Provable Secure and Lightweight Blockchain-Based V2I Handover Authentication and V2V Broadcast Protocol for VANETs

Qi Xie, Zixuan Ding, Wen Tang, Debiao He, *Member, IEEE*, and Xiao Tan

***Abstract*—As one of the most valuable vehicle-based Internet of Things (IoT) applications, Vehicular Ad-hoc Networks (VANETs) have received extensive attention since it was proposed. In order to ensure the safety of VANETs and improve the communication efficiency between moving vehicles and different Roadside Units (RSUs), some handover authentication protocols for VANETs have been proposed. However, the existing protocols have some problems such as excessive computation overhead, untraceable malicious messages, and the inability to resist RSU captured attacks. To solve the above problems, we propose a blockchain-based protocol to achieve Vehicle to Infrastructure (V2I) authentication, V2I handover authentication, and Vehicle to Vehicle (V2V) broadcasting authentication. The advantages of our protocol are: (1) It achieves lightweight V2I handover authentication and V2V broadcast authentication, dynamic anonymity strategy and embedding strategy of pseudo-identity and vehicle feature are used to guarantee anonymity and traceability simultaneously; (2) The announcement can be broadcasted verifiably without the help of transportation infrastructure (e.g., RSU) or the Trusted Authority (TA); and (3) The Physically Unclonable Functions (PUF) technology is used to resist RSU captured attacks. We use formal security proof under random oracle model to prove the security of the proposed protocol. Compared with related V2I handover authentication protocols, our protocol can resist RSU captured attacks and other various known attacks. The sum of first and handover authentication efficiency of our protocol is 37.93% higher than the previous most effective protocol, while maintaining the same level of communication and storage costs.**

***Index Terms*—Handover authentication, VANETs, blockchain, broadcast authentication, vehicle to infrastructure, vehicle to vehicle.**

I. Introduction

VANETS are the application of IoT technology in the field of transportation, which is based on On-Board Unit (OBU) and wireless communication technology to realize the communication between vehicles and other vehicles or entities. Therefore, VANETs can be divided into V2V, V2I, Vehicle to Network (V2N), and Vehicle to Cloud (V2C) according to the specific application scenarios. Based on VANETs, vehicles can upload road conditions to Roadside Units (RSUs) and network in real-time, or broadcast to other vehicles. The vehicle and other entities exchange and share vehicle status information including vehicle location, driving speed, etc., which can be used to help vehicles dynamically judge the road traffic flow, improve the intelligent driving of vehicles, provide users with safe, comfortable, intelligent, and efficient driving and traffic services, and ameliorate the traffic operation efficiency.

However, almost all communications between vehicles and RSUs are conducted through public channels [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], which provide an opportunity for attackers. For example, an attacker can intercept and modify the transmitted messages, launch forgery attacks and obtain the user's privacy, etc. Vehicles can also release malicious messages to interfere with normal driving. Therefore, it is necessary to design a secure and effective authentication protocol for VANETs to solve the above problems.

In the traditional V2I authentication mode, vehicles needed to be re-authenticated after entering a new RSU domain, but the vehicle cannot be authenticated in the absence of infrastructure. How to achieve reliable V2I handover authentication and V2V authentication without the participation of trusted infrastructure is also an urgent problem to be solved. As an emerging technology, blockchain has the advantages of non-tampering, decentralization, transparency, and self-maintenance. Researchers introduced blockchain as a storage medium into VANETs to assist authentication and achieve efficient V2I handover authentication [13], [14], [15], [16], [19]. However, uploading information on the blockchain for authentication may lead to user's privacy disclosure and impersonation attack. In addition, the V2I handover authentication in the above protocols may be insecure or require exorbitant computation overhead [13], [16]. On the other hand, in some authentication protocols for the VANETs [19], [20], [21], [22], [23], [24], the malicious behavior of legally registered users is difficult to prevent, and the dynamic anonymity strategy increases the difficulty of recovering real identity.

Manuscript received 20 September 2022; revised 26 February 2023; accepted 20 June 2023. Date of publication 26 June 2023; date of current version 19 December 2023. This work was supported in part by the National Natural Science Foundation of China under Grant U21A20466 and in part by the New 20 Project of Higher Education of Jinan under Grant 202228017. The review of this article was coordinated by Dr. Mario Marchese. *(Corresponding author: Qi Xie.)*

Qi Xie, Zixuan Ding, Wen Tang, and Xiao Tan are with the Key Laboratory of Cryptography of Zhejiang Province, Hangzhou Normal University, Hangzhou 311121, China (e-mail: qixie68@126.com; dingzixuan8899@163.com; tangwen1012@163.com; xiaotan_cs@163.com).

Debiao He is with the School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China, and also with the Shandong Provincial Key Laboratory of Computer Networks, Qilu University of Technology, Shandong Academy of Sciences, Jinan 250014, China (e-mail: hedebiao@163.com).

Digital Object Identifier 10.1109/TVT.2023.3289175

A. Motivations and Contributions

By analyzing the existing protocols, almost all existing protocols cannot resist the impersonation attacks, forgery attacks, and privacy disclosure due to the RSU captured attack and OBU intrusion attack. From the perspective of practical application, the existing protocols can only be used in scenarios with or without transport infrastructure, but not both. In terms of authentication function and computational efficiency, the existing protocols rely on trusted third parties to achieve authentication and do not design efficient handover authentication policies. As we know, vehicles always run in scenarios with different RSU domains or without traffic infrastructure, how to design a protocol that can be applied to the above scenarios, and achieve secure and fast handover authentication, or authentication without the participation of trusted infrastructure, and track malicious behaviors under the premise of protecting user privacy and anonymity are urgent problems to be solved.

