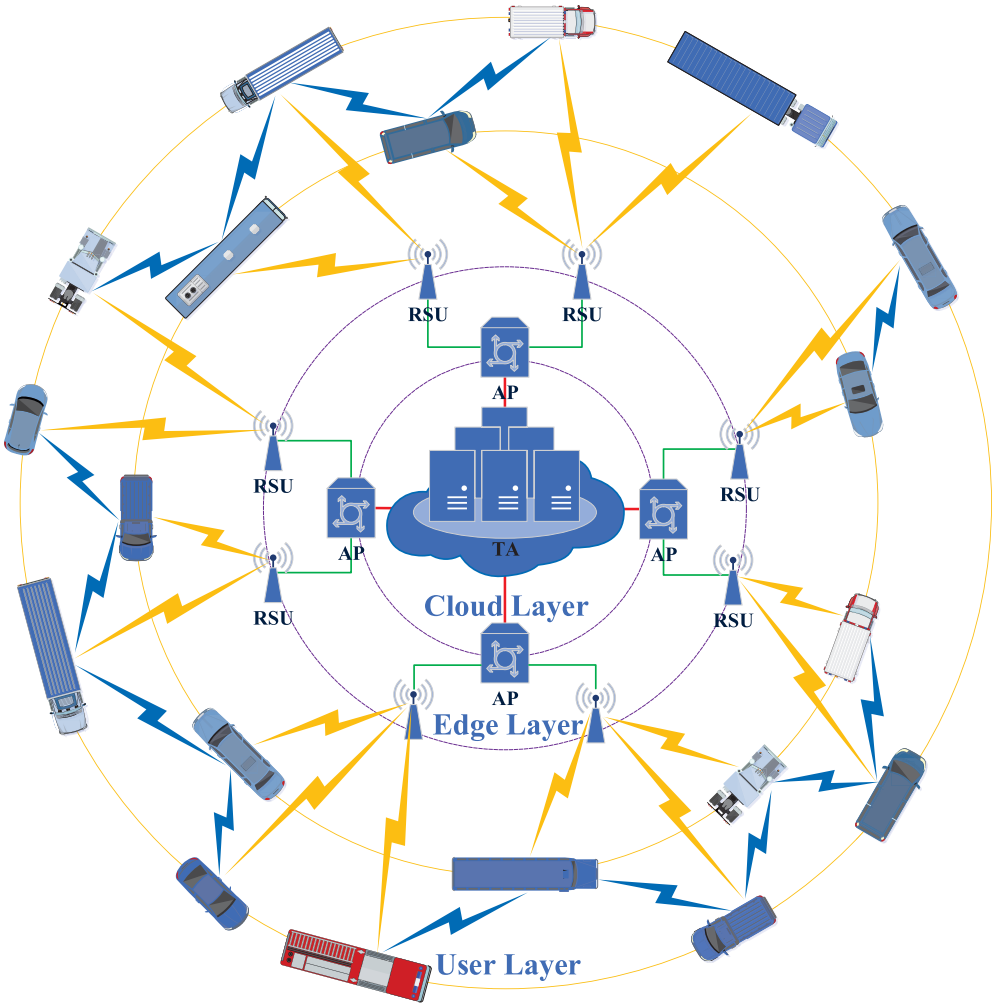


FIGURE 1. System model.

vehicle side. Therefore, lightweight authentication mechanism with comparatively limited computation and communication overhead is of great significance for VANETs.

G. NETWORKS ASSUMPTIONS

As illustrated in Fig. 1, TA is in charge of essential operations regarding all the participated RSUs and vehicles. With the implementation of local access points (APs), heterogeneous vehicular data aggregated in RSUs can be seamlessly delivered through wired connections with cloud server. However, some RSUs may be are compromised physically since they are far away from the cloud server, which cloud cause severe vehicle privacy disclosure. For this consideration, the original identity and master secret key of each vehicle should be distributed to RSU in an indirect way.

Generally, two types of VANETs wireless communication are executed, which includes vehicle to vehicle (V2V) communication and vehicle to RSU (V2R) communication. Note that both V2V and V2R exploits the dedicated short-range communications (DSRC) techniques. The vehicular data acquisition and feedback between specific vehicle and RSU are through V2R communication, while the distributed data sharing among nearby vehicles are conducted in V2V communication channel. Due to the intrinsic wireless transmission characteristics in open environment, both V2V and V2R communication are vulnerable to various security threats. Therefore, effective authentication and key distribution scheme should be designed for secure wireless transmission.

IV. PROPOSED V2R AUTHENTICATION SCHEME

In this section, the constructed certificateless authentication scheme is described, which emphasizes on V2R mutual authentication and session key distribution. Our design adopts the certificateless cryptography technique for key escrow avoidance, where TA and specific VANETs entity respectively manage the partial secret key pair. Anonymous identities of vehicles and RSUs are exploited during every authenticating session for identity preservation. Upon validation, the exclusive secret key is shared among TA and each legitimate vehicle so as to facilitate independent data exchange. Furthermore, bilinear pairing design is utilized in

RSUs side for superior security assurance, while the pairing operations are not conducted in resource-limited vehicle side. Intuitively, the proposed scheme can be roughly classified into **offline registration phase** and **authentication phase**. In offline registration phase, the nontrivial system initialization and essential key allocation are preliminarily performed. The registration process towards the participating vehicles and RSUs is conducted as well, which is mandatory for all the VANET devices. In this way, significant private information including the fundamental vehicle identities and initial secret keys are securely stored in TA side.

A. OFFLINE REGISTRATION PHASE

The offline registration phase is designed for VANET initialization and vehicle registration, which is explicitly executed in TA side. Note that TA is assumed to be valid and trustworthy during the entire authentication session. Initially, $\mathbb{G}_1$ and $\mathbb{G}_2$ are respectively defined as the cyclic additive group and cyclic multiplicative group generated by the same large prime order q, where P denotes a generator of $\mathbb{G}_1$. Meanwhile, map function $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is defined as bilinear pairing. The secure cryptographic hash functions $H_1, H_2, H_3, H_4, h_1, h_2$ are respectively performed as

$$\begin{cases} H_1 : \{0,1\}^* \times \{0,1\}^* \times \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{Z}_q^* \\ H_2 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times \mathbb{G}_1 \rightarrow \mathbb{Z}_q^* \\ H_3 : \{0,1\}^* \times \{0,1\}^* \times \mathbb{G}_1 \rightarrow \mathbb{Z}_q^* \\ H_4 : \mathbb{G}_1 \rightarrow \mathbb{Z}_q^* \\ h_1 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \rightarrow \mathbb{Z}_q^* \\ h_2 : \{0,1\}^* \times \{0,1\}^* \rightarrow \mathbb{Z}_q^*. \end{cases} \tag{1}$$

Accordingly, the parameters set is published, which contains $param=\{\mathbb{G}_1, \mathbb{G}_2, \hat{e}, q, P, H_1, H_2, H_3, H_4, h_1, h_2\}$.

Preliminarily, TA assigns the unique identity $ID_T \in \{0,1\}^*$ to each validated RSU, which will be well preserved in TA and RSU side. The corelated partial secret $s_{RSU} \in \mathbb{Z}_q^*$ is randomly generated for specific RSU. Therefore, the confidential RSU information set $\langle ID_T, s_{RSU} \rangle$ is safely shared among TA and RSU itself. Similarly, it is prerequisite for all the vehicles to register to TA in advance. In this way, the distinctive vehicle identity $ID_V^i \in \{0,1\}^*$ is distributed, along with the partial secret key $k_i \in \mathbb{Z}_q^*$ generated by TA. Note that the entire registration phase is securely executed in offline mode. Vital vehicular information involving user name, address, social identifier, and phone number, are recorded in cloud server.

Periodically, the registered RSU randomly generates $r_{RSU} \in \mathbb{Z}_q^*$ and computes RSU session identity ID_{RSU} as

$$ID_{RSU} = h_1 \left(ID_T, TS_1, r_{RSU} \right), \tag{2}$$

where the current timestamp TS_1 is adopted for freshness. In this case, each session identity ID_{RSU} is valid within certain time interval. The partial secret key pair is stored as $\langle s_{RSU}, r_{RSU} \rangle$, while r_{RSU} is kept secret to TA. Subsequently, the following calculations are conducted by RSU

$$\begin{cases} R = r_{RSU} P \\ Q = s_{RSU} h_2 \left(ID_{RSU}, r_{RSU} \right) P \\ Cert = H_1 \left(ID_{RSU}, TS_N, R, Q \right), \end{cases} \tag{3}$$

where TS_N denotes the latest timestamp. At this point, the RSU parameters set $\{TS_N, ID_{RSU}, R, Q, Cert\}$ is published to all entities within its effective range.

B. AUTHENTICATION PHASE

In this phase, the detailed authentication process is described step by step. Assuming the vehicle with identity ID_V^i and partial secret key k_i is approaching the communicating range of certain RSU, vehicle itself generates another partial secret key $r_i \in \mathbb{Z}_q^*$ on its own. At this moment, the partial secret key pair $\langle k_i, r_i \rangle$ is stored in vehicle side. Hence, the temporary identity used in the authentication session is computed as

$$ID_i = H_2 \left(ID_V^i, TS_2, k_i, r_i P \right). \tag{4}$$

Note that timestamp TS_2 refers to the current time point for vehicle authentication. Meanwhile, vehicle is acknowledged of the published RSU parameters set $\{TS_N, ID_{RSU}, R, Q, Cert\}$. By validating the certificate $Cert$, integrity of the received message can be guaranteed. Thereafter, vehicle calculates the authenticating message according to

$$\begin{cases} \mathscr{R}_i = r_i P \\ A_i = H_2 \left(ID_i, ID_{RSU}, TS_2, \mathscr{R}_i \right). \end{cases} \tag{5}$$

Accordingly, the vehicle signature $\mathscr{Z}_i$ is computed as

$$\mathscr{Z}_i = A_i \left[r_i Q + k_i H_3 \left(ID_i, TS_2, k_i P \right) R \right] + H_4 \left(r_i k_i P \right) P, \tag{6}$$

which combines the published RSU parameters with vehicle partial secret keys $\langle k_i, r_i \rangle$. Vehicle then sends the authentication request

$$\langle Request, ID_i, TS_2, \mathscr{R}_i, A_i, \mathscr{Z}_i \rangle \tag{7}$$

to RSU for further verification.

