February 2020
Doctoral Degree Thesis

Secure Authentication and Key Establishment Scheme with Consortium Blockchain in VANETs

Graduate School of Chosun University

Department of Computer Engineering

Haowen Tan

Secure Authentication and Key Establishment Scheme with Consortium Blockchain in VANETs

VANET 에서 컨소시엄 블록체인을 적용한
안전한 인증 및 키 관리 방식

February 25, 2020

Graduate School of Chosun University

Department of Computer Engineering

Haowen Tan

Secure Authentication and Key Establishment Scheme with Consortium Blockchain in VANETs

Advisor: Prof. Chung, Ilyong

A thesis submitted in partial fulfillment of the requirements for a Doctoral degree

October 2019

Graduate School of Chosun University

Department of Computer Engineering

Haowen Tan

HAOWEN TAN 의 박사학위논문을

인준함

위원장	조선대학교	교 수	모 상 만	(인)
위 원	전남대학교	교 수	김 영 철	(인)
위 원	조선대학교	교 수	신 석 주	(인)
위 원	조선대학교	교 수	강 문 수	(인)
위 원	조선대학교	교 수	정 일 용	(인)

2019 년 12 월

조선대학교 대학원

TABLE OF CONTENTS

LIST OF NOTATIONS iv

LIST OF FIGURES v

LIST OF TABLES v

한 글 요 약 vi

ABSTRACT viii

I. INTRODUCTION 1

A. Motivations 1

1. VANET Architecture 1

2. V2V and V2R Secure Transmission 3

3. Key Management in VANETs 4

4. Cloud Computing and Blockchain in VANETs 5

B. Contributions 6

C. Thesis Layout 7

II. AUTHENTICATION AND KEY MANAGEMENT 9

A. VANETs Authentication Mechanism 9

B. ID-PKC 10

C. CL-PKC 11

D. Cloud Computing in VANETs 12

E. Blockchain Technique in VANETs 13

III. DEFINITIONS AND PRELIMINARIES 15

A. Elliptic Curve Cryptosystem (ECC) 15
B. Bilinear Pairing 15
C. Hash Function 17
D. Chinese Remainder Theorem (CRT) 17
E. System Model 18
F. Network Assumptions 20

IV. PROPOSED V2R AUTHENTICATION SCHEME 22
A. Offline Registration Phase 22
B. Authentication Phase 24

V. PROPOSED V2V GROUP KEY MANAGEMENT SCHEME 34
A. V2V Group Construction Employing CRT 35
B. Dynamic Key Updating with Consortium Blockchain 37

VI. SECURITY ANALYSIS 40
A. Unforgeability Against Chosen Message Attack 40
B. Resistance to Replay Attack 45
C. Conditional Identity Privacy Preserving 46
D. Session Key Establishment 47
E. Certificateless Authentication 48
F. Comparison on Security Properties 49

VII. PERFORMANCE ANALYSIS 50
A. Storage Overhead 50
B. Computation Cost 52
C. Communication Cost 53

VIII. CONCLUSION **54**

REFERENCES **55**

PUBLICATIONS **61**

A. Journal 61

B. Conference 62

ACKNOWLEDGEMENTS **63**

LIST OF NOTATIONS

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 Communications
$\{\partial_i\}_{i\in[0,m]}$	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

LIST OF FIGURES

1 System Model 18

LIST OF TABLES

1 Comparison Result of Security Properties 49
2 Comparison Result of Storage Overhead 51
3 Comparison Result of Computation Cost 52
4 Comparison Result of Communication Cost 53

한 글 요 약

VANET에서 컨소시엄 블록체인을 적용한 안전한 인증 및 키 관리 방식

하오원 탄
지도교수: 정일용
컴퓨터공학과
조선대학교 대학원

오늘날 차량 텔레매틱스와 커뮤니케이션 기술의 빠른 발전과 함께 VANET (Vehicular Ad Hoc Network)의 확산은 괄목할 정도이고 이는 유망한 지능형 운송 시스템 (ITS)의 설계를 기능하게 하였다. 개방형 환경에서 고유한 무선 통신 기능으로 인해 수많은 VANET 엔티티간의 안전한 전송은 심각한 문제로 남아 있다. 현재 많은 연구가 이루어졌지만 대부분은 검증된 장치에 차량 대 차량 (V2V) 및 차량 대 RSU (V2R) 통신을 위한 범용 그룹 키를 할당하고 있다.

그러나 동일한 차량 그룹에 있는 많은 장치를 가진 이기종 VANET 환경에서는 복잡하고 가변적인 토폴로지는 매 순간 연속적인 키 업데이트로 진행되고 이는 V2R 데이터에 간섭을 야기하고 자원이 제한된 VANET 환경에서 신뢰할 수 없고 효율적이지도 않다. 또한, 더 이상 연구가 진행되지 않는 그룹 멤버쉽 기록 및 감지 메커니즘은 실시간 차량 해지 및 참여를 위해 필요하다. 본 논문에서는 안전한 인증 및 키 관리 체계를 제안하면서 위의 문제를 해결한다.

제안된 엣지 컴퓨팅 인프라를 갖춘 새로운 VANET 시스템 모델은 전통적인 VANET 구조와 비교하여 적합한 컴퓨팅 및 저장 용량을 제공하기 위해 채택된다. 서명서 없는 인증 방식은 간섭 회피를 위해 각 차량에 대해 독립적 인

세션 키를 적용하고 더 나아가 컨소시엄 블록 체인은 V2V 그룹 키 설계에 사용된다. 효율적인 그룹 키 업데이트을 통한 실시간 그룹 멤버십 배열이 제공된다. 공식적으로 보안성을 증명하고, 제안된 방식이 원하는 보안 속성을 달성할 수 있음을 보여준다. 성능 분석을 제시함으로써 본 논문에서 제안한 방식이 최신 기술과 비교해서도 우수함을 증명하였다.

ABSTRACT

Secure Authentication and Key Establishment Scheme with Consortium Blockchain in VANETs

Haowen Tan
Advisor: Prof. Chung, Ilyong, Ph.D.
Department of Computer Engineering
Graduate School of Chosun University

Nowadays, with the rapid advancements of vehicular telematics and communication techniques, proliferation of vehicular ad hoc networks (VANETs) has been witnessed, which facilitates the construction of promising intelligent transportation systems (ITSs). Due to inherent wireless communicating characteristics in open environment, secure transmission among numerous VANET entities remains a crucial issue. Currently, lots of research efforts have been made, while most of which tend to allocate a universal group key to the verified devices for vehicle-to-vehicle (V2V) and vehicle-to-RSU (V2R) communications.

However, in heterogeneous VANET environment with a large number of devices of the same vehicular group, complicated and variable topologies lead to continuous key updating in every moment, causing interference to regular V2R data exchange, which is neither reliable nor 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 thesis, 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 to each vehicle for interference avoidance. Furthermore, consortium blockchain is employed for V2V group key construction. Real time group membership arrangement with efficient 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 more efficient compared with the state-of-the-arts.

I. INTRODUCTION

A. Motivations

1. VANET Architecture

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]. With its foreseen benefits and prosperous future, ITS is capable of offering innovative services and applications involving various modes of transport and traffic management, which is especially important for metropolitan cities and areas with blossoming population.