To address the above problems, we propose a blockchain-based authentication protocol for VANETs. The contributions of this article are as follows:

1) To realize the application of more scenarios, we propose a novel protocol to achieve V2I authentication, V2I handover authentication, and V2V broadcasting authentication, which can be used in scenarios with different RSU domains or without transport infrastructure.
2) To achieve security, we use PUF to avoid RSU captured attacks, use bioinformation to avoid OBU intrusion attacks, and use the dynamic anonymity strategy to avoid attackers' tracking attacks. We also design an embedding strategy of pseudo-identity and vehicle feature to recover the real identity of the malicious message sender. The proposed protocol is provable secure under the random oracle model.
3) To achieve secure and efficient authentication, we skillfully use ECC and blockchain technology to make the communication and computation efficiencies superior to other protocols.

In the next section, we introduce the related work. The models and goals of this article are presented in Section III. Preliminaries are introduced in Section IV, and the proposed scheme is given in Section V. In Sections VI and VII, we present formal security proof under the random oracle model and informal security analysis to prove the security of the proposed scheme, respectively. The proposed scheme is compared with some related schemes in terms of security, computation, communication and storage in Section VIII. Section IX concludes this article.

II. Related Work

In 2010, Liu et al. [1] proposed a message authentication protocol for VANETs. Because the private vehicles and public vehicles use group signature and identity-based signature to authenticate their identities, their scheme requires high computational costs and cannot guarantee the user's privacy. Similarly, Xue and Ding [2] proposed a group signature based vehicle authentication protocol. Because of the use of fixed pseudo-identity and bilinear pairings based signatures, their scheme cannot obtain the untraceability and high computational efficiency. In 2016, Liu et al. [3] proposed an anonymous authentication protocol based on bilinear pairings and asymmetric encryption. Although the protocol realizes batch authentication, the high computational overhead is still an unavoidable problem. Wang and Yao [4] proposed an anonymous message authentication protocol based on local identity. The protocol uses Certificate Revocation List (CRL) to resolve the revocation of the vehicles and RSUs. Entities need to ensure that the other party is legal in the CRL before authentication. Similarly, because the protocol uses asymmetric signatures and bilinear pairs, the computational cost is very high. In order to deal with the communication overhead, storage overhead, computational overhead, and potential privacy disclosure brought by CRL, Jiang et al. [5] proposed an anonymous batch authentication scheme using the identity-based signature and the Hash Message Authentication Code (HMAC), In addition, the protocol uses RSUs to manage vehicles locally in the way of grouping by region, but asymmetric encryption and bilinear pair also bring considerable computational overhead. Zhang et al. [6] proposed a bilinear pairing-based authentication protocol combining batch group signature verification and group session key distribution for VANETs, which resists impersonation attacks by using tracking key implementation. Compared with the previous protocols, the efficiency of this protocol is not much improved. In 2019, Li et al. [7] proposed a hierarchical revocable authentication scheme based on the self-certified public keys and Elliptic Curve Cryptography (ECC)-based Schnorr signatures. Compared with the above schemes, the efficiency of this protocol has been greatly improved, but there is still the problem of location leakage caused by fixed pseudo-identity. Zhang et al. [8] constructed a group communication authentication protocol for VANETs using the Chinese Remainder Theorem (CRT). However, Xiong et al. [9] found out that Zhang et al.'s scheme is vulnerable to impersonation attack. The disadvantage of CRT is that the public parameters need to be updated when the members are added and removed, which may suffer from desynchronization attack. In 2021, Wang et al. [10] proposed a lightweight authentication protocol for an emergency vehicle. In their scheme, after the vehicle is authenticated by the first RSU, the vehicle can complete the mutual authentication with the subsequent RSU. The handover authentication is realized by the continuous forwarding of messages between RSUs, in which the fixed parameters of vehicles will lead to tracking attacks. Meanwhile, RSU has certain privileges, the protocol cannot resist privileged-insider attack and RSU captured attack. Wang and Liu [11] proposed a message authentication protocol for VANETs, which combines pseudonym and group signature to realize mutual authentication between vehicles and RSU. This protocol uses CRL and asymmetric signature to achieve V2I authentication, which cannot avoid the problems mentioned above. Xie et al. [12] proposed a lightweight V2V broadcast authentication and key agreement protocol without relying on a third party, which is based on ECC and the pseudo-identity to protect privacy and unlinkability. The advantage of this protocol is that it can perform V2V authentication and message broadcast in the scenario without traffic infrastructure.

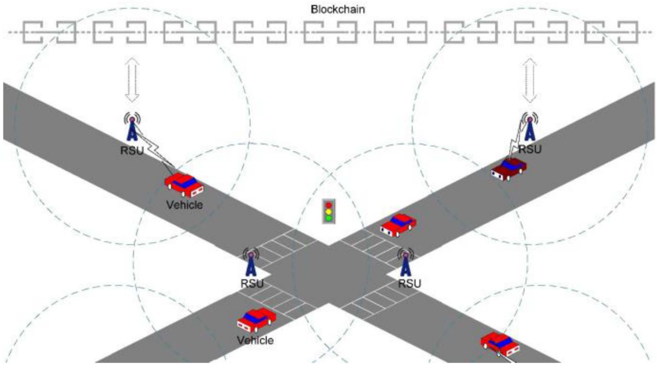


Fig. 1. The model of V2I authentication and announcement.