Upon receipt of the requesting message, RSU checks the freshness of the received timestamp TS_2 and verifies A_i according to its session identity ID_{RSU}. Subsequently, RSU forwards $\langle ID_i, TS_2, \mathscr{R}_i \rangle$ to the cloud server for final identification. As mentioned above, significant identity information $\langle ID_V^i, k_i \rangle$ of all the legitimate vehicles are stored in cloud server. Therefore, TA adopts the delivered TS_2 and $\mathscr{R}_i$ to the records and computes the vehicle identity with the received one. If matches, identity of certain vehicle is confirmed. Hence, TA extracts the partial secret k_i and computes

$$\begin{cases} \aleph_i = \hat{e} \left(H_4 \left(k_i \mathscr{R}_i \right) P, P \right) \\ \Im_i = \hat{e} \left(k_i H_3 \left(ID_i, TS_2, k_i P \right) P, P \right), \end{cases} \tag{8}$$

which will be delivered to the RSU with session identity ID_{RSU}.

At this point, RSU is capable of executing the authentication process by validating the following equation:

$$\frac{\hat{e}\left(\mathscr{Z}_i, P\right)}{\hat{e}\left(h_2\left(ID_{RSU}, r_{RSU}\right) P, A_i \mathscr{R}_i\right)^{s_{RSU}} \aleph_i} \stackrel{?}{=} \Im_i^{A_i r_{RSU}}. \tag{9}$$

Note that the $\langle \Im_i, \aleph_i \rangle$ packet received from TA, as well as the $\langle \mathscr{Z}_i, A_i, \mathscr{R}_i \rangle$ derived from vehicle request, are applied in the above calculation. According to the aforementioned $\mathscr{Z}_i = A_i\left[r_i Q + k_i H_3\left(ID_i, TS_2, k_i P\right) R\right] + H_4\left(r_i k_i P\right) P$, we can get

$$\begin{aligned}
&\hat{e}\left(\mathscr{Z}_i, P\right) \\
&= \hat{e}\Big(A_i\left[r_i Q + k_i H_3\left(ID_i, TS_2, k_i P\right) R\right] \\
&\quad + H_4\left(r_i k_i P\right) P, P\Big) \\
&= \hat{e}\Big(A_i\left[r_i Q + k_i H_3\left(ID_i, TS_2, k_i P\right) R\right], P\Big) \\
&\quad \times \hat{e}\Big(H_4\left(r_i k_i P\right) P, P\Big) \\
&= \hat{e}\Big(A_i r_i Q + A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\Big) \\
&\quad \times \hat{e}\Big(H_4\left(r_i k_i P\right) P, P\Big) \\
&= \hat{e}\Big(A_i r_i Q, P\Big) \cdot \hat{e}\Big(A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\Big) \\
&\quad \times \hat{e}\Big(H_4\left(r_i k_i P\right) P, P\Big).
\end{aligned} \tag{10}$$

With $Q = s_{RSU} h_2\left(ID_{RSU}, r_{RSU}\right) P$, $\mathscr{R}_i = r_i P$, $\aleph_i = \hat{e}\left(H_4\left(k_i \mathscr{R}_i\right) P, P\right)$, $R = r_{RSU} P$, and $A_i = H_2\left(ID_i, ID_{RSU}, TS_2, \mathscr{R}_i\right)$, the correctness of equation (9) can be elaborated as follows:

$$\begin{aligned}
&L.H.S. \\
&= \frac{\hat{e}\left(\mathscr{Z}_i, P\right)}{\hat{e}\left(h_2\left(ID_{RSU}, r_{RSU}\right) P, A_i \mathscr{R}_i\right)^{s_{RSU}} \aleph_i} \\
&= \frac{\hat{e}\left(A_i r_i Q, P\right) \hat{e}\left(A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\right)}{\hat{e}\left(h_2\left(ID_{RSU}, r_{RSU}\right) P, A_i \mathscr{R}_i\right)^{s_{RSU}}} \\
&\quad \times \frac{\hat{e}\left(H_4\left(r_i k_i P\right) P, P\right)}{\aleph_i} \\
&= \frac{\hat{e}\left(A_i r_i Q, P\right) \hat{e}\left(A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\right)}{\hat{e}\left(h_2\left(ID_{RSU}, r_{RSU}\right) P, A_i r_i P\right)^{s_{RSU}}} \\
&\quad \times \frac{\hat{e}\left(H_4\left(r_i k_i P\right) P, P\right)}{\aleph_i} \\
&= \frac{\hat{e}\left(A_i r_i Q, P\right) \hat{e}\left(A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\right)}{\hat{e}\left(A_i r_i h_2\left(ID_{RSU}, r_{RSU}\right) P, P\right)^{s_{RSU}}} \\
&\quad \times \frac{\hat{e}\left(H_4\left(r_i k_i P\right) P, P\right)}{\aleph_i} \\
&= \frac{\hat{e}\left(A_i r_i Q, P\right) \hat{e}\left(A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\right)}{\hat{e}\left(A_i r_i \left[s_{RSU} h_2\left(ID_{RSU}, r_{RSU}\right) P\right], P\right)} \\
&\quad \times \frac{\hat{e}\left(H_4\left(r_i k_i P\right) P, P\right)}{\aleph_i} \\
&= \frac{\hat{e}\left(A_i r_i Q, P\right) \hat{e}\left(A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\right)}{\hat{e}\left(A_i r_i Q, P\right)} \\
&\quad \times \frac{\hat{e}\left(H_4\left(r_i k_i P\right) P, P\right)}{\aleph_i} \\
&= \hat{e}\left(A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\right) \\
&\quad \times \frac{\hat{e}\left(H_4\left(r_i k_i P\right) P, P\right)}{\aleph_i} \\
&= \hat{e}\left(A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\right) \\
&\quad \times \frac{\hat{e}\left(H_4\left(r_i k_i P\right) P, P\right)}{\aleph_i} \\
&= \frac{\hat{e}\left(A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\right) \hat{e}\left(H_4\left(r_i k_i P\right) P, P\right)}{\hat{e}\left(H_4\left(k_i \mathscr{R}_i\right) P, P\right)} \\
&= \frac{\hat{e}\left(A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\right) \hat{e}\left(H_4\left(r_i k_i P\right) P, P\right)}{\hat{e}\left(H_4\left(k_i r_i P\right) P, P\right)} \\
&= \hat{e}\left(A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\right) \\
&= \hat{e}\Big(H_2\left(ID_i, ID_{RSU}, TS_2, \mathscr{R}_i\right) k_i \\
&\quad \cdot H_3\left(ID_i, TS_2, k_i P\right) R, P\Big) \\
&= \hat{e}\Big(H_2\left(ID_i, ID_{RSU}, TS_2, r_i P\right) k_i \\
&\quad \cdot H_3\left(ID_i, TS_2, k_i P\right) R, P\Big) \\
&= \hat{e}\Big(H_2\left(ID_i, ID_{RSU}, TS_2, r_i P\right) k_i \\
&\quad \cdot H_3\left(ID_i, TS_2, k_i P\right) r_{RSU} P, P\Big).
\end{aligned} \tag{11}$$

Hence, the value of $L.H.S.$ is derived. On the other hand, according to $\Im_i = \hat{e}\left(k_i H_3\left(ID_i, TS_2, k_i P\right) P, P\right)$, we can get

$$\begin{aligned}
R.H.S. &= \Im_i^{A_i r_{RSU}} \\
&= \hat{e}\Big(k_i H_3\left(ID_i, TS_2, k_i P\right) P, P\Big)^{A_i r_{RSU}} \\
&= \hat{e}\Big(A_i r_{RSU} k_i H_3\left(ID_i, TS_2, k_i P\right) P, P\Big) \\
&= \hat{e}\Big(H_2\left(ID_i, ID_{RSU}, TS_2, \mathscr{R}_i\right) r_{RSU} k_i \\
&\quad \cdot H_3\left(ID_i, TS_2, k_i P\right) P, P\Big) \\
&= \hat{e}\Big(H_2\left(ID_i, ID_{RSU}, TS_2, r_i P\right) k_i \\
&\quad \cdot H_3\left(ID_i, TS_2, k_i P\right) r_{RSU} P, P\Big) \\
&= L.H.S.
\end{aligned} \tag{12}$$

Intuitively, with $R.H.S. = L.H.S.$, equation (9) is proven to be correct. Therefore, if the request message does not pass the validation process, current authentication session is terminated. Otherwise, RSU computes

$$\begin{cases} ID_i^{\dagger} = h_2\left(ID_i, H_4\left(r_{RSU} \mathscr{R}_i\right)\right) \\ Cert_i^{\dagger} = H_2\left(ID_{RSU}, TS_3, ID_i^{\dagger}, \aleph_i\right) \end{cases} \tag{13}$$

and distributes the acknowledgement message as

$$\left\langle TS_3, ID_i^{\dagger}, Cert_i^{\dagger} \right\rangle, \tag{14}$$

where TS_3 denotes the latest timestamp.

Upon receiving the acknowledgement message, vehicle first checks the freshness of TS_3, then validates the

correctness of $ID_i^{\dagger}$ and $ID_i^{\dagger}$ according to

$$ID_i^{\dagger} = h_2\big(ID_i, H_4\left(r_{RSU}\mathscr{R}_i\right)\big) = h_2\big(ID_i, H_4\left(r_iR\right)\big). \quad (15)$$

Note that the updated identity $ID_i^{\dagger}$ is adopted for message unlinkability within the authentication session.