Accordingly, emerging as the fundamental infrastructure of ITS, the vehicular ad hoc network (VANET) 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]. Currently, a variety of VANET-driven applications and services have been developed. In this way, the relevant VANET safety-related functionalities, such as vehicular safety monitoring, traffic congestion avoidance, localization service, are delivered to terminal vehicles so as to provide road safety. Meanwhile, the corresponding commercial-oriented applications, such as weather forecast, surrounding information and navigation, are performed for better driving experience.

Typically, a basic VANET architecture is composed of three essential components: *trusted authority (TA)*, *road-side units (RSUs)* and *vehicles*. TA performs as the topmost service provider and trustworthy central 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 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, which results in tremendous computation and storage burden [5]. Nowadays, sophisticated communicating and processing techniques, including the promising 5G networking and cloud computing, have been dedicated to heterogeneous IoT environment including VANETs, where sufficient computing and storing ability can be guaranteed [6], [7]. Moreover, the integrated cloud server could organize 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 side at fixed intervals [8]. In order to deliver services to targeted vehicles, the effective range of the fixed RSUs is supposed to cover the whole road sections. Each RSU is responsible for direct communication with vehicles in its vicinity. Note that the vehicles can only access the VANET through seamless interactions with the nearby RSU [9]. In this case, RSUs are considered as the important communicating bridge between massive vehicles and central server. Particularly, RSU is capable of conducting necessary keying computation and storing essential data in its storage. Therefore, timely VANET applications and services can be provided to legitimate vehicles at any moment.

As the fundamental entities of VANETs, vehicle performs as both the

terminal user and major vehicular information collector. Massive heterogenous vehicular data and real-time road characteristics such as traffic congestion and accident report, are collaboratively acquired by vehicles [10]. The aggregated data are subsequently uploaded to VANET central server for further analysis and managements. Meanwhile, related VANET services and applications are forwarded to certain vehicles, which drastically enhances the driving safety. Technically, each vehicle is equipped with on-board unit (OBU) [11], in which the wireless communicating module including transceiver and transponder are implemented. The OBU of vehicle is supposed to handle all the message transmission and reception in high-mobility environment.

2. V2V and V2R Secure Transmission

In VANETs, interactions between vehicles can be guaranteed through vehicle to vehicle (V2V) communications [12]. Therefore, self-organized wireless vehicular networks involving multiple vehicles of certain vicinity can be constructed in this way, offering opportunities for real-time vehicular data exchange and aggregation. Meanwhile, communication between each vehicle and the surrounding RSU can be achieved by means of vehicle to RSU (V2R) communication [13]. Note that both V2V and V2R communications employ dedicated short-range communication (DSRC) technique designed for reliable automotive use in ITS. Accordingly, the integrated VANET framework with high connectivity and dynamic topology is built [14].

In practical VANET scenarios, the vital data exchange of V2V and V2R connections are conducted in open wireless environment, resulting in severe vulnerability to various security threats and privacy risks [15]. For example,

the transmitted vehicular information may be eavesdropped or forged so that the significant keying information and user secrets may be illegally revealed to adversaries. Under this circumstance, it is necessary to deploy effective mechanisms for VANET security preservation and privacy protection.

3. Key Management in VANETs

Nowadays, relevant researches on secure VANET transmission have attracted lots of attention from both academia and industry [16]–[18]. Many schemes with different safety strategies and cryptographic techniques have been adopted, where mutual authentication for vehicles and RSUs are conducted, followed by the session key distributing process towards verified vehicles. In this case, each RSU is designed to issue the shared group key to vehicles of its vicinity. Hence, the universal group communication channel for both V2V and V2R communications is built [18]. That is, the data sharing among neighboring vehicles, and the sensitive vehicular data transmission from each vehicle to central server, are all conducted through this group channel. However, due to intrinsic high mobility characteristic of vehicles, the allocated group key may be updated in every moment, resulting in severe inferences to regular V2R data exchange [19].

As for data sharing for V2V group communications, due to the dynamic topologies of vehicular group, timely and efficient key updating method should be provided [20], [21]. To be concrete, when some vehicles are revoked or compromised, the current group key cannot be used in subsequent transmission [22]. Meanwhile, the updated group key should be delivered to the newly joined vehicles as well. To achieve this, VANETs should be aware of

the accurate group information of every moment. The existing VANET security mechanisms mainly focus on authentication and efficient key management [23], while the corresponding group membership monitoring has not been further studied. Furthermore, in V2V group communications, valid and consistent vehicle record in vehicle side is of great significance for targeted transmission with particular entities [24].

4. Cloud Computing and Blockchain in VANETs

Nowadays, the remarkable progress in cloud computing techniques brings new paradigms for massive data processing in VANETs [8], [25]. The uploaded heterogeneous vehicular data can be analyzed and stored in cloud server, which provides adequate computation ability and storage. Meanwhile, the edge computing architecture can be deployed so as to satisfy the low latency requirement of V2R transmission [26]. That is, the nearby RSUs are mutually combined and perform as the local vehicular edge cluster, where the frequently used data can be cached in this edge layer instead of requesting from remote cloud server every time. In this case, the RSU clusters could assist the central server to execute lightweight computing tasks, which significantly alleviates the bandwidth burden for data center.

The studies on blockchain technology have attracted extensive attention so far [27], [28]. 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: public blockchains, private blockchains, hybrid blockchains, and consortium blockchains, all of which have been applied to diverse communicating

circumstances [29]. Specially, the consortium blockchain is able to allocate the pre-selected user group and establish decentralized paradigms for collaborative data sharing, thus has great potential for V2V group communicating deployment. In this way, the commonly shared record on group membership can be dynamically managed by all the legitimate vehicles. Accordingly, the historical communicating record can be validated and traced, which is helpful for conditional privacy preserving [11]. Moreover, effective key updating mechanism involving all the current legitimate vehicles is achievable [30], [31].

In this thesis, with the purpose of offering advanced security properties for VANET transmission, V2R mutual authentication design is developed. Specifically, the cloud-assisted VANET infrastructure with edge computing layer is deployed, which facilitates sufficient computing and storing ability compared to traditional VANET 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 recording. Moreover, efficient group key updating mechanism is designed, which satisfies practical requirements for resource-limited VANET occasions.

B. Contributions

In this thesis, we develop a secure authentication and key establishment scheme with consortium blockchain for dynamic key updating in VANETs. Our nontrivial contributions can be briefly summarized as follows:

- *Certificateless authentication scheme for cloud-assisted VANETs with edge computing infrastructure:* Our design adopts novel VANET infrastructure with edge computing for efficient V2R transmission. The heterogenous

vehicular data are to be processed and stored in remote 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 of identity-based encryption.

- *Efficient group key distribution deploying consortium blockchain:* In the proposed scheme, vehicular group channel involving individual RSU and its 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 affiliated to same group, which facilitates accurate group management in distributed way.

- *Dynamic group key updating strategies for V2V vehicular group:* Reliable group key updating mechanism is designed, where the Chinese remainder theorem is applied. The updating process requires comparatively small computation overhead in vehicle side, which satisfies the practical requirements for resource-limited VANET occasions. Additionally, considering of the resource limitation, complex pairing calculations are executed in RSU and TA side, while relatively lightweight tasks during authentication and key management are conducted in vehicle side.