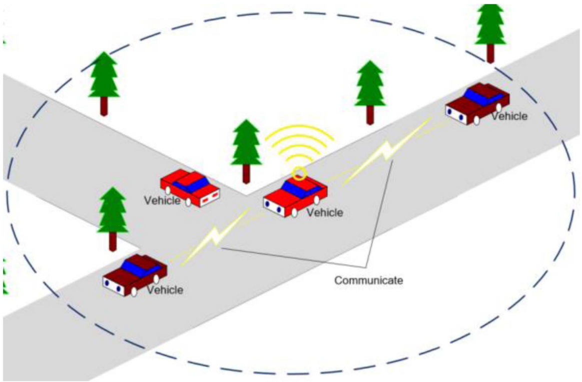


Fig. 2. The model of V2V broadcast.

The above signature strategies based on asymmetric encryption have high computing and communication overhead, group communication and group signature also have great limitations in practical applications. In addition, RSUs are independent entities deployed on the roadside which stored secret values [10], [13], [14], [15], [16], once the RSU is captured, attackers can obtain the information stored in RSU, and launch impersonation attack, forgery attack, and obtain user's identity.

As a new technology with many advantages, blockchain has also been applied to VANETs and V2I handover authentication. In 2019, Zheng et al. [13] proposed an access authentication system for VANETs. Blockchain is regarded as a public distributed ledger to realize authentication and accident recording. Zheng et al.'s protocol eliminates the computational and time overhead caused by repeated authentication. However, vehicles still need to use asymmetric encryption-based signatures to authenticate, and an attacker can impersonate any vehicle to publish forged information by capturing RSU. The scheme is not secure enough and still has a high computation overhead. In 2020, Ma et al. [14] proposed a decentralized key management mechanism for VANETs, which realizes registration, update, and revocation of vehicles' public keys based on the smart contract. In addition, they presented a bivariate polynomial-based authentication protocol. However, the RSU handover authentication is not considered and designed, so the vehicle needs to be re-authenticated when entering a new RSU domain. Wang et al. [15] proposed a V2I authentication scheme using blockchain to realize trusted and scalable computing. Their scheme realizes rapid re-authentication of vehicles through ownership transfer between RSUs. Nonetheless, the use of bilinear pairs makes the scheme maintain a high time overhead. In 2022, Son et al. [16] proposed a scheme of handover authentication for VANETs to avoid unnecessary duplicate authentication. During the first V2I authentication, the vehicle and RSU agree on the session key based on Elliptic Curve Discrete Logarithm Problem (ECDLP), and RSU uploads the vehicle authentication information and signature to the blockchain. Nevertheless, we found that in the subsequent blockchain-based handover authentication, vehicles and other RSUs still need time-consuming authentication processes, and their scheme cannot resist RSU captured attacks. Qureshi et al. [17] proposed a blockchain-based authentication model for intelligent transportation systems. The model uses smart contracts and RSU to authenticate the vehicles. The scheme realizes decentralized data storage based on the blockchain network. Yang et al. [18] proposed a decentralized handover authentication protocol for VANETs based on the bilinear pairing and ECC. After the first authentication with the edge node, the vehicle will receive an authentication token based on the identity signature, and the handover authentication is based on the token. Mei et al. proposed a blockchain-based authentication scheme for the transportation cyber-physical system [19].

However, it can be seen from the above protocols [13], [14], [15], [16], [18] that the introduction of blockchain has not solved RSU captured attack, privacy disclosure, and high computation overhead.

III. Models and Goals

A. System Model

The proposed scheme consists of vehicles (OBU), RSUs, TA, and the blockchain. TA is officially trusted and used for the registration of vehicles and RSUs. In addition, TA can track the real identity of the malicious message. Fig. 1 shows the scene of first authentication, handover authentication, and V2I announcement during driving. When the vehicle enters the road area composed of legal RSUs for the first time, the vehicle selects an RSU to conduct the first mutual authentication, then the RSU uploads the authentication information to the blockchain. When a vehicle issues an announcement, it sends a request to an RSU nearby. The RSU first performs handover authentication for the vehicle with the help of the blockchain. After the authentication is passed, the RSU broadcasts the announcement of the vehicle and uploads it to the blockchain. RSU can be regarded as an official terminal device providing professional, extensive, and guaranteed services for vehicles.

Considering that the deployment of RSU is not fully covered in the actual application scenario. If an emergency occurs in the road section without RSU, the vehicle safety may be threatened due to time delay. Therefore, in addition to the V2I authentication and announcement protocol, the proposed protocol can also realize V2V broadcasting authentication without RSU or TA. The broadcast protocol model is shown in Fig. 2. When the vehicle encounters a situation, it broadcasts a message to the surrounding vehicles. After receiving the broadcast message, other vehicles first verify the legitimacy of the sender's identity and the integrity of the broadcast content. If the verification passes, other vehicles trust the broadcast message and take further actions.

B. Adversary Model

Combined with Dolev-Yao (DY) model [25] and the actual application scenario of VANETs, the attacker model for VANETs is shown as below.

1) The adversary A could be a legitimately registered vehicle (user) or internal attacker, which means that the attacker may launch the impersonation attacks or send malicious messages.
2) A can eavesdrop, modify, intercept, and replay the messages transmitted publicly.
3) A can launch the side-channel attacks on OBU and RSU to obtain stored data, but it is difficult for attackers to obtain biological keys and crack PUF.
4) The content of the blockchain is public to attackers, but attackers cannot tamper with the content on the blockchain.

C. Design Goals

1) The proposed protocol can realize V2I authentication, V2I handover authentication, and V2V broadcasting authentication, which can be used in scenarios with different RSU domains or without transport infrastructure.
2) The proposed protocol is provably secure, which can resist all known attacks, such as RSU captured attacks, OBU intrusion attacks, and can achieve several known advantages, such as perfect forward secrecy, identity traceability, etc.
3) The proposed protocol is lightweight, the communication and computation costs are more efficient than other protocols.

IV. Preliminaries

In this section, we introduce the technologies used in the proposed scheme.