At this point, mutual authentication among vehicle and RSU is provided, which adopts certificateless cryptographic technique for avoidance of key escrow issue. That it, the partial secret keys of individual vehicle are respectively generated by TA and vehicle itself. Moreover, bilinear pairing is utilized, while the complex pairing calculations are mainly executed by cloud server, offering new prospect for resource constrained VANET devices. In our design, the shared session key sk_i for individual vehicle is independently constructed as $sk_i = H_4\left(\aleph_i\right)$, which can be used for secure V2R data exchange.

Practically, in VANETs environment involving large numbers of vehicles, individual RSU takes the responsibility for simultaneous authentication towards all the requesting vehicles in its vicinity. Hence, efficient batch authentication design is of significance. In this way, instead of independently conducting validation for all vehicles, each RSU is capable of processing the request message from multiple devices at a time, which significantly reduces the computation cost for massive vehicles validation. The corresponding authentication process is briefly described as follows.

Assuming n vehicles are to be authenticated by same RSU, each are allocated the distinctive vehicle identity and the partial secret key $k_i \in \mathbb{Z}_q^*$ $(i \in [1,n])$ during registration phase. In this way, authentication requests $\langle Request, ID_i, TS_2, \mathscr{R}_i, A_i, \mathscr{Z}_i\rangle_{i\in[1,n]}$ from n vehicles are respectively delivered to RSU. As mentioned above, the RSU parameters set is defined as $\{TS_N, ID_{RSU}, R, Q, Cert\}$. Hence, RSU executes the following batch authentication calculation

$$\frac{\hat{e}\left(\sum_{i=1}^{n}\mathscr{Z}_i, P\right)}{\hat{e}\left(h_2\left(ID_{RSU}, r_{RSU}\right)P, \sum_{i=1}^{n}A_i\mathscr{R}_i\right)^{s_{RSU}}\prod_{i=1}^{n}\aleph_i} \stackrel{?}{=} \left(\prod_{i=1}^{n}\Im_i^{A_i}\right)^{r_{RSU}}. \quad (16)$$

With the previously acquired $\mathscr{Z}_i$ from n different vehicles, we can get

$$\begin{aligned}
&\hat{e}\left(\sum_{i=1}^{n}\mathscr{Z}_i, P\right)\\
&= \hat{e}\Big(\sum_{i=1}^{n}\Big(A_i\left[r_iQ + k_iH_3\left(ID_i, TS_2, k_iP\right)R\right]\\
&\quad + H_4\left(r_ik_iP\right)P\Big), P\Big)\\
&= \hat{e}\Big(\sum_{i=1}^{n}A_i\left[r_iQ + k_iH_3\left(ID_i, TS_2, k_iP\right)R\right]\\
&\quad + \sum_{i=1}^{n}H_4\left(r_ik_iP\right)P, P\Big)\\
&= \hat{e}\left(\sum_{i=1}^{n}A_i\left[r_iQ + k_iH_3\left(ID_i, TS_2, k_iP\right)R\right], P\right)\\
&\quad \times\hat{e}\Big(\sum_{i=1}^{n}H_4\left(r_ik_iP\right)P, P\Big)\\
&= \hat{e}\Big(\sum_{i=1}^{n}\left(A_ir_iQ\right) + \sum_{i=1}^{n}A_ik_iH_3\left(ID_i, TS_2, k_iP\right)R, P\Big)\\
&\quad \times\hat{e}\Big(\sum_{i=1}^{n}H_4\left(r_ik_iP\right)P, P\Big)\\
&= \hat{e}\left(\sum_{i=1}^{n}A_ik_iH_3\left(ID_i, TS_2, k_iP\right)R, P\right)\\
&\quad \times\hat{e}\left(\sum_{i=1}^{n}A_ir_iQ, P\right)\hat{e}\left(\sum_{i=1}^{n}H_4\left(r_ik_iP\right)P, P\right). \quad (17)
\end{aligned}$$

Due to $Q = s_{RSU}h_2\left(ID_{RSU}, r_{RSU}\right)P$ and $\aleph_i = \hat{e}\left(H_4\left(k_i\mathscr{R}_i\right)P, P\right)$, the correctness of equation (16) can be briefly elaborated as

$$\begin{aligned}
L.H.S. &= \frac{\hat{e}\left(\sum_{i=1}^{n}\mathscr{Z}_i, P\right)}{\hat{e}\left(h_2\left(ID_{RSU}, r_{RSU}\right)P, \sum_{i=1}^{n}A_i\mathscr{R}_i\right)^{s_{RSU}}\prod_{i=1}^{n}\aleph_i}\\
&= \frac{\hat{e}\left(\sum_{i=1}^{n}A_ik_iH_3\left(ID_i, TS_2, k_iP\right)R, P\right)}{\hat{e}\left(s_{RSU}h_2\left(ID_{RSU}, r_{RSU}\right)P, \sum_{i=1}^{n}A_ir_iP\right)}\\
&\quad \times\frac{\prod_{i=1}^{n}\hat{e}\left(A_ir_iQ, P\right)\hat{e}\left(\sum_{i=1}^{n}H_4\left(r_ik_iP\right)P, P\right)}{\prod_{i=1}^{n}\aleph_i}\\
&= \frac{\hat{e}\left(\sum_{i=1}^{n}A_ik_iH_3\left(ID_i, TS_2, k_iP\right)R, P\right)}{\hat{e}\left(\sum_{i=1}^{n}A_ir_i\left[s_{RSU}h_2\left(ID_{RSU}, r_{RSU}\right)P\right], P\right)}\\
&\quad \times\frac{\prod_{i=1}^{n}\hat{e}\left(A_ir_iQ, P\right)\hat{e}\left(\sum_{i=1}^{n}H_4\left(r_ik_iP\right)P, P\right)}{\prod_{i=1}^{n}\aleph_i}\\
&= \frac{\hat{e}\left(\sum_{i=1}^{n}A_ik_iH_3\left(ID_i, TS_2, k_iP\right)R, P\right)}{\prod_{i=1}^{n}\aleph_i}\\
&\quad \times\frac{\prod_{i=1}^{n}\hat{e}\left(A_ir_iQ, P\right)\hat{e}\left(\sum_{i=1}^{n}H_4\left(r_ik_iP\right)P, P\right)}{\prod_{i=1}^{n}\hat{e}\left(A_ir_iQ, P\right)}
\end{aligned}$$

$$= \hat{e}\left(\sum_{i=1}^{n} A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\right) \times \frac{\hat{e}\left(\sum_{i=1}^{n} H_4\left(r_i k_i P\right) P, P\right)}{\prod_{i=1}^{n} \aleph_i}$$

$$= \hat{e}\left(\sum_{i=1}^{n} A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\right) \times \frac{\hat{e}\left(\sum_{i=1}^{n} H_4\left(r_i k_i P\right) P, P\right)}{\prod_{i=1}^{n} \hat{e}\left(H_4\left(k_i \mathscr{R}_i\right) P, P\right)}$$

$$= \hat{e}\left(\sum_{i=1}^{n} A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\right) \quad . \tag{18}$$

Hence, $L.H.S. = \hat{e}\left(\sum_{i=1}^{n} A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\right)$. Moreover, according to $\Im_i = \hat{e}\left(k_i H_3\left(ID_i, TS_2, k_i P\right) P, P\right)$, we can get

$$\begin{aligned} R.H.S. &= \left(\prod_{i=1}^{n} \Im_i^{A_i}\right)^{r_{RSU}} \\ &= \prod_{i=1}^{n} \hat{e}\left(k_i H_3\left(ID_i, TS_2, k_i P\right) P, P\right)^{A_i r_{RSU}} \\ &= \prod_{i=1}^{n} \hat{e}\left(A_i k_i H_3\left(ID_i, TS_2, k_i P\right)\left[r_{RSU} P\right], P\right) \\ &= \prod_{i=1}^{n} \hat{e}\left(A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\right) \\ &= \hat{e}\left(\sum_{i=1}^{n} A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\right) \\ &= L.H.S. \end{aligned} \tag{19}$$

Intuitively, with $R.H.S. = L.H.S.$, equation (16) is proven to be correct.The batch authentication process involving n vehicles is performed in this way. V2R secure communication channel between TA and individual vehicle is guaranteed with the shared session key $sk_i = H_4\left(\aleph_i\right)$.

V. PROPOSED V2V GROUP KEY MANAGEMENT SCHEME

As one of the major functionalities in VANETs, vehicle to vehicle (V2V) communication facilitates continuous vehicular data exchange among neighboring vehicles, which is essential for specific VANET services such as traffic congestion control and emergency rescue. In this case, with the purpose of offering secure V2V transmission, advanced security strategies are indispensable.

Commonly, the existing researches emphasize on constructing the universally shared session key among RSU and all effective vehicles in it range. Therefore, the multipurpose group communication channel is built, where both V2R data exchange and V2V data sharing are concurrently executed. However, due to high mobility of participating vehicles, V2V group topology varies at every moment. The distributed group key should be timely updated as long as the group membership changes, which severely interferes the V2R data exchange and causes large computation and communication burden for resource limited vehicles.

For this consideration, instead of maintaining the universal session key, we design the specialized group channel for V2V communications so that the variation in vehicle topology will not affect the V2R connection. Furthermore, reliable group key management mechanism employing CRT is adopted, where the generated group key can be distributed in a secure way. During the key updating process, consortium blockchain is utilized for recording the identity of participating vehicle. Hence, the historical vehicle information can be traced if necessary. Note that the key updating process requires limited calculation in vehicle side, while the revoked devices cannot correctly decrypt the newly updated session key. The proposed group key management scheme is described as **V2V group construction employing CRT**, and **dynamic key updating with consortium blockchain**, respectively.