C. Thesis Layout

The thesis is organized as follows. Chapter II briefly introduces the related research progress. Chapter III illustrates the necessary preliminary work and the

designed ystem model in order for the reader to obtain a better understanding of this topic. Chapter IV presents the proposed V2R certificateless authentication and key management scheme in detail. Chapter V describes V2V group key management scheme. Chapter VI demonstrates the formal security analysis on significant security properties. Chapter VII displays the performance analysis. Finally, the conclusion is drawn in Chapter VIII.

II. AUTHENTICATION AND KEY MANAGEMENT

A. VANETs Authentication Mechanism

In recent years, the topic on VANET secure authentication and key management has been widely investigated.

In 2012, emphasizing on user privacy preservation and key updating efficiency, Lu *et al.* [32] proposed the dynamic key management scheme for location-based services (LBSs). The LBS session is divided into various time slots with different session keys. The new session key can be autonomously updated, where forward secrecy and backward secrecy can be achieved. Subsequently, an efficient cooperative authentication scheme for verifying massive messages in VANETs is presented in [8]. By eliminating redundant authenticating operations for individual vehicles, the verification delay is drastically reduced. Moreover, the whole authentication process is conducted with the evidence token for workload management, offering resistance to multiple security risks.

At the same time, a vehicular data authenticating mechanism is described in [16], 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 [20]. Cooperative message authentication is enabled, which dramatically alleviates the computation burden. Similarly, Chuang *et al.* [21] developed a decentralized trust-extended authentication mechanism (TEAM) for decentralized V2V communications.

Note that the transitive trust relationships frame is applied in order to improve the authenticating efficiency.

Thereafter, Wang *et al.* [33] proposed a two-factor lightweight VANET authenticating schemes 2FLIP, which adopts the decentralized certificate authority (CA) and biological password. By applying hash function and message authentication code (MAC) for V2V communications, computation cost of message signing and verifying process is significantly reduced. Moreover, Zhang *et al.* [31] developed the one-time identity-based aggregate signature with multiple trusted authority (MTA-BTIBAS) and further constructed the distributed VANET authentication scheme. Accordingly, each vehicle is capable of verifying multiple messages simultaneously with compressed signatures. Recently, multiple authentication schemes have been developed [3], which emphasizes on lightweight VANET verification and privacy preserving.

B. ID-PKC

Identity-based public key cryptography (ID-PKC) [34] has been widely applied for secure certificate management in VANETs.

Zhang *et al.* [10] proposed the batch signature verification scheme for V2R communication. Individual RSU is able to process multiple received signatures from different vehicles so that the total time consumption can be drastically decreased. Conditional privacy preservation authentication (CPPA) for participating vehicles is achieved as well, where TA is able to retrieve the real identity of any vehicle. Nevertheless, this scheme is vulnerable to replay attack [24].

Meanwhile, Jung *et al.* [5] developed the universal re-encryption scheme

with identity-based key establishment, where anonymous certificate for specific vehicle is issued by neighboring RSU. In this way, unlinkability and traceability can be provided. Subsequently, the VANET authentication framework with preservation and repudiation (ACPN) is presented [19]. In their design, self-generated PKC-based pseudo identities are applied.

Subsequently, He *et al.* [15] developed an efficient identity-based CPPA scheme for VANETs. Note that bilinear pairing operations are not used, leading to comparatively low computation cost. Similarly, another two CPPA schemes for VANETs are respectively developed [1], [14]. Furthermore, Gao *et al.* [13] developed the message authentication scheme for PMIPv6 in VANETs (PAAS), where mutual authentication is achieved with hierarchical identity-based signature.

C. CL-PKC

With the purposed of addressing the key escrow problem of ID-PKC, certificateless public key cryptography (CL-PKC) was introduced [35]. In CL-PKC, the partial private keys for specific user 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.* [17] developed a privacy preserving authentication protocol based on certificateless signature and reputation systems. Thereafter, Song *et al.* [9] proposed a lightweight VANET certificateless key agreement scheme without pairing. Note that the proposed scheme can be deployed for secure V2V communications without available RSU. The allocated ephemeral key pairs are used in one certain key exchange.

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. The proposed scheme can achieve conditional privacy and is resistant to multiple security attacks. Thereafter, Tan *et al.* [36] constructed the certificateless authentication scheme with anomaly detection strategy. Hence, redundant computation for authentication can be drastically alleviated. Additionally, efficient group key management method is designed as well, providing fast key updating for legitimate vehicles.

Meanwhile, Cui *et al.* [18] proposed an efficient certificateless aggregate signature based on elliptic curve cryptosystem (ECC), which achieves optimized performance in practical VANET scenarios with large numbers of vehicles. After that, several VANET authentication schemes with CL-PKC are developed recently [11], [22].

D. Cloud Computing in VANETs

As mentioned above, with conspicuous advantages in massive data processing and storing, emerging cloud computing technique has been extensively exploited in various VANET applications.

The integrated fog computing infrastructure with VANETs is clarified by Khattak *et al.* in [25], which facilitates heterogeneous data interaction, lower latency, and location-aware service provision. In 2017, Soleymani *et al.* [37] constructed a fuzzy VANET trust model based on experience and plausibility. Note that location-based traffic event evaluation is conducted by the utilized fog nodes near the terminal users. Data uncertainty and imprecision can be avoided

in this way. Meanwhile, the safety message dissemination in VANETs has been investigated in [4], where the particular gateway combing both cellular network and VANET is able to deliver safety messages from cloud server to neighboring vehicles through V2V communications.

Subsequently, Khan *et al.* [6] proposed a hierarchical 5G-based VANET framework, which integrates centralized software defined networks (SDN) and cloud radio access network (C-RAN). The allocated fog computing clusters in edge layer is able to offer minimized delayed and overhead. Similarly, another vehicular content distribution scheme with edge computing for 5G-VANETs is presented [26]. The legitimate vehicles are responsible for handling content requests from neighboring devices, causing less communication burden for the vehicular networks. The proposed multiple-factor prefetching scheme could satisfy the practical requirements on dynamic topology changes. Thereafter, another vehicular message dissemination scheme is proposed by Ullah *et al.* [7], where message congestion avoidance is provided.

E. Blockchain Technique in VANETs

The development of blockchain techniques facilitates decentralized trust management in VANETs. The relevant privacy-preserving VANET trust model is proposed in [30]. 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) [29]. As for SDN-enabled 5G-VANETs in promising ITS environment, decentralized blockchain framework [27] 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.

Moerover, a traceable Internet of vehicle (IoV) system model is constructed [12]. The vehicle transparency and announcement are conducted by the adopted blockchain design. Conditional privacy is achieved as well. As one of the important paradigms, 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 [28]. 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. DEFINITIONS AND PRELIMINARIES

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

A. Elliptic Curve Cryptosystem (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 this curve is defined as point doubling when the two points are identical. Otherwise, it is defined as point addition. All the points on the curve $E_p(a,b)$, 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 mapping function $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ 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 defined as the identity element of $\mathbb{G}_2$.

3. *Computability:* $\forall P,Q \in \mathbb{G}_1$, there exists 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 [38] on the supersingular elliptic curve $\mathbb{G}_1$, where the following characteristics are presented.