A. Blockchain

As an emerging technology, blockchain has received great attention and has been widely applicated since it was proposed [26]. The blockchain is essentially a distributed shared ledger and database, which has the characteristics of decentralization, non-tampering, openness and transparency, and traceability of records. Therefore, it is widely used in finance, insurance, medical care, VANETs, and other fields. According to the openness of blockchain, it can be divided into public blockchains, alliance blockchains, and private blockchains. The public blockchain has the highest degree of openness and decentralization, and its complex consensus mechanism also has an extremely high overhead. The alliance blockchain is only used by consortium members, so they are less open than the public blockchain. The private blockchain is for internal use only. In terms of computational overhead, the alliance blockchain and the private blockchain are usually much lower than the public blockchain [27].

Structurally, a blockchain can be viewed as a chain of multiple blocks, each of which consists of a block header and a block. Usually, the header information of the block mainly includes the version number, the hash value of the previous block, the timestamp, the Merkle tree, and the nonce. Due to the avalanche effect of the hash value, the content written to the blockchain will be difficult to be tampered with.

We use the transparency of the blockchain to ensure the public verifiability of the vehicle identity between RSUs, so the vehicle can be quickly handover authenticated in subsequent RSU after the initial authentication. The tamper-proof feature of blockchain can resist message tampering and identity impersonation attacks. Compared with database sharing and public transmission, the decentralization of blockchain will not be affected by single point of failure. In addition, in order to prevent tracking attacks on content on the blockchain, we use dynamic anonymity and encryption strategies to protect vehicle privacy.

B. Physically Unclonable Function

PUF is a hardware security technology that exploits inherent device variation to produce an unclonable unique device response to a given input [28]. PUF can be thought of as similar to human biometrics, they are an inherent and unique identifier for each piece of silicon. Due to imperfect silicon processing technology, each Integrated Circuit (IC) produced is physically different. These process variations manifest themselves in different path delays, transistor threshold voltages, voltage gains, and countless other ways between different integrated circuits. PUF exploits this inherent difference in IC behavior to generate a unique encryption key for each IC. Unlike traditional encryption methods that use a single stored key, PUF works by implementing challenge-response authentication. For a given PUF, a specific input called a "challenge", will produce an output called a "response", that is unique to the specific PUF and therefore unclonable. Attempting to detect a PUF greatly affects its response to a challenge, so even if the hardware device is acquired by an attacker, the PUF-protected information in the device will not be leaked [29].

The security of the existing protocols is destroyed due to RSU captured attacks, the deployment of PUF in RSU can effectively solve this problem. The reason is that the special circuit design of PUF may change the output value of PUF when an adversary analyze and uses data in RSU even if the RSU is captured, which ensures that the information encrypted by PUF will not be used by the adversary.

PUF is a fast hardware operation based on the circuit, the operating frequency level of PUF is MHz, and the time cost of a single operation is generally less than 1 nanosecond (ns). In contrast, the time cost of hash operation is at the millisecond (ms) level, so the time cost of PUF can generally be ignored. In addition, PUF is only calculated in the RSU and will not generate additional communication overhead.

TABLE I
NOTATIONS

Notations	Description
TA	Trusted-authority
VID_i	Unique vehicle identity (e.g., engine number) of vehicle i
RSU_t	t-th roadside unit
RID_t	Unique identity of RSU_t
$PUF(.)$	Physical unclonable function
(Cha_t, Res_t)	The challenge and response of PUF in RSU_t
P	The generator of the elliptic curve
SK_{TA}	The secret key of TA
PK_{TA}	The public key of TA, $PK_{TA} = SK_{TA} \cdot P$
SK_{Vi}	The secret parameter of vehicle i
PK_{Vi}	The public key of vehicle i, $PK_{Vi} = SK_{Vi} \cdot P$
VaI_i	Appearance information of vehicle i
T_1, T_2, T_3, T_4	Timestamps
$\triangle T$	Time threshold
K_{RSU}	Secret value shared between $RSUs$
Bio_i	The biological information of user
$Gen(.), Rep(.)$	The generation and reproduction functions of Fuzzy extractor
σ_i, τ_i	Biological key and reproduction parameter of user

V. Proposed Scheme

In this section, we introduce the proposed blockchain-based lightweight handover authentication and secure broadcasting protocol for VANETs. The protocol consists of initialization phase, registration phase, first authentication phase, V2I handover authentication and announcement phase, V2V message broadcast phase, and pseudo-identity of vehicle updates phase. The notations used in the protocol are listed in Table I.

A. Initialization Phase

The trusted-authority TA selects an elliptic curve $E(GF_q)$, where $GF(q)$ and q are the finite field and a large prime number, respectively. Then, TA selects a secret parameter K_{RSU}, and publishes the generator point P of the elliptic curve. TA generates its secret key SK_{TA}, computes and publishes PK_{TA}, where $PK_{TA} = SK_{TA} \cdot P$.

B. Registration Phase

The registration phases include vehicle registration and RSU registration. The registration phases are shown in Figs. 3 and 4, respectively.