A. V2V GROUP CONSTRUCTION EMPLOYING CRT

In this section, detailed V2V group formation process is illustrated step by step. As mentioned above, the RSU public parameters set $\{TS_N, ID_{RSU}, R, Q, Cert\}$ has already been published, where $R = r_{RSU} P$. Initially, RSU randomly generates $r_G \in \mathbb{Z}_q^*$ and computes

$$\begin{cases} \Phi = r_G P \\ Cert_G^{\ddagger} = H_1\left(ID_{RSU}, TS_G, R, \Phi\right). \end{cases} \tag{20}$$

Subsequently, $\left\langle Request, ID_{RSU}, TS_G, \Phi, Cert_G^{\ddagger}\right\rangle$ is distributed to all legitimate vehicles in its range. Note that TS_G denotes the current timestamp.

Upon receiving the grouping request, the vehicles independently make their decision on whether to participate in the current vehicle group. The willing vehicles check freshness and validity of the grouping request. If verified, the vehicle randomly generates $r_i^v \in \mathbb{Z}_q^*$ and computes

$$\begin{cases} \Theta_i = r_i^v P \\ ID_i^{\hbar} = H_3\left(ID_V^i, TS_G^2, \Phi\right) \\ Cert_G^i = H_4\left(sk_i H_4\left(k_i \Theta_i\right) \Phi\right). \end{cases} \tag{21}$$

Therefore, the responding message $\left\langle TS_G^2, ID_i^{\hbar}, \Phi, \Theta_i, Cert_G^i\right\rangle$ is delivered to RSU. At this moment, assuming RSU receives responding messages from m legitimate vehicles, the message sets will then be forwarded to TA for further verification. Subsequently, TA derives the vehicle private key as

$$vsk_i = H_4\left(k_i \Theta_i\right) \Phi \tag{22}$$

and forwards vsk_i $(i \in [1, m])$ to RSU.

Consequently, for $i \in [1, m]$, RSU computes

$$\begin{cases} \Psi = \prod_{i=1}^{m} vsk_i \\ \sigma_i = \dfrac{\Psi}{vsk_i} \\ \mu_i \equiv \sigma_i^{-1} \bmod vsk_i. \end{cases} \tag{23}$$

Note that $\mu_i \sigma_i = 1 \pmod{vsk_i}$ holds. Hence, RSU randomly generates the group key $gk \in \mathbb{Z}_q^*$ and computes keying value

$$\tau = gk \sum_{i=1}^{m} (\mu_i \sigma_i). \tag{24}$$

At this point, the following function is constructed by RSU:

$$\Upsilon(x) = \tau + \prod_{i=1}^{m} (x - vsk_i), \tag{25}$$

where the keying value and vehicle private key set $\{vsk_i\}_{i\in[1,m]}$ is adopted. The above equation (25) can be extracted into

$$\Upsilon(x) = \sum_{i=0}^{m} \partial_i x^i, \tag{26}$$

where the coefficients set is illustrated as $\{\partial_i\}_{i\in[0,m]}$. Obviously, for $\forall \ell \in [1, m]$, we have

$$\Upsilon(vsk_\ell) = \tau + \prod_{i=1}^{m} (vsk_\ell - vsk_i) = \tau. \tag{27}$$

Hence, the following computation is conducted as

$$Cert_{gk} = h\left(ID_{RSU}, TS_{gk}, \partial_0, \ldots, \partial_m, \tau\right), \tag{28}$$

where $h(\cdot)$ denotes the secure hash function. Accordingly, RSU issues the keying packet as

$$\left\langle TS_{gk}, ID_{RSU}, \{\partial_i\}_{i\in[0,m]}, Cert_{gk} \right\rangle. \tag{29}$$

Finally, the vehicles receive the keying packet and reconstructs the function $\Upsilon(x)$ after validating TS_{gk} and $Cert_{gk}$. Therefore, the distributed group key gk can be correctly derived by all the m vehicles according to

$$gk = \Upsilon(vsk_i) \bmod vsk_i. \tag{30}$$

In this way, the V2V group key is shared among all requesting vehicles. The vehicle group involving m neighboring vehicles is constructed accordingly.

B. DYNAMIC KEY UPDATING WITH CONSORTIUM BLOCKCHAIN

Motivated by the design of consortium blockchain, the dynamic key updating strategy is introduced. As mentioned above, specific vehicle group key is generated and distributed so as to support V2V data sharing. Considering the high mobility of vehicles, efficient key updating mechanism is of great significance. In our design, the m vehicles affiliated to certain group broadcasts their identities $ID_i^{\hbar}$ at certain time interval. Hence, each vehicle is aware of identities of all the participating vehicles and respectively stores the identity set $\{ID_i^{\hbar}\}_{i\in[1,m]}$. Again, each vehicle securely delivers the acquired identity set to RSU using the previously allocated session key sk_i. At this point, all the m legitimate vehicles, along with the RSU and TA, are informed of the currently attending vehicles record in this group. In this way, the real time record on group members can be generated. The following calculation is conducted by all the vehicles and TA:

$$\Delta_0 = h\left(ID_1^{\hbar}, \ldots, ID_m^{\hbar}\right). \tag{31}$$

In this way, TA is capable of conducting timely key update adjusting to group changes. After certain time interval, broadcasting among the attending vehicles are conducted periodically. Assuming m_1 vehicles are available at this moment, each vehicle then computes

$$\Delta_1 = h\left(\Delta_0, ID_1^{\hbar}, \ldots, ID_{m_1}^{\hbar}\right), \tag{32}$$

which adopts the previously stored hash value Δ_0 and current vehicle identity set $\left\langle ID_1^{\hbar}, \ldots, ID_{m_1}^{\hbar} \right\rangle$. Accordingly, in future moment with m_i vehicles, we can get

$$\Delta_i = h\left(\Delta_{i-1}, ID_1^{\hbar}, \ldots, ID_{m_i}^{\hbar}\right). \tag{33}$$

Note that the calculated Δ_i is related to all the historical information, as well as the current identity set $\left\langle ID_1^{\hbar}, \ldots, ID_{m_i}^{\hbar} \right\rangle$. The dynamic key updating process is available as follows:

Assuming α vehicles with private session key $vsk_i^{\oslash}$ ($i \in [1, \alpha]$) are to be revoked from the group, RSU updates the related $\langle \mu_i, \sigma_i \rangle$ for the remaining $m - \alpha$ vehicles. The modified $\Upsilon(x)$ function is then built in the way of

$$\Upsilon(x) = gk^{\oslash} \sum_{i=1}^{m-\alpha} (\mu_i \sigma_i) + \prod_{i=1}^{m-\alpha} (x - vsk_i). \tag{34}$$

The above equation (34) can be extracted into

$$\Upsilon(x) = \sum_{i=0}^{m-\alpha} \partial_i x^i, \tag{35}$$

where the coefficients set is illustrated as $\{\partial_i\}_{i\in[0,m-\alpha]}$. Hence, the new keying packet is defined as

$$\left\langle TS_{gk}^{\oslash}, ID_{RSU}, \{\partial_i\}_{i\in[0,m-\alpha]}, Cert_{gk}^{\oslash} \right\rangle. \tag{36}$$

Therefore, the distributed group key $gk^{\oslash}$ can be correctly derived by the remaining $m - \alpha$ vehicles according to

$$gk^{\oslash} = \Upsilon(vsk_i) \bmod vsk_i. \tag{37}$$

In this way, the V2V group key involving multiple vehicles can be safely updated. Note that the new vehicle join process is similar with the revocation design. It is worth noting that the proposed key updating strategy is able to provide efficient group key updating involving multiple joined and revoked vehicles simultaneously. The revoked vehicles cannot derive the updated key due to the removal of session key $vsk_i^{\oslash}$ from $\Upsilon(x)$ function. Similarly, the newly joined vehicles can derive the updated group key using the stored vsk_i. At this point, the group key updating strategy is enabled in this way.

VI. SECURITY ANALYSIS

In this section, the featured security properties of the proposed authentication scheme are analyzed. The security theorems along with the corresponding proofs are formally given. Furthermore, the comparisons in terms of the major security characteristics with the state-of-the-arts are presented.

A. UNFORGEABILITY AGAINST CHOSEN MESSAGE ATTACK

We analysis the unforgeability against adaptive chosen message attack (CMA) in the proposed authentication scheme.

Definition 3 (Forking Lemma [48]): Let $\mathscr{A}$ be a probabilistic polynomial time Turing machine, given only the public data as input. Within a certain time bound $\mathcal{T}$, if $\mathscr{A}$ can produce, with non-negligible probability, a valid signature $(m, \sigma_1, h, \sigma_2)$, where the tuple (σ_1, h, σ_2) can be simulated without knowing the secret key, then, with an indistinguishable distribution probability, there is another machine which has control over the machine obtained from $\mathscr{A}$ replacing interaction with the signer by simulation and produces two valid signatures $(m, \sigma_1, h, \sigma_2)$ and $(m, \sigma_1, h', \sigma_2')$ such that $h \neq h'$.

Theorem 1: The proposed certificateless authentication scheme is provably unforgeable towards adaptive chosen message attack (CMA) in the assumption of random oracle model, if and only if the CDHP is hard.