Definition 1 (Computational Diffie-Hellman Problem)**.** *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 for any probabilistic polynomial-time (PPT) algorithm $\mathscr{A}$ in computing abP so as to solve the CDHP problem is negligible, which can be defined as:*

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

Definition 2 (Elliptic Curve Discrete Logarithm Problem)**.** *Given $P,Q \in \mathbb{G}_1$, where $Q = aP$. The advantage for any probabilistic polynomial-time (PPT) algorithm $\mathscr{A}$ in finding the integer $a \in \mathbb{Z}_q^*$ so as to solve the ECDLP problem is negligible, which can be defined as:*

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

C. Hash Function

A one-way hash function $h(\cdot)$ is defined to be secure if the following three properties can be achieved all [39]:

1. Input a message x of arbitrary length, it is easy to compute the 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

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

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

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

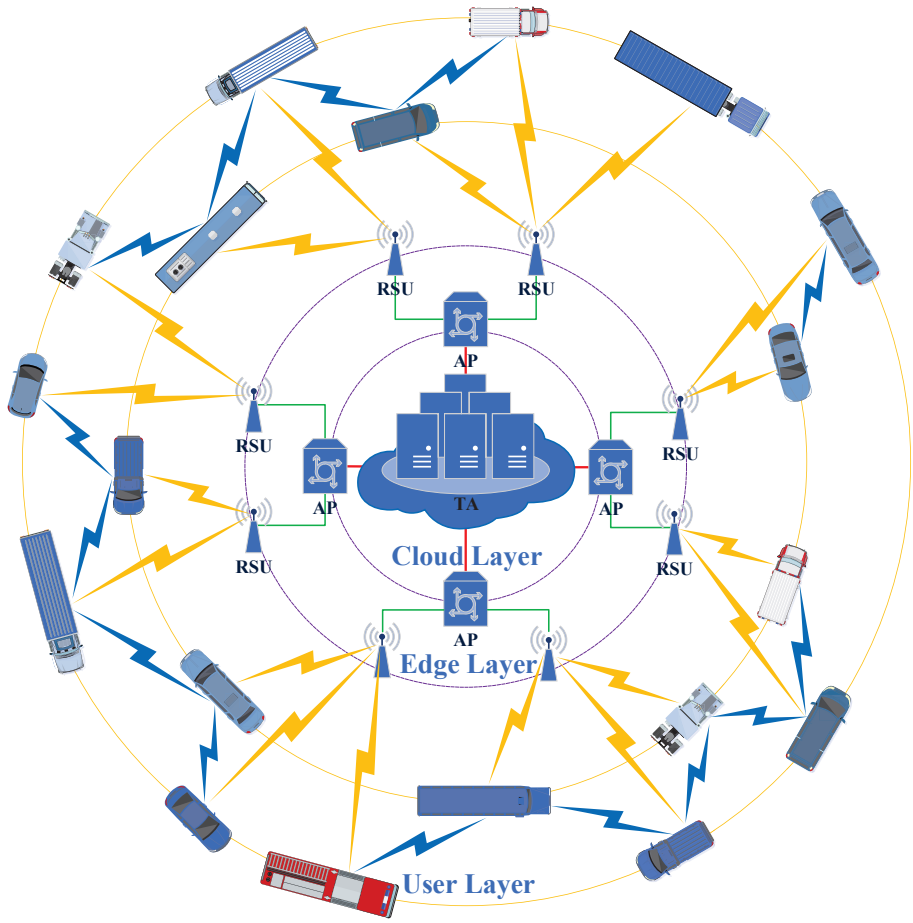

Figure 1: System Model

E. System Model

In our design, the novel VANET system model employing cloud server and edge computing infrastructure is constructed. As shown in Fig. 1, the entire VANET system model consists of three different layers with distinctive functionalities: *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 entire VANET 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 TA is assumed to be valid and trustworthy anytime. With full authority, TA handles vital VANET 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 these RSUs may be compromised or disabled. In this way, for privacy preserving consideration, the crucial vehicles secret information, along with the specific vehicle identity message, should not be fully controlled by RSUs.

User layer is composed of the vehicle networks built with V2V and

V2R communications. The on-board units (OBUs) with wireless communicating 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 vehicle side. Therefore, lightweight authentication mechanism with comparatively limited computation and communication overhead is of great significance for VANETs.

F. Network 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 remote RSUs may be physically compromised since they are far away from the cloud server, which causes 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. Moreover, in our system model, adequate cryptographic and security strategies could be implemented for TA-to-RSU data exchange. Hence, the TA-to-RSU communication is not taken into consideration in our design.

Generally, two types of VANET wireless communication are executed,

which includes vehicle to vehicle (V2V) communications and vehicle to RSU (V2R) communications. The vehicular data acquisition and feedback between specific vehicle and RSU are through V2R communications, while the distributed data sharing among nearby vehicles are conducted in V2V communication channel. Note that both V2V and V2R communications exploit the dedicated short-range communications (DSRC) techniques, where the transmitted data may be easily monitored, altered and forged. Hence, due to the intrinsic wireless transmission characteristics in open environment, both V2V and V2R communications 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 VANET 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 RSU 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 are conducted as well, which is mandatory for all the VANET devices. In this way, significant private information including the fundamental vehicle identity and initial secret key are securely stored in TA side.

A. Offline Registration Phase

Initially, the offline registration phase is designed for VANET initialization and vehicle registration, which are 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, mapping function $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is defined as a bilinear pairing. The secure cryptographic hash functions including $H_1, H_2, H_3, H_4, h_1, h_2$ are respectively defined 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 $param = \{\mathbb{G}_1, \mathbb{G}_2, \hat{e}, q, P, H_1, H_2, H_3, H_4, h_1, h_2\}$ is published.

Preliminarily, TA assigns the unique identity $ID_T \in \{0,1\}^*$ to each validated RSU, which is well preserved in both 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 in 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

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

to RSU for further verification.

Upon receipt of the requesting message, RSU checks 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 $\left\langle ID_V^i, k_i \right\rangle$ 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, and the $\langle \mathscr{Z}_i, A_i, \mathscr{R}_i \rangle$ derived from vehicle request, are all 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 derive

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

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:

$$\begin{aligned}
&L.H.S. \\
&= \frac{\hat{e}\left(\mathscr{Z}_i, P\right)}{\hat{e}\left(h_2\left(ID_{RSU}, r_{RSU}\right)P, A_i\mathscr{R}_i\right)^{s_{RSU}}\aleph_i}
\end{aligned}$$

$$= \frac{\hat{e}\left(A_i r_i Q, P\right)\hat{e}\left(A_i k_i H_3\left(ID_i, TS_2, k_i P\right)R, P\right)\hat{e}\left(H_4\left(r_i k_i P\right)P, P\right)}{\hat{e}\left(h_2\left(ID_{RSU}, r_{RSU}\right)P, A_i \mathscr{R}_i\right)^{s_{RSU}}\aleph_i}$$

$$= \frac{\hat{e}\left(A_i r_i Q, P\right)\hat{e}\left(A_i k_i H_3\left(ID_i, TS_2, k_i P\right)R, P\right)\hat{e}\left(H_4\left(r_i k_i P\right)P, P\right)}{\hat{e}\left(h_2\left(ID_{RSU}, r_{RSU}\right)P, A_i r_i P\right)^{s_{RSU}}\aleph_i}$$

$$= \frac{\hat{e}\left(A_i r_i Q, P\right)\hat{e}\left(A_i k_i H_3\left(ID_i, TS_2, k_i P\right)R, P\right)\hat{e}\left(H_4\left(r_i k_i P\right)P, P\right)}{\hat{e}\left(A_i r_i h_2\left(ID_{RSU}, r_{RSU}\right)P, P\right)^{s_{RSU}}\aleph_i}$$