1) Vehicle Registration Phase:

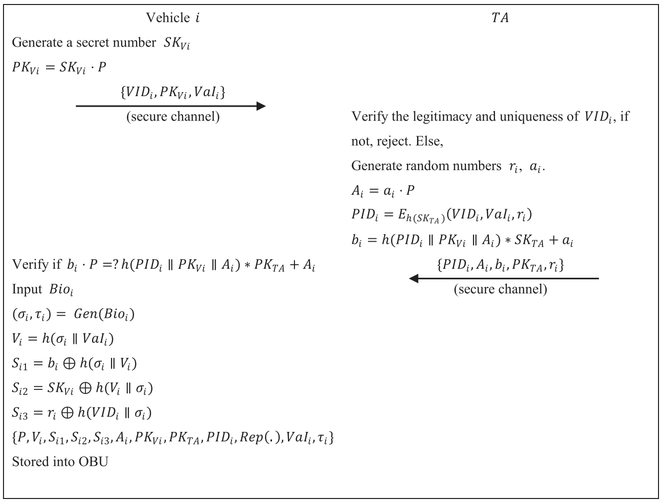
Step VR1: The vehicle (with driver) generates a secret number SK_{Vi}, and computes $PK_{Vi} = SK_{Vi} \cdot P$. Then, it sends the identity of the vehicle (e.g., engine number) VID_i, the appearance information VaI_i, and PK_{Vi} to the trusted authority TA.

Step VR2: After receiving the message, TA first checks the legitimacy and uniqueness of VID_i. If not, TA rejects the registration requestion. Else, it generates random numbers r_i and a_i, and computes

$$A_i = a_i \cdot P,$$

$$PID_i = E_{h(SK_{TA})}\left(VID_i, VaI_i, r_i\right),$$

$$\text{and } b_i = h\left(PID_i \parallel PK_{Vi} \parallel A_i\right) * SK_{TA} + a_i.$$



Vehicle i

TA

Generate a secret number SK_{Vi}

$PK_{Vi} = SK_{Vi} \cdot P$

$\{VID_i, PK_{Vi}, VaI_i\}$

(secure channel)

Verify the legitimacy and uniqueness of VID_i, if not, reject. Else,

Generate random numbers r_i, a_i.

$A_i = a_i \cdot P$

$PID_i = E_{h(SK_{TA})}(VID_i, VaI_i, r_i)$

$b_i = h(PID_i \parallel PK_{Vi} \parallel A_i) * SK_{TA} + a_i$

Verify if $b_i \cdot P =? h(PID_i \parallel PK_{Vi} \parallel A_i) * PK_{TA} + A_i$

$\{PID_i, A_i, b_i, PK_{TA}, r_i\}$

(secure channel)

Input Bio_i

$(\sigma_i, \tau_i) = Gen(Bio_i)$

$V_i = h(\sigma_i \parallel VaI_i)$

$S_{i1} = b_i \oplus h(\sigma_i \parallel V_i)$

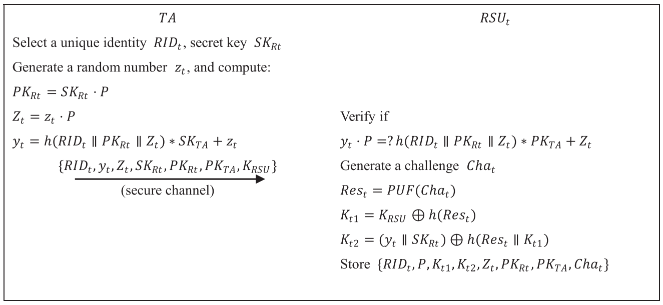
$S_{i2} = SK_{Vi} \oplus h(V_i \parallel \sigma_i)$

$S_{i3} = r_i \oplus h(VID_i \parallel \sigma_i)$

$\{P, V_i, S_{i1}, S_{i2}, S_{i3}, A_i, PK_{Vi}, PK_{TA}, PID_i, Rep(.), VaI_i, \tau_i\}$

Stored into OBU

Fig. 3. Vehicle registration phase.



TA

RSU_t

Select a unique identity RID_t, secret key SK_{Rt}

Generate a random number z_t, and compute:

$PK_{Rt} = SK_{Rt} \cdot P$

$Z_t = z_t \cdot P$

$y_t = h(RID_t \parallel PK_{Rt} \parallel Z_t) * SK_{TA} + z_t$

$\{RID_t, y_t, Z_t, SK_{Rt}, PK_{Rt}, PK_{TA}, K_{RSU}\}$

(secure channel)

Verify if

$y_t \cdot P =? h(RID_t \parallel PK_{Rt} \parallel Z_t) * PK_{TA} + Z_t$

Generate a challenge Cha_t

$Res_t = PUF(Cha_t)$

$K_{t1} = K_{RSU} \oplus h(Res_t)$

$K_{t2} = (y_t \parallel SK_{Rt}) \oplus h(Res_t \parallel K_{t1})$

Store $\{RID_t, P, K_{t1}, K_{t2}, Z_t, PK_{Rt}, PK_{TA}, Cha_t\}$

Fig. 4. RSU registration phase.

Then, TA sends the message $\{PID_i, A_i, b_i, PK_{TA}, r_i\}$ to the vehicle through the secure channel.

Step VR3: On receiving the message $\{PID_i, A_i, b_i, PK_{TA}, r_i\}$, the vehicle first verifies if$b_i \cdot P = h(PID_i \parallel PK_{Vi} \parallel A_i) * PK_{TA} + A_i$, if not, aborts it. Else, the owner inputs the biological information Bio_i, and computes

$$\left(\sigma_i, \tau_i\right) = Gen\left(Bio_i\right),$$

$$V_i = h\left(\sigma_i \parallel VaI_i\right),$$

$$S_{i1} = b_i \oplus h\left(\sigma_i \parallel V_i\right),$$

$$S_{i2} = SK_{Vi} \oplus h\left(V_i \parallel \sigma_i\right),$$

$$\text{and } S_{i3} = r_i \oplus h\left(VID_i \parallel \sigma_i\right).$$

$\{P, V_i, S_{i1}, S_{i2}, S_{i3}, A_i, PK_{Vi}, PK_{TA}, PID_i, Rep(.), VaI_i, \tau_i\}$ is stored in the OBU by the vehicle.