Proof: Formally, the unforgeability of the proposed scheme can be defined through the game $\mathscr{G}_1$. Initially, let $\mathscr{A}_1$ be a probabilistic polynomial time (PPT) adversary. Note that $\mathscr{A}_1$ is assumed to have the capability to break the proposed authentication scheme. In the constructed game $\mathscr{G}_1$, the utilized hash functions are defined as random oracles. In this way, it is claimed that by operating the following queries from adversary $\mathscr{A}_1$, the challenger $\mathscr{C}_1$ is able to break the randomness of oracles' outputs with the assistance of adversary $\mathscr{A}_1$. Moreover, the hash recording lists are maintained by $\mathscr{C}_1$. Meanwhile, $\mathscr{C}_1$ is able to simulate all the oracles. The corresponding queries of $\mathscr{C}_1$ can be adaptively issued by $\mathscr{A}_1$ as follows:

- *H_3 Hash Query:* Assume that $\mathscr{A}_1$ does not have the ability to calculate the hash function $H_3(\cdot)$. In order to respond to *H_3 Hash Query*, $\mathscr{C}_1$ maintains a hash list H^3_{list} of couples $\langle \circledast_i, \eta_i \rangle$ initialized to be empty. Note that $\circledast_i$ is defined as the input value pair including $\langle ID_i, TS_2, k_iP \rangle$, where $k_iP \in \mathbb{G}$. In this case, when the adversary $\mathscr{A}_1$ invokes the *H_3 Hash Query* with a particular input value set $\circledast_i$, $\mathscr{C}_1$ checks whether the parameter $\circledast_i$ exists in the current hash list H^3_{list}, and executes as follows:
  - If the value pair $\circledast_i$ has already been stored in H^3_{list}, $\mathscr{C}_1$ outputs $\eta_i = H_3\,(ID_i, TS_2, k_iP)$ to $\mathscr{A}_1$.
  - Otherwise, $\mathscr{C}_1$ chooses a random $\eta_i \in \mathbb{Z}_q^*$ and forwards it to $\mathscr{A}_1$. Note that the new tuple $\langle \circledast_i, \eta_i \rangle$ will be subsequently added to H^3_{list}.
- *H_4 Hash Query:* Assume that $\mathscr{A}_1$ does not have the ability to calculate the hash function $H_4(\cdot)$. In order to respond to *H_4 Hash Query*, $\mathscr{C}_1$ maintains a hash list H^4_{list} of couples $\langle \circledcirc_i, \eth_i \rangle$ initialized to be empty. Note that $\circledcirc_i$ is defined as the input value pair including $r_ik_iP \in \mathbb{G}$, where $k_iP \in \mathbb{G}$. In this case, when the adversary $\mathscr{A}_1$ invokes the *H_4 Hash Query* with a particular input value set $\circledcirc_i$, $\mathscr{C}_1$ checks whether the parameter $\circledcirc_i$ exists in the current hash list H^4_{list}, and executes as follows:
  - If the value pair $\circledcirc_i$ has already been stored in H^4_{list}, $\mathscr{C}_1$ outputs $\eth_i = H_4\,(r_ik_iP)$ to $\mathscr{A}_1$.
  - Otherwise, $\mathscr{C}_1$ chooses a random $\eth_i \in \mathbb{Z}_q^*$ and forwards it to $\mathscr{A}_1$. Note that the new tuple $\langle \circledcirc_i, \eth_i \rangle$ will be subsequently added to H^4_{list}.
- *h Hash Query:* Assume that $\mathscr{A}_1$ does not have the ability to calculate the hash function $h_2(\cdot)$. In order to respond to *h Hash Query*, $\mathscr{C}_1$ maintains a hash list h^2_{list} of couples $\langle \odot_i, \wp_i \rangle$ initialized to be empty. Note that $\odot_i$ is defined as the input value pair including $\langle ID_{RSU}, r_{RSU} \rangle$, where $k_iP \in \mathbb{G}$. In this case, when the adversary $\mathscr{A}_1$ invokes the *h Hash Query* with a particular input value set $\odot_i$, $\mathscr{C}_1$ checks whether the parameter $\odot_i$ exists in the current hash list h^2_{list}, and executes as follows:
  - If the value pair $\odot_i$ has already been stored in h^2_{list}, $\mathscr{C}_1$ outputs $\wp_i = h_2\,(ID_{RSU}, r_{RSU})$ to $\mathscr{A}_1$.
  - Otherwise, $\mathscr{C}_1$ chooses a random $\wp_i \in \mathbb{Z}_q^*$ and forwards it to $\mathscr{A}_1$. Note that the new tuple $\langle \odot_i, \wp_i \rangle$ will be subsequently added to h^2_{list}.
- *Extracting Query:* Upon the *Extracting Query* with $\circledast_i$ is made to $\mathscr{C}_1$, $\mathscr{C}_1$ conducts *H_3 hash Query* on the input $\circledast_i$ and outputs the corresponding tuple $\langle \circledast_i, \eta_i \rangle$. Note that the tuple $\langle \circledast_i, \eta_i \rangle$ has already been recorded in H^3_{list} previously. Similarly, *H_4 hash Query* and *h hash Query* are executed by $\mathscr{C}_1$, respectively with the input value $\langle \circledcirc_i, \eth_i \rangle$ and $\langle \odot_i, \wp_i \rangle$. Thereafter, $\mathscr{C}_1$ randomly selects $r_i, k_i \in \mathbb{Z}_q^*$ and computes $\langle \mathscr{R}_i, A_i, \mathscr{Z}_i, \aleph_i, \Im_i \rangle$. The calculated tuple $\langle \mathscr{R}_i, A_i, \mathscr{Z}_i, \aleph_i, \Im_i \rangle$ will be sent to $\mathscr{A}_1$.

Finally, according to **Definition 3**, within a polynomial time, adversary $\mathscr{A}_1$ is able to obtain two validated signatures $\langle ID_i, TS_2, \mathscr{R}_i, A_i, \mathscr{Z}_i, \aleph_i, \Im_i \rangle$ and $\left\langle ID_i, TS_2, \mathscr{R}_i, A_i, \mathscr{Z}_i^*, \aleph_i, \Im_i^* \right\rangle$ after querying $\mathscr{C}_1$, where both tuples can pass the authentication process. Let $h_2 = h_2\,(ID_{RSU}, r_{RSU})$, $H_3 = H_3\,(ID_i, TS_2, k_iP)$, $H_4 = H_4\,(r_ik_iP)$. That is,

$$\begin{cases} \dfrac{\hat{e}\,(\mathscr{Z}_i, P)}{\hat{e}\,(h_2\,P, A_i\mathscr{R}_i)^{s_{RSU}}\,\hat{e}\,(H_4P, P)} = \hat{e}\,(k_iH_3P, P)^{A_ir_{RSU}} \\ \dfrac{\hat{e}\left(\mathscr{Z}_i^*, P\right)}{\hat{e}\,(h_2\,P, A_i\mathscr{R}_i)^{s_{RSU}}\,\hat{e}\,(H_4P, P)} = \hat{e}\left(k_iH_3^*P, P\right)^{A_ir_{RSU}} \end{cases}, \tag{38}$$

which can be formulated into

$$\begin{cases} \left[\dfrac{\hat{e}\,(\mathscr{Z}_i, P)}{\hat{e}\,(h_2P, A_i\mathscr{R}_i)^{s_{RSU}}\,\hat{e}\,(H_4P, P)}\right]^{H_3^*} \\ = \hat{e}\,(k_iH_3P, P)^{A_iH_3^*r_{RSU}} \\ \left[\dfrac{\hat{e}\left(\mathscr{Z}_i^*, P\right)}{\hat{e}\,(h_2P, A_i\mathscr{R}_i)^{s_{RSU}}\,\hat{e}\,(H_4P, P)}\right]^{H_3} \\ = \hat{e}\left(k_iH_3^*P, P\right)^{A_iH_3r_{RSU}}. \end{cases} \tag{39}$$

Due to $\hat{e}\left(k_i H_3 P, P\right)^{A_i H_3^* r_{RSU}} = \hat{e}\left(k_i H_3^* P, P\right)^{A_i H_3 r_{RSU}}$, we can get

$$\left[\frac{\hat{e}\left(\mathscr{Z}_i, P\right)}{\hat{e}\left(h_2 P, A_i \mathscr{R}_i\right)^{s_{RSU}} \hat{e}\left(H_4 P, P\right)}\right]^{H_3^*} = \left[\frac{\hat{e}\left(\mathscr{Z}_i^*, P\right)}{\hat{e}\left(h_2 P, A_i \mathscr{R}_i\right)^{s_{RSU}} \hat{e}\left(H_4 P, P\right)}\right]^{H_3}, \quad (40)$$

which is further illustrated as

$$\frac{\hat{e}\left(H_3^* \mathscr{Z}_i, P\right)}{\hat{e}\left(s_{RSU} H_3^* h_2 P, A_i \mathscr{R}_i\right) \hat{e}\left(H_3^* H_4 P, P\right)} = \frac{\hat{e}\left(H_3 \mathscr{Z}_i^*, P\right)}{\hat{e}\left(s_{RSU} H_3 h_2 P, A_i \mathscr{R}_i\right) \hat{e}\left(H_3 H_4 P, P\right)}. \quad (41)$$

At this point, let $Q = aP$ and $A_i \mathscr{R}_i = bP$ for some $a, b \in \mathbb{Z}_q^*$. Then we have

$$\begin{aligned}
&\frac{\hat{e}\left(H_3^* \mathscr{Z}_i, P\right)}{\hat{e}\left(H_3 \mathscr{Z}_i^*, P\right)} \\
&= \frac{\hat{e}\left(s_{RSU} H_3^* h_2 P, A_i \mathscr{R}_i\right) \hat{e}\left(H_3^* H_4 P, P\right)}{\hat{e}\left(s_{RSU} H_3 h_2 P, A_i \mathscr{R}_i\right) \hat{e}\left(H_3 H_4 P, P\right)} \\
&= \hat{e}\left(s_{RSU} H_3^* h_2 P - s_{RSU} H_3 h_2 P, A_i \mathscr{R}_i\right) \\
&\quad \times \hat{e}\left(H_3^* H_4 P - H_3 H_4 P, P\right) \\
&= \hat{e}\left(\left(H_3^* - H_3\right) s_{RSU} h_2 P, A_i \mathscr{R}_i\right) \hat{e}\left(\left(H_3^* - H_3\right) H_4 P, P\right) \\
&= \hat{e}\left(\left(H_3^* - H_3\right) Q, A_i \mathscr{R}_i\right) \hat{e}\left(\left(H_3^* - H_3\right) H_4 P, P\right) \\
&= \hat{e}\left(\left(H_3^* - H_3\right) aP, bP\right) \hat{e}\left(\left(H_3^* - H_3\right) H_4 P, P\right) \\
&= \hat{e}\left(\left(H_3^* - H_3\right) abP, P\right) \hat{e}\left(\left(H_3^* - H_3\right) H_4 P, P\right) \\
&= \hat{e}\left(\left(H_3^* - H_3\right) (abP + H_4 P), P\right) \\
&= \hat{e}\left(H_3^* \mathscr{Z}_i - H_3 \mathscr{Z}_i^*, P\right). \quad (42)
\end{aligned}$$

According to $H_3 \neq H_3^*$ and $\mathscr{Z}_i \neq \mathscr{Z}_i^*$, $\mathscr{C}_1$ extracts the following equation:

$$H_3^* \mathscr{Z}_i - H_3 \mathscr{Z}_i^* = \left(H_3^* - H_3\right)(abP + H_4 P). \quad (43)$$

Thereafter, $\mathscr{C}_1$ calculates

$$abP = \left(H_3^* \mathscr{Z}_i - H_3 \mathscr{Z}_i^*\right)\left(H_3^* - H_3\right)^{-1} - H_4 P \quad (44)$$

and outputs abP as the solution to the CDHP instance $(Q, A_i \mathscr{R}_i) = (aP, bP)$.