$$= \frac{\hat{e}\left(A_i r_i Q, P\right)\hat{e}\left(A_i k_i H_3\left(ID_i, TS_2, k_i P\right)R, P\right)\hat{e}\left(H_4\left(r_i k_i P\right)P, P\right)}{\hat{e}\left(A_i r_i \left[s_{RSU} h_2\left(ID_{RSU}, r_{RSU}\right)P\right], P\right)\aleph_i}$$

$$= \frac{\hat{e}\left(A_i r_i Q, P\right)\hat{e}\left(A_i k_i H_3\left(ID_i, TS_2, k_i P\right)R, P\right)\hat{e}\left(H_4\left(r_i k_i P\right)P, P\right)}{\hat{e}\left(A_i r_i Q, P\right)\aleph_i}$$

$$= \frac{\hat{e}\left(A_i k_i H_3\left(ID_i, TS_2, k_i P\right)R, P\right)\hat{e}\left(H_4\left(r_i k_i P\right)P, P\right)}{\aleph_i}$$

$$= \frac{\hat{e}\left(A_i k_i H_3\left(ID_i, TS_2, k_i P\right)R, P\right)\hat{e}\left(H_4\left(r_i k_i P\right)P, P\right)}{\hat{e}\left(H_4\left(k_i \mathscr{R}_i\right)P, P\right)}$$

$$= \frac{\hat{e}\left(A_i k_i H_3\left(ID_i, TS_2, k_i P\right)R, P\right)\hat{e}\left(H_4\left(r_i k_i P\right)P, P\right)}{\hat{e}\left(H_4\left(k_i r_i P\right)P, P\right)}$$

$$= \hat{e}\left(A_i k_i H_3\left(ID_i, TS_2, k_i P\right)R, P\right)$$

$$= \hat{e}\left(H_2\left(ID_i, ID_{RSU}, TS_2, \mathscr{R}_i\right) k_i H_3\left(ID_i, TS_2, k_i P\right) R, P \right)$$
$$= \hat{e}\left(H_2\left(ID_i, ID_{RSU}, TS_2, r_i P\right) k_i H_3\left(ID_i, TS_2, k_i P\right) R, P \right)$$
$$= \hat{e}\left(H_2\left(ID_i, ID_{RSU}, TS_2, r_i P\right) k_i H_3\left(ID_i, TS_2, k_i P\right) r_{RSU} P, P \right). \quad (11)$$

Hence, $L.H.S.$ 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

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

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

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

and distributes the acknowledgement message as

$$\left\langle TS_3, ID_i^{\dagger}, Cert_i^{\dagger} \right\rangle, \quad (14)$$

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

$$ID_i^{\dagger} = h_2\Big(ID_i, H_4\left(r_{RSU}\mathscr{R}_i\right)\Big) = h_2\Big(ID_i, H_4\left(r_i R\right)\Big). \tag{15}$$

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 fully 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 VANET environment involving large numbers of vehicles, individual RSU takes the responsibility for simultaneous authentication towards all the requesting vehicles within 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 as

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

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

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

Due to the previously acquired information $Q = s_{RSU}h_2\left(ID_{RSU}, r_{RSU}\right)P$ 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 follows:

$$
\begin{aligned}
&L.H.S.\\
&= \frac{\hat{e}\left(\sum_{i=1}^{n} \mathscr{Z}_i, P\right)}{\hat{e}\left(h_2\left(ID_{RSU}, r_{RSU}\right)P, \sum_{i=1}^{n} A_i \mathscr{R}_i\right)^{s_{RSU}} \prod_{i=1}^{n} \aleph_i}\\
&= \frac{\hat{e}\left(\sum_{i=1}^{n} A_i r_i Q, P\right)\hat{e}\left(\sum_{i=1}^{n} A_i k_i H_3\left(ID_i, TS_2, k_i P\right)R, P\right)\hat{e}\left(\sum_{i=1}^{n} H_4\left(r_i k_i P\right)P, P\right)}{\hat{e}\left(h_2\left(ID_{RSU}, r_{RSU}\right)P, \sum_{i=1}^{n} A_i \mathscr{R}_i\right)^{s_{RSU}} \prod_{i=1}^{n} \aleph_i}\\
&= \frac{\hat{e}\left(\sum_{i=1}^{n} A_i r_i Q, P\right)\hat{e}\left(\sum_{i=1}^{n} A_i k_i H_3\left(ID_i, TS_2, k_i P\right)R, P\right)\hat{e}\left(\sum_{i=1}^{n} H_4\left(r_i k_i P\right)P, P\right)}{\hat{e}\left(h_2\left(ID_{RSU}, r_{RSU}\right)P, \sum_{i=1}^{n} A_i r_i P\right)^{s_{RSU}} \prod_{i=1}^{n} \aleph_i}\\
&= \frac{\prod_{i=1}^{n}\hat{e}\left(A_i r_i Q, P\right)\hat{e}\left(\sum_{i=1}^{n} A_i k_i H_3\left(ID_i, TS_2, k_i P\right)R, P\right)\hat{e}\left(\sum_{i=1}^{n} H_4\left(r_i k_i P\right)P, P\right)}{\hat{e}\left(h_2\left(ID_{RSU}, r_{RSU}\right)P, \sum_{i=1}^{n} A_i r_i P\right)^{s_{RSU}} \prod_{i=1}^{n} \aleph_i}\\
&= \frac{\prod_{i=1}^{n}\hat{e}\left(A_i r_i Q, P\right)\hat{e}\left(\sum_{i=1}^{n} A_i k_i H_3\left(ID_i, TS_2, k_i P\right)R, P\right)\hat{e}\left(\sum_{i=1}^{n} H_4\left(r_i k_i P\right)P, P\right)}{\hat{e}\left(\sum_{i=1}^{n} A_i r_i \left[s_{RSU} h_2\left(ID_{RSU}, r_{RSU}\right)P\right], P\right)\prod_{i=1}^{n} \aleph_i}\\
&= \frac{\prod_{i=1}^{n}\hat{e}\left(A_i r_i Q, P\right)\hat{e}\left(\sum_{i=1}^{n} A_i k_i H_3\left(ID_i, TS_2, k_i P\right)R, P\right)\hat{e}\left(\sum_{i=1}^{n} H_4\left(r_i k_i P\right)P, P\right)}{\hat{e}\left(\sum_{i=1}^{n} A_i r_i Q, P\right)\prod_{i=1}^{n} \aleph_i}
\end{aligned}
$$

$$
\begin{aligned}
&= \frac{\prod_{i=1}^{n} \hat{e}\left(A_i r_i Q, P\right) \hat{e}\left(\sum_{i=1}^{n} A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\right) \hat{e}\left(\sum_{i=1}^{n} H_4\left(r_i k_i P\right) P, P\right)}{\prod_{i=1}^{n} \hat{e}\left(A_i r_i Q, P\right) \prod_{i=1}^{n} \aleph_i} \\
&= \frac{\hat{e}\left(\sum_{i=1}^{n} A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\right) \hat{e}\left(\sum_{i=1}^{n} H_4\left(r_i k_i P\right) P, P\right)}{\prod_{i=1}^{n} \aleph_i} \\
&= \frac{\hat{e}\left(\sum_{i=1}^{n} A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\right) \prod_{i=1}^{n} \hat{e}\left(H_4\left(r_i k_i P\right) P, P\right)}{\prod_{i=1}^{n} \hat{e}\left(H_4\left(k_i \mathscr{R}_i\right) P, P\right)} \\
&= \frac{\hat{e}\left(\sum_{i=1}^{n} A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\right) \prod_{i=1}^{n} \hat{e}\left(H_4\left(r_i k_i P\right) P, P\right)}{\prod_{i=1}^{n} \hat{e}\left(H_4\left(k_i r_i P\right) P, P\right)} \\
&= \hat{e}\left(\sum_{i=1}^{n} A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\right). \qquad (18)
\end{aligned}
$$

Hence, $L.H.S. = \hat{e}\left(\sum_{i=1}^{n} A_i k_i H_3\left(ID_i, TS_2, k_i P\right) R, P\right)$ in this way. 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

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

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

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 $sk_i = H_4(\aleph_i)$.