2) RSU Registration Phase:

Step RR1: TA selects a unique identity RID_t and the secret key SK_{Rt} for the t-th RSU. Then, TA generates a random number z_t and computes

$$PK_{Rt} = SK_{Rt} \cdot P,$$

$$Z_t = z_t \cdot P,$$

$$\text{and } y_t = h\left(RID_t \parallel PK_{Rt} \parallel Z_t\right) * SK_{TA} + z_t.$$

The message $\{RID_t, y_t, Z_t, SK_{Rt}, PK_{Rt}, PK_{TA}, K_{RSU}\}$ is sent to the RSU_t through the secure channel.

Step RR2: On receiving the message, RSU_t first verifies if $y_t \cdot P = h(RID_t \parallel PK_{Rt} \parallel Z_t) * PK_{TA} + Z_t$. If not, aborts it, else, RSU_t generates a challenge Cha_t and computes

$$Res_t = PUF\left(Cha_t\right),$$

$$K_{t1} = K_{RSU} \oplus h\left(Res_t\right),$$

$$\text{and } K_{t2} = \left(y_t \parallel SK_{Rt}\right) \oplus h\left(Res_t \parallel K_{t1}\right).$$

RSU_t stores $\{RID_t, P, K_{t1}, K_{t2}, Z_t, PK_{Rt}, PK_{TA}, Cha_t\}$.

C. First Authentication Phase

In this phase, the vehicle enters the RSU domain and sends an authentication request to RSU_t for the first time. The steps are as follows:

Step FA1: The user inputs the biological information Bio'_i, and the vehicle computes $\sigma'_i = Rep(Bio'_i, \tau_i)$. If $V_i \neq h(\sigma'_i \parallel \ VaI_i)$, the vehicle refuses the login requestion, else, computes

$$b_i = S_{i1} \oplus h\left(\sigma'_i \parallel V_i\right),$$

$$\text{and } SK_{Vi} = S_{i2} \oplus h\left(V_i \parallel \sigma'_i\right).$$

The vehicle generates a random number d_i, timestamp T_1, then computes

$$D_i = d_i \cdot P,$$

$$\text{and } c_i = b_i + SK_{Vi} + h(PID_i \parallel T_1 \parallel D_i) * d_i.$$

The message $\{PID_i, A_i, D_i, PK_{Vi}, c_i, T_1\}$ is sent to RSU_t via the public channel.

Step FA2: Upon receiving the message $\{PID_i, A_i, D_i, PK_{Vi}, c_i, T_1\}$, RSU_t first checks the freshness of T_1, if T_1 is fresh and $c_i \cdot P = h(PID_i \parallel PK_{Vi} \parallel A_i) \cdot PK_{TA} + A_i + PK_{Vi} + h(PID_i \parallel T_1 \parallel D_i) \cdot D_i$, RSU_t generates a random number e_t and computes

$$Res_t = PUF\left(Cha_t\right),$$

$$K_{RSU} = K_{t1} \oplus h\left(Res_t\right),$$

$$\left(y_t \parallel SK_{Rt}\right) = K_{t2} \oplus h\left(Res_t \parallel K_{t1}\right),$$

$$E_t = e_t \cdot P,$$

$$\text{and } SK_{ti} = h\left(e_t \cdot D_i\right).$$

Then, RSU_t generates a timestamp T_2 and computes

$$f_t = y_t + SK_{Rt} + h\left(E_t \parallel RID_t \parallel T_2\right) * e_t,$$

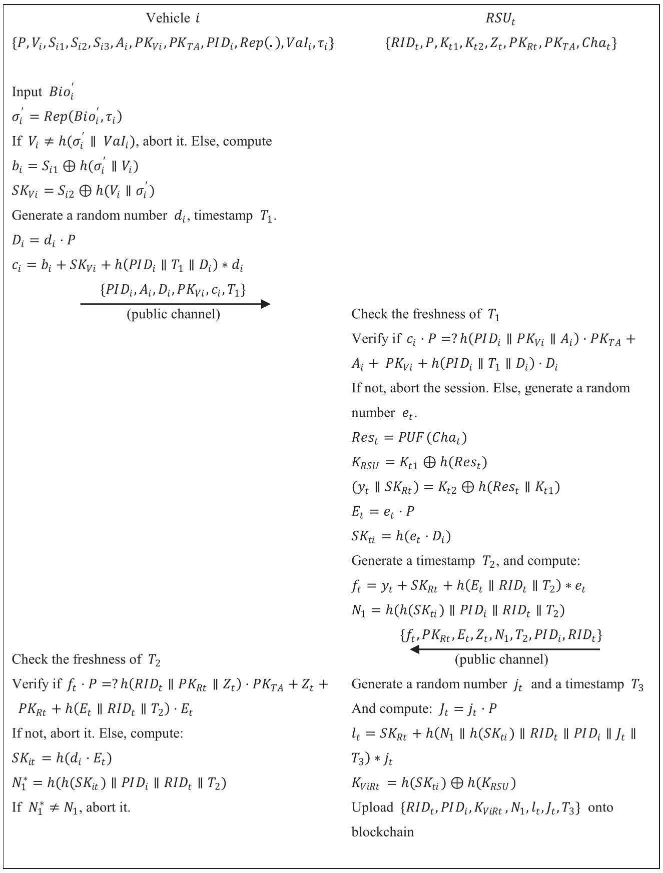
$$\text{and } N_1 = h\left(h\left(SK_{ti}\right) \parallel PID_i \parallel RID_t \parallel T_2\right).$$