At this moment, we show that $\mathscr{C}_1$ is able to use $\mathscr{A}_1$ to solve the given instance of CDHP. However, this contradicts with the hardness of the aforementioned CDHP. Hence, the advantage of $\mathscr{C}_1$ winning $\mathscr{G}_1$ is negligible. That is, the attacker cannot forge the transmitted message to successfully pass the verification process. The proposed authentication scheme is secure against forgery attack with CMA under random oracle model. Accordingly, message authentication, integrity and non-repudiation are achieved. ■

B. RESISTANCE TO REPLAY ATTACK

As one of the most common wireless networks attacking types, replay attack is carried out through maliciously reusing the acquired previous information in the current authentication process. The replay attack resistance of the proposed authentication scheme is illustrated as follows.

Theorem 2: The proposed VANETs authentication scheme provides resistance to replay attack during the entire authentication process. The transmitted messages from past sessions cannot pass the current validation.

Proof: Assuming that in current timepoint $\mathscr{T}_c$, the adversary $\mathscr{A}_2$ has access to all the transmitted packets during time interval $[\mathscr{T}_s, \mathscr{T}_e]$, where $\mathscr{T}_s < \mathscr{T}_e$. $\mathscr{A}_2$ extracts the vehicle packet $\left\langle Request, ID_i, TS_2^{\mathscr{T}}, \mathscr{R}_i, A_i, \mathscr{Z}_i \right\rangle$ with $TS_2^{\mathscr{T}} \in [\mathscr{T}_s, \mathscr{T}_e]$ and forwards it to receiver at $\mathscr{T}_c$. In the first place, freshness of the timestamp is verified in the receiver side. Since $TS_2^{\mathscr{T}} < TS_2^{\mathscr{T}_c}$, vehicle rejects the packet. Note that the timestamp is attached to all packets during each transmission. In other way, $\mathscr{A}_2$ replaces $TS_2^{\mathscr{T}}$ with $TS_2^{\mathscr{T}_c}$ and generates $\left\langle Request, ID_i, TS_2^{\mathscr{T}_c}, \mathscr{R}_i, A_i, \mathscr{Z}_i \right\rangle$. Obviously, $A_i^* = H_2\left(ID_i, ID_{RSU}, TS_2^{\mathscr{T}_c}, \mathscr{R}_i\right) \neq H_2\left(ID_i, ID_{RSU}, TS_2^{\mathscr{T}}, \mathscr{R}_i\right)$ with $TS_2^{\mathscr{T}} \neq TS_2^{\mathscr{T}_c}$, indicating that the usage towards historical information and current fresh timestamp is not achievable in our design. During each communication of our scheme, data integrity and confidentiality are timely preserved by the corresponding timestamp and certificates. Any modification towards the acquired messages results in failure of the verification process in receiver side. Note that the analysis for the remaining packet types are similar. In conclusion, the transmitted messages are fully protected with hash function. Moreover, each packet is mapped to precise timestamp. The replaying attack can be prevented in this way. ■

C. CONDITIONAL IDENTITY PRIVACY PRESERVING

In practical VANETs scenarios, open wireless transmission characteristics result in potential vulnerability towards illegal tracing, which are performed by malicious entities. In this case, user identity information and specific vehicular data from different sessions may be linked, leading to severe identity leaking towards targeted vehicle. Hence, vehicle identity privacy should be preserved during entire VANET transmission process. On the other hand, in order to provide non-repudiation, TA should have the ability to reveal real identity of malicious entities if necessary. Consequently, conditional identity privacy preserving is indispensable for practical VANETs. The provision to conditional identity privacy preserving is illustrated as follows.

Theorem 3: The proposed authentication scheme provides resistance to illegal tracing towards specific vehicles. Conditional identity privacy preserving for both vehicles and RSUs is guaranteed.

Proof: As described in the aforementioned offline registration phase, the initial identity for validated RSU is defined as $ID_T \in \{0, 1\}^*$, which is kept confidential all the time. Meanwhile, the RSU session identity is computed as $ID_{RSU} = h_1\left(ID_T, TS_1, r_{RSU}\right)$. It is worth noting that the included r_{RSU} is randomly generated by TA

TABLE 2. Comparison result on security properties.

Scheme	PATF [28]	IBCA [18]	ECAS [43]	EPFA [13]	Our Scheme
Unforgeability	√	√	√	√	√
Replay Attack Resistance	√	√	√	√	√
Conditional Anonymity	√	√	×	√	√
Session Key Establishment	√	×	√	√	√
Key Escrow Resilience	×	√	√	√	√
Scalability	×	√	×	√	√
Efficient Key Updating	√	×	√	×	√

in registration phase, while the timestamp TS_1 varies for individual session. That is, the RSU session identity ID_{RSU} is unique in each authentication process. Unlinkability in different session is provided in this way. Similarly, the vehicle original identity ID_V^i is kept secret. Instead, temporary vehicle identity $ID_i = H_2\left(ID_V^i, TS_2, k_i, r_iP\right)$ is applied. This way, illegal tracing towards certain VANET entity is prevented. Moreover, TA stores necessary keying information in its server. Hence, identity in each session can be further extracted if necessary, offering conditional identity privacy preserving. ■

D. SESSION KEY ESTABLISHMENT

In practical VANETs scenarios, secure and reliable data interactions in open wireless environment should be guaranteed. Hence, session keys for both V2R and V2V communication are constructed in the proposed design, respectively. The session key establishment property is briefly described as follows.

Theorem 4: The unique session key is delivered for individual vehicle, while the V2V group communication for neighboring vehicles is preserved with shared group key employing efficient updating mechanism.

Proof: Accordingly, the V2R certificateless authentication is carried out for all legitimate vehicles. Thereafter, vehicle session key is extracted as $sk_i = H_4(\aleph_i)$, which adopts the vehicle partial secret key k_i and random value r_i. Note that each vehicle maintains exclusive secret key for reliable data transmission. Moreover, the V2V secure communication is achieved by issuing the function $\Upsilon(x)$ to all entities, where $\Upsilon(x) = \tau + \prod_{i=1}^{m}(x - vsk_i)$. In this way, the keying information τ can be successfully delivered to m different vehicles as $\Upsilon(vsk_\ell) = \tau$ for $\forall \ell \in [1, m]$. Note that the utilized vehicle private key vsk_i is known only to TA and vehicle itself. That is, $\forall vsk^* \notin \{vsk_1, \ldots, vsk_m\}$, $\Upsilon(vsk^*) = \tau + \prod_{i=1}^{m}(vsk^* - vsk_i) \neq \tau$. In this way, the keying value can only be correctly derived using the validated vsk_i. Similarly, CRT is adopted to the key distribution process, where the final group key gk can be extracted as $gk = \Upsilon(vsk_i) \bmod vsk_i$. In conclusion, each vehicle maintains session keys sk_i and gk for V2R and V2V secure transmission. ■

E. CERTIFICATELESS AUTHENTICATION

As the significant variant of ID-based cryptography, certificateless authentication is capable of addressing the intrinsic key escrow problem. The key generation process is collaboratively conducted in key generation center (KGC) and user side. The proposed V2R design employs certificateless authentication structure, where TA does not have full authority of the allocated vehicle private key. In this section, we analysis the certificateless authentication property as follows.

Theorem 5: The proposed V2R authentication scheme is able to provide certificateless authentication property for all VANETs devices. The entire authentication and session key establishment processes are performed by adopting both partial keys from TA and vehicle itself.

Proof: In the aforementioned V2R registration phase, the partial secret key $s_{RSU} \in \mathbb{Z}_q^*$ for certain RSU is issued by TA, while the remaining partial secret key $r_{RSU} \in \mathbb{Z}_q^*$ is decided by RSU itself. In this case, the complete breakdown of central server will not lead to severe key information leakage. That is, deriving r_{RSU} from the published RSU parameter $R = r_{RSU}P$ is difficult due to ECDLP. Note that r_{RSU} is kept secret to TA during the entire process. In this way, impersonation towards specific vehicle sensors cannot be validated. Similarly, the vehicle partial secret key pair is defined as $\langle k_i, r_i \rangle$, where $r_i \in \mathbb{Z}_q^*$ is randomly generated by vehicle and kept confidential to all other entities. Hence, the certificateless authentication property is provided in the proposed scheme. ■

F. COMPARISON ON SECURITY PROPERTIES

In this section, the comparison results in terms of the crucial security properties for VANETs communication are presented. The proposed protocol is compared with the state-of-the-art VANETs authentication and key agreement schemes including PATF [28], IBCA [18], ECAS [43], and EPFA [13] with the purpose of demonstrating its superiority on security properties. The comparison results are presented in Table 2, indicating that the proposed scheme satisfies the desired security requirements.