V. PROPOSED V2V GROUP KEY MANAGEMENT SCHEME

As one of the major functionalities in VANETs, vehicle to vehicle (V2V) communications facilitate 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 of it range. Therefore, the multi-purpose 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 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 can be 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, the grouping request $\left\langle Request, ID_{RSU}, TS_G, \Phi, Cert_G^{\ddagger} \right\rangle$ is issued 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, $\forall \ell \in [1,m]$, 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 broadcast their identities $ID_i^{\hbar}$ at certain time interval. Hence, each vehicle is aware of identities of all the participating vehicles and then 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 is safely updated. Note that the new vehicle joining 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 [40])**.** *Let $\mathscr{A}$ be a probabilistic polynomial time Turing machine, given only the public information as input. Within a certain time bound $\mathscr{T}$, if $\mathscr{A}$ is able to 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, hence, with an indistinguishable distribution probability, there exists 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 the adversary $\mathscr{A}_1$. 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 $r_ik_iP \in \mathbb{G}$. 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 $\eth_i = H_4(r_i k_i P)$ to $\mathscr{A}_1$.

– Otherwise, $\mathscr{C}_1$ chooses a random $\eth_i \in \mathbb{Z}^*_q$ and forwards it to the adversary $\mathscr{A}_1$. 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 $\langle ID_{RSU}, r_{RSU} \rangle$. 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 $\langle ID_i, TS_2, \mathscr{R}_i, A_i, \mathscr{Z}_i^*, \aleph_i, \Im_i^* \rangle$ after querying $\mathscr{C}_1$, where both tuples can pass the authentication process. Let $h_2 = h_2(ID_{RSU}, r_{RSU})$, $H_3 = H_3(ID_i, TS_2, k_i P)$, $H_4 = H_4(r_i k_i P)$. That is,

$$\begin{cases} \dfrac{\hat{e}\left(\mathscr{Z}_i, P\right)}{\hat{e}\left(h_2 P, A_i \mathscr{R}_i\right)^{s_{RSU}} \hat{e}\left(H_4 P, P\right)} = \hat{e}\left(k_i H_3 P, P\right)^{A_i r_{RSU}} \\ \dfrac{\hat{e}\left(\mathscr{Z}_i^*, P\right)}{\hat{e}\left(h_2 P, A_i \mathscr{R}_i\right)^{s_{RSU}} \hat{e}\left(H_4 P, P\right)} = \hat{e}\left(k_i H_3^* P, P\right)^{A_i r_{RSU}} \end{cases}, \tag{38}$$

which can be formulated into

$$\begin{cases} \left[\dfrac{\hat{e}\left(\mathscr{Z}_i, P\right)}{\hat{e}\left(h_2 P, A_i \mathscr{R}_i\right)^{s_{RSU}} \hat{e}\left(H_4 P, P\right)}\right]^{H_3^*} = \hat{e}\left(k_i H_3 P, P\right)^{A_i H_3^* r_{RSU}} \\ \left[\dfrac{\hat{e}\left(\mathscr{Z}_i^*, P\right)}{\hat{e}\left(h_2 P, A_i \mathscr{R}_i\right)^{s_{RSU}} \hat{e}\left(H_4 P, P\right)}\right]^{H_3} = \hat{e}\left(k_i H_3^* P, P\right)^{A_i H_3 r_{RSU}} \end{cases}. \tag{39}$$

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

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

which is further illustrated as

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

At this point, let $Q = aP$ and $A_i \mathscr{R}_i = bP$ for some $a, b \in \mathbb{Z}_q^*$. Then $\mathscr{C}_1$ is able to

conduct the following calculation:

$$\begin{aligned}
&\frac{\hat{e}\left(H_3^*\mathscr{Z}_i,P\right)}{\hat{e}\left(H_3\mathscr{Z}_i^*,P\right)}\\
&=\frac{\hat{e}\left(s_{RSU}H_3^*h_2P,A_i\mathscr{R}_i\right)\hat{e}\left(H_3^*H_4P,P\right)}{\hat{e}\left(s_{RSU}H_3h_2P,A_i\mathscr{R}_i\right)\hat{e}\left(H_3H_4P,P\right)}\\
&=\hat{e}\left(s_{RSU}H_3^*h_2P-s_{RSU}H_3h_2P,A_i\mathscr{R}_i\right)\hat{e}\left(H_3^*H_4P-H_3H_4P,P\right)\\
&=\hat{e}\left(\left(H_3^*-H_3\right)s_{RSU}h_2P,A_i\mathscr{R}_i\right)\hat{e}\left(\left(H_3^*-H_3\right)H_4P,P\right) \qquad . \qquad (42)\\
&=\hat{e}\left(\left(H_3^*-H_3\right)Q,A_i\mathscr{R}_i\right)\hat{e}\left(\left(H_3^*-H_3\right)H_4P,P\right)\\
&=\hat{e}\left(\left(H_3^*-H_3\right)aP,bP\right)\hat{e}\left(\left(H_3^*-H_3\right)H_4P,P\right)\\
&=\hat{e}\left(\left(H_3^*-H_3\right)abP,P\right)\hat{e}\left(\left(H_3^*-H_3\right)H_4P,P\right)\\
&=\hat{e}\left(\left(H_3^*-H_3\right)\left(abP+H_4P\right),P\right)\\
&=\hat{e}\left(H_3^*\mathscr{Z}_i-H_3\mathscr{Z}_i^*,P\right)
\end{aligned}$$

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

$$H_3^*\mathscr{Z}_i - H_3\mathscr{Z}_i^* = \left(H_3^*-H_3\right)\left(abP+H_4P\right). \qquad (43)$$

Thereafter, $\mathscr{C}_1$ calculates

$$abP = \left(H_3^*\mathscr{Z}_i - H_3\mathscr{Z}_i^*\right)\left(H_3^*-H_3\right)^{-1} - H_4P \qquad (44)$$

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 network attacking types, replay attack is carried out through maliciously reusing the previously acquired information in the current authentication process. The replay attack resistance of the proposed authentication scheme is illustrated as follows.