The message $\{f_t, PK_{Rt}, E_t, Z_t, N_1, T_2, PID_i, RID_t\}$ is sent to the vehicle through the public channel. RSU_t generates a random number j_t, timestamp T_3, then computes

$$J_t = j_t \cdot P,$$

$$l_t = SK_{Rt} + h(N_1 \parallel h(SK_{ti}) \parallel RID_t \parallel PID_i \parallel J_t \parallel T_3) * j_t,$$

$$\text{and } K_{ViRt} = h(SK_{ti}) \oplus h(K_{RSU}).$$



Vehicle i

$\{P, V_i, S_{i1}, S_{i2}, S_{i3}, A_i, PK_{Vi}, PK_{TA}, PID_i, Rep(.), VaI_i, \tau_i\}$

Input $Bio_i^{'}$

$\sigma_i^{'} = Rep(Bio_i^{'}, \tau_i)$

If $V_i \neq h(\sigma_i^{'} \parallel VaI_i)$, abort it. Else, compute

$b_i = S_{i1} \oplus h(\sigma_i^{'} \parallel V_i)$

$SK_{Vi} = S_{i2} \oplus h(V_i \parallel \sigma_i^{'})$

Generate a random number d_i, timestamp T_1.

$D_i = d_i \cdot P$

$c_i = b_i + SK_{Vi} + h(PID_i \parallel T_1 \parallel D_i) * d_i$

$\xrightarrow[\text{(public channel)}]{\{PID_i, A_i, D_i, PK_{Vi}, c_i, T_1\}}$

RSU_t

$\{RID_t, P, K_{t1}, K_{t2}, Z_t, PK_{Rt}, PK_{TA}, Cha_t\}$

Check the freshness of T_1

Verify if $c_i \cdot P =? h(PID_i \parallel PK_{Vi} \parallel A_i) \cdot PK_{TA} + A_i + PK_{Vi} + h(PID_i \parallel T_1 \parallel D_i) \cdot D_i$

If not, abort the session. Else, generate a random number e_t.

$Res_t = PUF(Cha_t)$

$K_{RSU} = K_{t1} \oplus h(Res_t)$

$(y_t \parallel SK_{Rt}) = K_{t2} \oplus h(Res_t \parallel K_{t1})$

$E_t = e_t \cdot P$

$SK_{ti} = h(e_t \cdot D_i)$

Generate a timestamp T_2, and compute:

$f_t = y_t + SK_{Rt} + h(E_t \parallel RID_t \parallel T_2) * e_t$

$N_1 = h(h(SK_{ti}) \parallel PID_i \parallel RID_t \parallel T_2)$

$\xleftarrow[\text{(public channel)}]{\{f_t, PK_{Rt}, E_t, Z_t, N_1, T_2, PID_i, RID_t\}}$

Check the freshness of T_2

Verify if $f_t \cdot P =? h(RID_t \parallel PK_{Rt} \parallel Z_t) \cdot PK_{TA} + Z_t + PK_{Rt} + h(E_t \parallel RID_t \parallel T_2) \cdot E_t$

If not, abort it. Else, compute:

$SK_{it} = h(d_i \cdot E_t)$

$N_1^* = h(h(SK_{it}) \parallel PID_i \parallel RID_t \parallel T_2)$

If $N_1^* \neq N_1$, abort it.

Generate a random number j_t and a timestamp T_3

And compute: $J_t = j_t \cdot P$

$l_t = SK_{Rt} + h(N_1 \parallel h(SK_{ti}) \parallel RID_t \parallel PID_i \parallel J_t \parallel T_3) * j_t$

$K_{ViRt} = h(SK_{ti}) \oplus h(K_{RSU})$

Upload $\{RID_t, PID_i, K_{ViRt}, N_1, l_t, J_t, T_3\}$ onto blockchain

Fig. 5. First authentication phase.

The record $\{RID_t, PID_i, K_{ViRt}, N_1, l_t, J_t, T_3\}$ is uploaded onto the blockchain by RSU_t, which indicates that the vehicle PID_i was authenticated by RSU_t at time T_3. As a shared immutable ledger, the content of the blockchain cannot be tampered with. Other RSUs can perform fast handover authentication for the vehicle PID_i based on the first authentication information on the blockchain.

Step FA3: On receiving the message $\{f_t, PK_{Rt}, E_t, Z_t, N_1, T_2, PID_i, RID_t\}$, the vehicle first checks if the timestamp T_2 is fresh and if $f_t \cdot P = h(RID_t \parallel PK_{Rt} \parallel Z_t) \cdot PK_{TA} + Z_t + PK_{Rt} + h(E_t \parallel RID_t \parallel T_2) \cdot E_t$ is correct, if not, the vehicle terminates the session. Otherwise, computes

$$SK_{it} = h\left(d_i \cdot E_t\right),$$

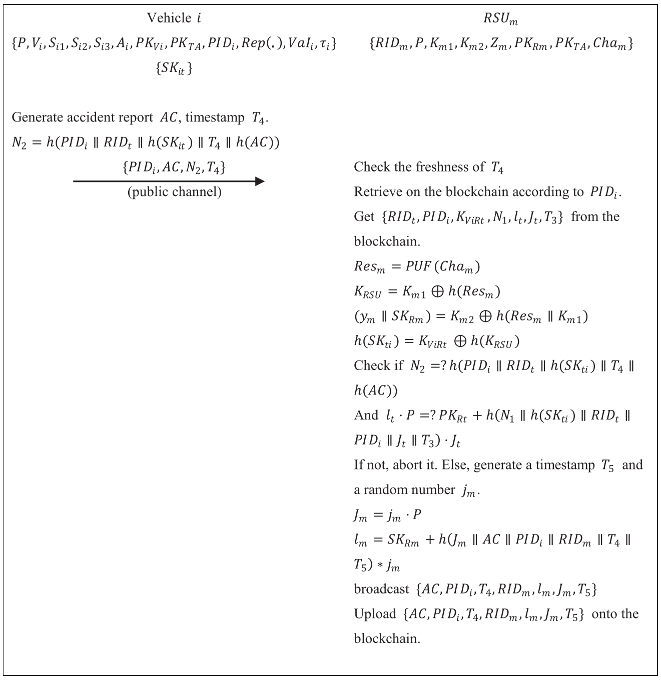
$$\text{and } N_1^* = h\left(h\left(SK_{it}\right) \parallel PID_i \parallel RID_t \parallel T_2\right).$$

If $N_1^* \neq N_1$, aborts it. Else, stores SK_{it}. The first authentication phase is shown in Fig. 5.