VII. PERFORMANCE ANALYSIS

In this section, analysis towards performance of the proposed scheme is presented, which specifically emphasizes on the

TABLE 3. Comparison result on storage overhead.

Scheme	PATF [28]	IBCA [18]	ECAS [43]	EPFA [13]	Our Scheme
Storage Cost (RSU)	$1936n + 1048$ bits	$1760n + 1056$ bits	$2072n + 1344$ bits	$3992n + 1376$ bits	$1616n + 1360$ bits
Storage Cost (Vehicle)	3432 bits	2112 bits	2552 bits	4368 bits	2208 bits

crucial properties for resource-limited VANETs environment: **storage overhead**, **computation cost**, and **communication cost**.

A. STORAGE OVERHEAD

As illustrated in the VANET system model, vehicles and RSUs perform as the basic units in VANET communication, where massive vehicular data are aggregated and transited. However, due to the resource constraints for VANET devices in practical environment, storage overhead required for authentication process should be optimized. In the contrast, the cloud server (TA) is assumed to be core facility with adequate storing capacity. Therefore, our analysis mainly focuses on storage overhead of RSU and individual vehicle during V2R authentication process. The state-of-the-art VANET authentication schemes including PATF [28], IBCA [18], ECAS [43], and EPFA [13] are analyzed as well. Hence, advantages of our scheme on storage overhead can be demonstrated by the comparison results.

Initially, the static identity ID_T and corelated partial secret key $\langle s_{RSU}, r_{RSU} \rangle$ for individual RSU are safely stored. Upon registration, the RSU session identity ID_{RSU} is generated. Subsequently, the calculations on $\{R, Q, Cert\}$ are executed. Accordingly, we define the length of the identity such as ID_T and ID_{RSU} is 32 bits, while length of the elements in group $\mathbb{G}_1$ and $\mathbb{G}_2$ is 256 bits. The length of $Cert$ and s_{RSU}, and the timestamp TS_1 and TS_N are assumed to be 160 bits and 24 bits respectively. At this point, the total storage for individual RSU is calculated as $32 \times 2 + 256 \times 3 + 160 \times 3 + 24 \times 2 = 1360$ bits. In the subsequent authentication phase, RSU derives the authentication request from vehicles, which includes $\langle ID_i, TS_2, \mathscr{R}_i, A_i, \mathscr{Z}_i \rangle$. The received $\aleph_i$ and $\Im_i$ from TA is delivered for verification process. Moreover, the acknowledgement message $\left\langle TS_3, ID_i^{\dagger}, Cert_i^{\dagger} \right\rangle$ is generated. In this way, the storage overhead for n vehicles is computed as $(32 \times 2 + 256 \times 4 + 160 \times 2 + 24 \times 2)\, n = 1456n$ bits. With the distributed vehicle key sk_i, the total storage cost in RSU side is $1456n + 160n + 1360 = 1616n + 1360$ bits.

As for individual vehicle, the initial vehicle identity ID_V^i and partial secret key k_i is stored in offline registration phase. In the authentication phase, the randomly generated r_i, as well as the temporary identity ID_i is generated. Hence, with the published RSU parameter set $\{TS_N, ID_{RSU}, R, Q, Cert\}$, vehicle delivered the authentication request $\langle ID_i, TS_2, \mathscr{R}_i, A_i, \mathscr{Z}_i \rangle$ for RSU verification. Finally, the acknowledgement message $\left\langle TS_3, ID_i^{\dagger}, Cert_i^{\dagger} \right\rangle$ is received and verified. Note that the delivered session key sk_i is stored as well. Hence, the total storage cost for individual vehicle is $32 \times 4 + 256 \times 4 + 160 \times 6 + 24 \times 4 = 2208$ bits. The comparison results with existing VANETs authentication schemes are shown in Table 3. Moreover, the storage cost comparison on RSU side are extracted in Fig. 2. It is obvious that less storage overhead is required in the proposed scheme.

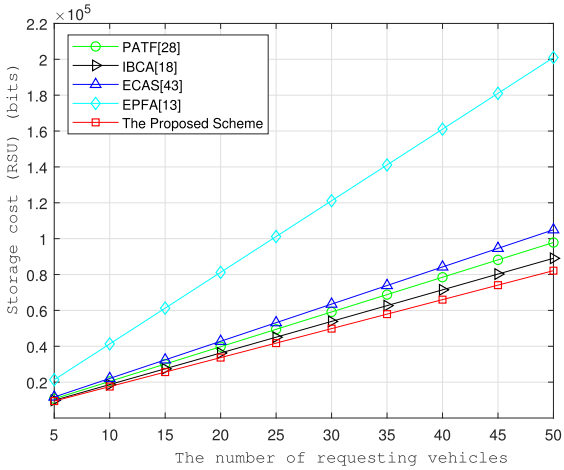


FIGURE 2. Storage cost in RSU side.

B. COMPUTATION COST

In this section, computation cost of the proposed authentication scheme is analyzed. The necessary calculations in RSU and vehicle side for VANETs verification and key distribution are respectively discussed. For better description, the point multiplication and the pairing operation are respectively denoted as p and e. The employed secure hash functions, multiplication, and exponential operation are respectively denoted as H, M, and Ex. The comparison results on computation cost is shown in Table 4, where the approximate execution time is given according to [18]. As described above, bilinear pairing is applied in the proposed design, offering advanced security properties. Note that the complex pairing calculations are all conducted in RSU side. Hence, better security assurance can be provided with less computation overhead for resource limited vehicles, which is of significance to practical VANET scenarios.

Furthermore, in order to demonstrate the effectiveness, the simulation on the proposed authentication scheme are conducted in terms of execution time for V2R authentication process is conducted. The experiments are conducted on Ubuntu 16.04 LTS with a 2.70 GHz Intel(R) Core i7-6820HK CPU and 32GB DDR4 memory. The Pairing-Based Cryptography (PBC) library (pbc-0.5.13) built on the GMP library

TABLE 4. Comparison result of computation cost.

Scheme	PATF [28]	IBCA [18]	ECAS [43]	EPFA [13]	Our Scheme
Computation Cost (RSU)	$3ne{+}2np{+}2nH+2nM$ $\approx (13.5174n)$ ms	$(2n{+}2)p{+}3nM$ $\approx (3.4183n+3.418)$ ms	$(n{+}1)p{+}nH{+}M$ $\approx (1.709n+1.7091)$ ms	$(5n{+}3)p{+}(2n{+}3)H{+}2M$ $\approx (8.5454n+5.1273)$ ms	$2e{+}(2n{+}2)p{+}(2n{+}3)H{+}2nEx{+}(n{+}1)M$ $\approx (1.763n+10.1849)$ ms
Computation Cost (Vehicle)	$4p{+}2H{+}3M$ $\approx (5.5695)$ ms	$3p{+}3H{+}2M$ $\approx (2.4416)$ ms	$4p{+}4H$ $\approx (6.8364)$ ms	$4p{+}5H{+}6M$ $\approx (3.6327)$ ms	$3p{+}3H{+}M$ $\approx (1.8697)$ ms

TABLE 5. Comparison result of communication cost.

Scheme	PATF [28]	IBCA [18]	ECAS [43]	EPFA [13]	Our Scheme
Communication rounds	$4n+1$	$4n+2$	$2n+1$	$2n$	$2n+1$

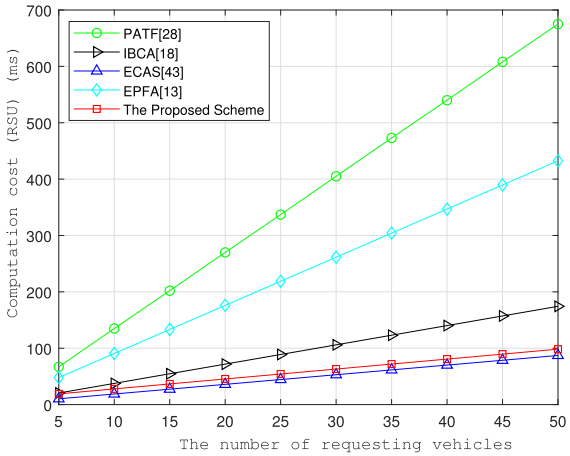


FIGURE 3. Computation cost in RSU side.

(GMP-5.0.5) is implemented for mathematical operations underlying pairing-based crypto-systems. The intuitive comparison result on execution time of RSU side is given in Fig. 3.

C. COMMUNICATION COST

The required communication rounds for VANET authentication in RSU side is discussed in this section, where totally n vehicles are assumed to be successfully verified. Initially, the system parameter set $\{TS_N, ID_{RSU}, R, Q, Cert\}$ is broadcast. Thereafter, authentication request $\langle Request, ID_i, TS_2, \mathscr{R}_i, A_i, \mathscr{Z}_i\rangle$ from n vehicles are distributed. Finally, the acknowledgement message $\left\langle TS_3, ID_i^{\dagger}, Cert_i^{\dagger}\right\rangle$ is delivered to each validated vehicle. In this way, the total communication rounds involving n vehicles is $2n+1$ in total. Accordingly, the comparison result on communication cost is given in Table 5, demonstrating that less communication rounds are required in our scheme comparing with the state-of-the-arts.

VIII. CONCLUSION

Emphasizing on secure data transmission in resource-constrained practical VANET scenarios, enhanced certificateless authentication mechanism is proposed. Novel VANETs model with edge computing infrastructure is adopted, where the RSU clusters collaboratively carries out necessary operations. Based on this, secure authentication design is constructed for V2R data exchange. Note that independent session key for each legitimate vehicle is issued. Moreover, vehicle to vehicle data sharing among neighboring vehicles is taken into consideration. The corresponding V2V group key management scheme is developed in this case. It is worth noting that the consortium blockchain is adopted to the grouping process so that the group management record is maintained by all validated vehicles. Efficient V2V group key distribution process is introduced, where the dynamic key updating design is guaranteed with CRT. Formal security analysis is presented, demonstrating that the proposed scheme can achieve desired security properties and provide resistance to various attacks. The presented performance analysis proves that the proposed scheme is more efficient compared with the state-of-the-arts.