Theorem 2. *The proposed VANET 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 $\langle Request, ID_i, TS_2^{\mathscr{T}}, \mathscr{R}_i, A_i, \mathscr{Z}_i \rangle$ 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 VANET 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 the entire VANET transmission. 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 $ID_{RSU} = h_1(ID_T, TS_1, r_{RSU})$. It is worth noting that the included r_{RSU} is randomly generated by TA 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 $ID_i = H_2\left(ID_V^i, TS_2, k_i, r_i P\right)$ 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 provision. □

D. Session Key Establishment

In practical VANET scenarios, secure and reliable data interactions in open wireless environment should be guaranteed. Hence, session keys for both V2R and V2V communications 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 communications 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 transmission 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 transmissions. □

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 VANET 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 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

The comparison results in terms of the crucial security properties for VANET communications are presented in this section. The proposed design is compared with the state-of-the-art VANET authentication and key agreement schemes including PATF [23], IBCA [15], ECAS [36], and EPFA [11] with the purpose of demonstrating its superiority on security properties. The comparison results are presented in Table 1, indicating that the proposed scheme satisfies the desired security requirements.

Table 1: Comparison Result of Security Properties

Scheme	**PATF** [23]	**IBCA** [15]	**ECAS** [36]	**EPFA** [11]	**Our Scheme**
Unforgeability	√	√	√	√	√
Replay Attack Resistance	√	√	√	√	√
Conditional Anonymity	√	√	×	√	√
Session Key Establishment	√	×	√	√	√
Key Escrow Resilience	×	√	√	√	√
Scalability	×	√	×	√	√
Efficient Key Updating	√	×	√	×	√

VII. PERFORMANCE ANALYSIS

In this section, analysis towards performance of the proposed scheme is presented, which specifically emphasizes on the crucial properties for resource-limited VANET 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 communications, 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 [23], IBCA [15], ECAS [36], and EPFA [11] 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 keys $\langle s_{RSU}, r_{RSU} \rangle$ for individual RSU are safely stored. Upon registration, the RSU session identity ID_{RSU} is generated. Subsequently, the calculation on $\{R, Q, Cert\}$ are executed. Accordingly, we define the length of the identity 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 respectively assumed to be 160 bits and 24 bits. 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 are 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 delivers 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 VANET authentication schemes are shown in Table 2. It is obvious that less storage overhead is required in the proposed scheme.

Table 2: Comparison Result of Storage Overhead

Scheme	Storage Cost (RSU)	Storage Cost (Vehicle)
PATF [23]	$1936n + 1048$ bits	3432 bits
IBCA [15]	$1760n + 1056$ bits	2112 bits
ECAS [36]	$2072n + 1344$ bits	2552 bits
EPFA [11]	$3992n + 1376$ bits	4368 bits
Our Scheme	$1616n + 1360$ bits	2208 bits

B. Computation Cost

In this section, computation cost of the proposed authentication scheme is analyzed. The necessary calculation in RSU and vehicle side for VANET verification and key distribution are respectively discussed. For better description, the point multiplication and pairing operation are respectively denoted as p and e. The employed secure hash functions, multiplications, and exponential operations are respectively denoted as H, M, and Ex. The comparison results on computation cost is shown in Table 3, where the approximate execution time is given according to [15]. 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.

Table 3: Comparison Result of Computation Cost

Scheme	Computation Cost (RSU)	Computation Cost (Vehicle)
PATF [23]	$3ne+2np+2nH+2nM$ $\approx (13.5174n)$ ms	$4p+2H+3M$ $\approx (5.5695)$ ms
IBCA [15]	$(2n+2)p+3nM$ $\approx (3.4183n+3.418)$ ms	$3p+3H+2M$ $\approx (2.4416)$ ms
ECAS [36]	$(n+1)p+nH+M$ $\approx (1.709n+1.7091)$ ms	$4p+4H$ $\approx (6.8364)$ ms
EPFA [11]	$(5n+3)p+(2n+3)H+2M$ $\approx (8.5454n+5.1273)$ ms	$4p+5H+6M$ $\approx (3.6327)$ ms
Our Scheme	$2e+(2n+2)p+(2n+3)H+2nEx+(n+1)M$ $\approx (1.763n+10.1849)$ ms	$3p+3H+M$ $\approx (1.8697)$ ms

C. Communication Cost

The required communication rounds for the 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. Subsequently, 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 communication rounds involving n vehicles is $2n+1$ in total. Accordingly, the comparison result of communication cost is given in Table 4, demonstrating that less communication rounds are required in our scheme compared with the state-of-the-arts.

Table 4: Comparison Result of Communication Cost

Scheme	**PATF** [23]	**IBCA** [15]	**ECAS** [36]	**EPFA** [11]	**Our Scheme**
Communication rounds	$4n+1$	$4n+2$	$2n+1$	$2n$	$2n+1$

VIII. CONCLUSION

Emphasizing on secure data transmission in resource-constrained practical VANET scenarios, enhanced certificateless authentication mechanism is proposed.

- Novel VANET model with edge computing infrastructure is adopted, where the RSU cluster collaboratively carries out necessary operations. Secure authentication design is constructed for V2R data exchange. Note that the independent session key for each legitimate vehicle is issued.

- Vehicle to vehicle data sharing among neighboring vehicles is taken into consideration. The corresponding V2V group key management scheme is developed in this case.

- Consortium blockchain is adopted to the grouping process so that the group management record is maintained by all the valid vehicles. Efficient V2V group key distribution process is introduced, where the dynamic key updating designed 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 efficient compared with the state-of-the-arts.

REFERENCES

[1] N. Lo and J. Tsai, "An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks Without Pairings", *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 5, pp. 1319–1328, 2016.

[2] S. Horng, S. Tzeng, P. Huang, X. Wang, T. Li, and M. K. Khan, "An Efficient Certificateless Aggregate Signature with Conditional Privacy-preserving for Vehicular Sensor Networks", *Information Sciences*, vol. 317, pp. 48–66, 2015.

[3] J. Cui, D. Wu, J. Zhang, Y. Xu, and H. Zhong, "An Efficient Authentication Scheme Based on Semi-Trusted Authority in VANETs", *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2972–2986, 2019.

[4] B. Liu, D. Jia, J. Wang, K. Lu, and L. Wu, "Cloud-Assisted Safety Message Dissemination in VANET–Cellular Heterogeneous Wireless Network", *IEEE Systems Journal*, vol. 11, no. 1, pp. 128–139, 2017.

[5] C. D. Jung, C. Sur, Y. Park, and K. Rhee, "A Robust and Efficient Anonymous Authentication Protocol in VANETs", *Journal of Communications and Networks*, vol. 11, no. 6, pp. 607–614, 2009.

[6] A. A. Khan, M. Abolhasan, and W. Ni, "5G next generation VANETs using SDN and fog computing framework", in *2018 15th IEEE Annual Consumer Communications Networking Conference (CCNC)*, 2018, pp. 1–6.

[7] 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.

[8] X. Lin and X. Li, "Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks", *IEEE Transactions on Vehicular Technology*, vol. 62, no. 7, pp. 3339–3348, 2013.

[9] J. Song, C. He, L. Zhang, S. Tang, and H. Zhang, "Toward an RSU-unavailable Lightweight Certificateless Key Agreement Scheme for VANETs", *China Communications*, vol. 11, no. 9, pp. 93–103, 2014.

[10] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks", in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, 2008, pp. 246–250.

[11] N. B. Gayathri, G. Thumbur, P. V. Reddy, and Z. U. R. Muhammad, "Efficient Pairing-Free Certificateless Authentication Scheme With Batch Verification for Vehicular Ad-Hoc Networks", *IEEE Access*, vol. 6, pp. 31 808–31 819, 2018.

[12] 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. 117 716–117 726, 2019.

[13] 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. 37 480–37 492, 2018.

[14] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks", *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 9, pp. 1227–1239, 2010.

[15] D. He, S. Zeadally, B. Xu, and X. Huang, "An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks", *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[16] J. Molina-Gil, P. Caballero-Gil, and C. Caballero-Gil, "Aggregation and Probabilistic Verification for Data Authentication in VANETs", *Information Sciences*, vol. 262, pp. 172–189, 2014.

[17] A. Malip, S. Ng, and Q. Li, "A Certificateless Anonymous Authenticated Announcement Scheme in Vehicular Ad Hoc Networks", *Security and Communication Networks*, vol. 7, no. 3, pp. 588–601, 2014.

[18] J. Cui, J. Zhang, H. Zhong, R. Shi, and Y. Xu, "An Efficient Certificateless Aggregate Signature without Pairings for Vehicular Ad Hoc Networks", *Information Sciences*, vol. 451-452, pp. 1–15, 2018.

[19] J. Li, H. Lu, and M. Guizani, "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs", *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 938–948, 2015.

[20] X. Zhu, S. Jiang, L. Wang, and H. Li, "Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks", *IEEE Transactions on Vehicular Technology*, vol. 63, no. 2, pp. 907–919, 2014.

[21] M. Chuang and J. Lee, "TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks", *IEEE Systems Journal*, vol. 8, no. 3, pp. 749–758, 2014.

[22] 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, 2018.

[23] S. Jiang, X. Zhu, and L. Wang, "An Efficient Anonymous Batch Authentication Scheme Based on HMAC for VANETs", *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 8, pp. 2193–2204, 2016.

[24] C. Lee and Y. Lai, "Toward A Secure Batch Verification with Group Testing for VANET", *Wireless Networks*, vol. 19, no. 6, pp. 1441–1449, 2013.

[25] H. A. Khattak, S. U. Islam, I. U. Din, and M. Guizani, "Integrating Fog Computing with VANETs: A Consumer Perspective", *IEEE Communications Standards Magazine*, vol. 3, no. 1, pp. 19–25, 2019.

[26] 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 Communications*, vol. 15, no. 7, pp. 1–17, 2018.

[27] 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. 56 656–56 666, 2019.

[28] X. Zhang and D. Wang, "Adaptive Traffic Signal Control Mechanism for Intelligent Transportation Based on a Consortium Blockchain", *IEEE Access*, vol. 7, pp. 97 281–97 295, 2019.

[29] 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. 79 694–79 713, 2019.

[30] 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. 45 655–45 664, 2018.

[31] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed Aggregate Privacy-Preserving Authentication in VANETs", *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516–526, 2017.

[32] R. Lu, X. Lin, X. Liang, and X. Shen, "A Dynamic Privacy-Preserving Key Management Scheme for Location-Based Services in VANETs", *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, no. 1, pp. 127–139, 2012.

[33] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, "2FLIP: A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET", *IEEE Transactions on Vehicular Technology*, vol. 65, no. 2, pp. 896–911, 2016.

[34] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes", in *Advances in Cryptology - CRYPTO 1984*, Berlin, Heidelberg: Springer Berlin Heidelberg, 1984, pp. 47–53.

[35] S. S. Al-Riyami and K. G. Paterson, “Certificateless Public Key Cryptography”, in *Advances in Cryptology-ASIACRYPT 2003*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 452–473.

[36] 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. 74 260–74 276, 2018.

[37] 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. 15 619–15 629, 2017.

[38] A. Miyaji, M. Nakabayashi, and S. Takano, “New Explicit Conditions of Elliptic Curve Traces for FR-reduction”, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 84, no. 5, pp. 1234–1243, 2001.

[39] J. L. Carter and M. N. Wegman, “Universal Classes of Hash Functions”, *Journal of Computer and System Sciences*, vol. 18, no. 2, pp. 143–154, 1979.

[40] D. Pointcheval and J. Stern, “Security Arguments for Digital Signatures and Blind Signatures”, *Journal of Cryptology*, vol. 13, no. 3, pp. 361–396, 2000.

PUBLICATIONS

A. Journal

1. H. Tan and I. Chung, "Secure Authentication and Key Management with Blockchain in VANETs", *IEEE Access*, 2019. DOI: 10.1109/ACCESS.2019.2962387.

2. H. Tan and I. Chung, "Secure Authentication and Group Key Distribution Scheme for WBANs Based on Smartphone ECG Sensor", *IEEE Access*, vol. 7, pp. 151 459–151 474, Oct. 2019.

3. 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, pp. 1–20, Aug. 2019.

4. 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 Transactions on Intelligent Transportation Systems*, vol. 19, no. 7, pp. 2149–2151, Jul. 2018.

5. 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. 74 260–74 276, Nov. 2018.

6. H. Tan and I. Chung, "A Secure and Efficient Group Key Management Protocol with Cooperative Sensor Association in WBANs", *Sensors*, vol. 18, no. 11, pp. 1–25, Nov. 2018.

7. H. Tan, D. Choi, P. Kim, S. Pan, and I. Chung, "Secure Certificateless Authentication and Road Message Dissemination Protocol in VANETs", *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1–13, May 2018.

8. H. Tan, D. Choi, P. Kim, S. Pan, and I. Chung, "An Efficient Hash-based RFID Grouping Authentication Protocol Providing Missing Tags Detection", *Journal of Internet Technology*, vol. 19, no. 2, pp. 481–488, Mar. 2018.

B. Conference

1. H. Tan and I. Chung, "A Secure Cloud-Assisted Certificateless Group Authentication Scheme for VANETs in Big Data Environment", in *Proceedings of the 2019 International Conference on Big Data Engineering*, Jun. 2019, pp. 107–113.

ACKNOWLEDGEMENTS

First and foremost, I would like to express my deep and sincere gratitude to my supervisor Prof. Ilyong Chung, for giving me the opportunity to do research and providing invaluable guidance and continuous support throughout my Ph.D study. His patience, vision, dynamism, and sincerity have deeply inspired me. It's a great privilege and honor to work and study under his supervision.

I would like to thank the rest of my thesis committee: Prof. Sangman Moh, Prof. Seokjoo Shin, Prof. Moonsoo Kang, and Prof. Youngchul Kim, for their insightful comments and constructive suggestions, which have helped significantly improve this thesis.

I am extremely grateful to my parents Baizhi Tan and Shixiu Fan, who have provided me with continuous encouragement and unfailing support throughout my years of study and through the process of researching and writing this thesis. I am also grateful to my sibling Jingyuan Tan and other family members who have supported me along the way.

A very special gratitude goes out to my beloved fiancee Yuanzhao Song. This accomplishment would not have been possible without her warm love, constant patience, and endless support. You are the sunshine of my life.

I would also like to express my heartfelt gratitude to Prof. Jian Shen for his genuine support throughout my research work. My sincere thanks also goes to Prof. Youngju Cho, who has always been so helpful and cooperative in giving her support at all times to help me achieve my goal.

Finally, last but not the least, I would like to thank all my fellow labmates. It was great sharing laboratory with all of you during my Ph.D study.