REFERENCES

[1] N.-W. Lo and J.-L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 5, pp. 1319–1328, May 2016.

[2] S.-J. Horng, S.-F. Tzeng, P.-H. Huang, X. Wang, T. Li, and M. K. Khan, "An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," *Inf. Sci.*, vol. 317, pp. 48–66, Oct. 2015.

[3] J. Shen, T. Zhou, X. Liu, and Y.-C. Chang, "A novel latin-square-based secret sharing for M2M communications," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3659–3668, Aug. 2018.

[4] B. Liu, D. Jia, J. Wang, K. Lu, and L. Wu, "Cloud-assisted safety message dissemination in VANET-cellular heterogeneous wireless network," *IEEE Syst. J.*, vol. 11, no. 1, pp. 128–139, Mar. 2017.

[5] C. D. Jung, C. Sur, Y. Park, and K.-H. Rhee, "A robust and efficient anonymous authentication protocol in VANETs," *J. Commun. Netw.*, vol. 11, no. 6, pp. 607–614, Dec. 2009.

[6] H. Tan, D. Choi, P. Kim, S. Pan, and I. Chung, "An efficient hash-based RFID grouping authentication protocol providing missing tags detection," *J. Internet Technol.*, vol. 19, no. 2, pp. 481–488, 2018.

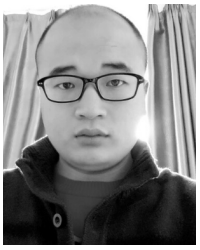
[7] A. A. Khan, M. Abolhasan, and W. Ni, "5G next generation VANETs using SDN and fog computing framework," in *Proc. 15th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2018, pp. 1–6.

[8] A. Ullah, S. Yaqoob, M. Imran, and H. Ning, "Emergency message dissemination schemes based on congestion avoidance in VANET and vehicular FoG computing," *IEEE Access*, vol. 7, pp. 1570–1585, 2019.

[9] Q. Jiang, X. Huang, N. Zhang, K. Zhang, X. Ma, and J. Ma, "Shake to communicate: Secure handshake acceleration-based pairing mechanism for wrist worn devices," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5618–5630, Jun. 2019.

[10] J. Song, C. He, L. Zhang, S. Tang, and H. Zhang, "Toward an RSU-unavailable lightweight certificateless key agreement scheme for VANETs," *China Commun.*, vol. 11, no. 9, pp. 93–103, Sep. 2014.

[11] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. 27th Conf. Comput. Commun. (INFOCOM)*, Apr. 2008, pp. 246–250.
[12] H. Tan, D. Choi, P. Kim, S. Pan, and I. Chung, "Secure certificateless authentication and road message dissemination protocol in VANETs," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–13, 2018.
[13] N. Gayathri, G. Thumbur, P. V. Reddy, and M. Z. Ur Rahman, "Efficient pairing-free certificateless authentication scheme with batch verification for vehicular ad-hoc networks," *IEEE Access*, vol. 6, pp. 31808–31819, 2018.
[14] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preservation in VANETs," *IEEE Access*, vol. 7, pp. 117716–117726, 2019.
[15] R. Madhusudhan, M. Hegde, and I. Memon, "A secure and enhanced elliptic curve cryptography-based dynamic authentication scheme using smart card," *Int. J. Commun. Syst.*, vol. 31, no. 11, p. e3701, Jul. 2018.
[16] T. Gao, X. Deng, Y. Wang, and X. Kong, "PAAS: PMIPv6 access authentication scheme based on identity-based signature in VANETs," *IEEE Access*, vol. 6, pp. 37480–37492, 2018.
[17] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 9, pp. 1227–1239, Sep. 2010.
[18] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.
[19] H. Tan and I. Chung, "Secure authentication and group key distribution scheme for WBANs based on smartphone ECG sensor," *IEEE Access*, vol. 7, pp. 151459–151474, 2019.
[20] J. Molina-Gil, P. Caballero-Gil, and C. Caballero-Gil, "Aggregation and probabilistic verification for data authentication in VANETs," *Inf. Sci.*, vol. 262, pp. 172–189, Mar. 2014.
[21] A. Malip, S.-L. Ng, and Q. Li, "A certificateless anonymous authenticated announcement scheme in vehicular ad hoc networks," *Secur. Commun. Netw.*, vol. 7, no. 3, pp. 588–601, Mar. 2014.
[22] Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen, and S. A. Chaudhry, "Efficient end-to-end authentication protocol for wearable health monitoring systems," *Comput. Electr. Eng.*, vol. 63, pp. 182–195, Oct. 2017.
[23] J. Li, H. Lu, and M. Guizani, "ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 4, pp. 938–948, Apr. 2015.
[24] H. Tan, D. Choi, P. Kim, S. Pan, and I. Chung, "Comments on 'dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks,'" *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2149–2151, Apr. 2018.
[25] X. Zhu, S. Jiang, L. Wang, and H. Li, "Efficient privacy-preserving authentication for vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 63, no. 2, pp. 907–919, Feb. 2014.
[26] M.-C. Chuang and J.-F. Lee, "TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks," *IEEE Syst. J.*, vol. 8, no. 3, pp. 749–758, Sep. 2014.
[27] Y. Ming and X. Shen, "PCPA: A practical certificateless conditional privacy preserving authentication scheme for vehicular ad hoc networks," *Sensors*, vol. 18, no. 5, p. 1573, May 2018.
[28] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on HMAC for VANETs," *IEEE Trans. Intell. Transport. Syst.*, vol. 17, no. 8, pp. 2193–2204, Aug. 2016.
[29] H. Tan and I. Chung, "A secure and efficient group key management protocol with cooperative sensor association in WBANs," *Sensors*, vol. 18, no. 11, p. 3930, Nov. 2018.
[30] C.-C. Lee and Y.-M. Lai, "Toward a secure batch verification with group testing for VANET," *Wireless Netw.*, vol. 19, no. 6, pp. 1441–1449, Aug. 2013.
[31] H. A. Khattak, S. U. Islam, I. U. Din, and M. Guizani, "Integrating fog computing with VANETs: A consumer perspective," *IEEE Commun. Stand. Mag.*, vol. 3, no. 1, pp. 19–25, Mar. 2019.
[32] G. Luo, Q. Yuan, H. Zhou, N. Cheng, Z. Liu, F. Yang, and X. S. Shen, "Cooperative vehicular content distribution in edge computing assisted 5G-VANET," *China Commun.*, vol. 15, no. 7, pp. 1–17, Jul. 2018.
[33] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs," *IEEE Access*, vol. 7, pp. 56656–56666, 2019.
[34] X. Zhang and D. Wang, "Adaptive traffic signal control mechanism for intelligent transportation based on a consortium blockchain," *IEEE Access*, vol. 7, pp. 97281–97295, 2019.
[35] T. A. Butt, R. Iqbal, K. Salah, M. Aloqaily, and Y. Jararweh, "Privacy management in social Internet of vehicles: Review, challenges and blockchain based solutions," *IEEE Access*, vol. 7, pp. 79694–79713, 2019.
[36] H. Tan, Y. Song, S. Xuan, S. Pan, and I. Chung, "Secure D2D group authentication employing smartphone sensor behavior analysis," *Symmetry*, vol. 11, no. 8, p. 969, Aug. 2019.
[37] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, 2018.
[38] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs," *IEEE Trans. Intell. Transport. Syst.*, vol. 18, no. 3, pp. 516–526, Mar. 2017.
[39] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 1, pp. 127–139, Mar. 2012.
[40] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *J. Netw. Comput. Appl.*, vol. 106, pp. 117–123, Mar. 2018.
[41] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*. Berlin, Germany: Springer, 1984, pp. 47–53.
[42] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology*. Berlin, Germany: Springer, 2003, pp. 452–473.
[43] H. Tan, Z. Gui, and I. Chung, "A secure and efficient certificateless authentication scheme with unsupervised anomaly detection in VANETs," *IEEE Access*, vol. 6, pp. 74260–74276, 2018.
[44] S. A. Soleymani, A. H. Abdullah, M. Zareei, M. H. Anisi, C. Vargas-Rosales, M. K. Khan, and S. Goudarzi, "A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing," *IEEE Access*, vol. 5, pp. 15619–15629, 2017.
[45] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. 84, no. 5, pp. 1234–1243, 2001.
[46] I. Memon, I. Hussain, R. Akhtar, and G. Chen, "Enhanced privacy and authentication: an efficient and secure anonymous communication for location based service using asymmetric cryptography scheme," *Wireless Pers. Commun.*, vol. 84, no. 2, pp. 1487–1508, Sep. 2015.
[47] J. Carter and M. N. Wegman, "Universal classes of hash functions," *J. Comput. Syst. Sci.*, vol. 18, no. 2, pp. 143–154, Apr. 1979.
[48] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *J. Cryptol.*, vol. 13, no. 3, pp. 361–396, Jun. 2000.



HAOWEN TAN received the B.E. and M.E. degrees in computer science from the Nanjing University of Information Science and Technology, Nanjing, China, in 2013 and 2016, respectively. He is currently pursuing the Ph.D. degree with the Department of Computer Engineering, Chosun University, Gwangju, South Korea. His research interests include information security, wireless body area networks, radio frequency identification, and vehicular ad-hoc networks.

ILYONG CHUNG received the B.E. degree from Hanyang University, Seoul, South Korea, in 1983, and the M.S. and Ph.D. degrees in computer science from The City University of New York, in 1987 and 1991, respectively. From 1991 to 1994, he was a Senior Technical Staff of the Electronic and Telecommunication Research Institute (ETRI), Dajeon, South Korea. Since 1994, he has been a Professor with the Department of Computer Science, Chosun University, Gwangju, South Korea. His research interests include computer networking, security systems, and coding theory.