D. V2I Handover Authentication and Announcement Phase

After the first authentication, the vehicle sends an accident report to the RSU and the RSU announces it. The steps are as follows:

Step AN1: The vehicle generates the accident report AC and the timestamp T_4, then computes $N_2 = h(PID_i \parallel RID_t \parallel$



Vehicle i

$\{P, V_i, S_{i1}, S_{i2}, S_{i3}, A_i, PK_{Vi}, PK_{TA}, PID_i, Rep(.), VaI_i, \tau_i\}$

$\{SK_{it}\}$

RSU_m

$\{RID_m, P, K_{m1}, K_{m2}, Z_m, PK_{Rm}, PK_{TA}, Cha_m\}$

Generate accident report AC, timestamp T_4.

$N_2 = h(PID_i \parallel RID_t \parallel h(SK_{it}) \parallel T_4 \parallel h(AC))$

$\xrightarrow[\text{(public channel)}]{\{PID_i, AC, N_2, T_4\}}$

Check the freshness of T_4

Retrieve on the blockchain according to PID_i.

Get $\{RID_t, PID_i, K_{ViRt}, N_1, l_t, J_t, T_3\}$ from the blockchain.

$Res_m = PUF(Cha_m)$

$K_{RSU} = K_{m1} \oplus h(Res_m)$

$(y_m \parallel SK_{Rm}) = K_{m2} \oplus h(Res_m \parallel K_{m1})$

$h(SK_{ti}) = K_{ViRt} \oplus h(K_{RSU})$

Check if $N_2 =?\, h(PID_i \parallel RID_t \parallel h(SK_{ti}) \parallel T_4 \parallel h(AC))$

And $l_t \cdot P =?\, PK_{Rt} + h(N_1 \parallel h(SK_{ti}) \parallel RID_t \parallel PID_i \parallel J_t \parallel T_3) \cdot J_t$

If not, abort it. Else, generate a timestamp T_5 and a random number j_m.

$J_m = j_m \cdot P$

$l_m = SK_{Rm} + h(J_m \parallel AC \parallel PID_i \parallel RID_m \parallel T_4 \parallel T_5) * j_m$

broadcast $\{AC, PID_i, T_4, RID_m, l_m, J_m, T_5\}$

Upload $\{AC, PID_i, T_4, RID_m, l_m, J_m, T_5\}$ onto the blockchain.

Fig. 6. V2I handover authentication and announcement phase.

$h(SK_{it}) \parallel T_4 \parallel h(AC))$. The message $\{PID_i, AC, N_2, T_4\}$ is sent to RSU_m.

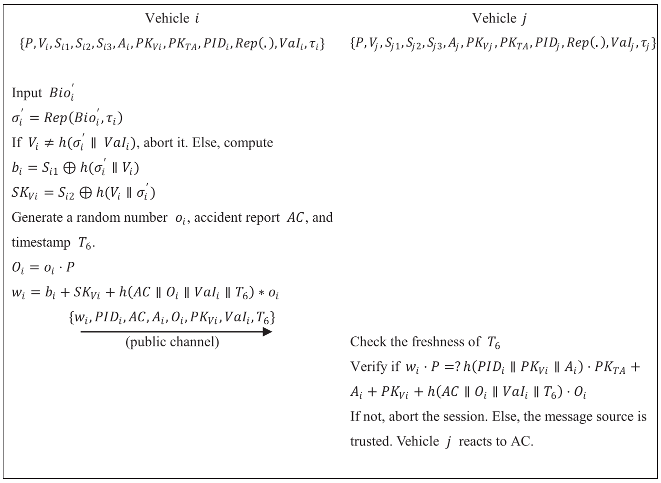
Step AN2: On receiving the message, RSU_m checks the freshness of T_4 and retrieves the record $\{RID_t, PID_i, K_{ViRt}, N_1, l_t, J_t, T_3\}$ according to PID_i on the blockchain, which is the certification that the vehicle PID_i has been authenticated by RSU_t. Then RSU_m computes

$$\begin{aligned} Res_m &= PUF\left(Cha_m\right), \\ K_{RSU} &= K_{m1} \oplus h\left(Res_m\right), \\ (y_m \parallel SK_{Rm}) &= K_{m2} \oplus h\left(Res_m \parallel K_{m1}\right), \\ \text{and } h\left(SK_{ti}\right) &= K_{ViRt} \oplus h\left(K_{RSU}\right). \end{aligned}$$

If $N_2 \neq h(PID_i \parallel RID_t \parallel h(SK_{ti}) \parallel T_4 \parallel h(AC))$ or $l_t \cdot P \neq PK_{Rt} + h(N_1 \parallel h(SK_{ti}) \parallel RID_t \parallel PID_i \parallel J_t \parallel T_3) \cdot J_t$, RSU_m aborts it. Else, RSU_m generates a timestamp T_5, a random number j_m, and computes

$$J_m = j_m \cdot P, \text{ and}$$
$$l_m = SK_{Rm} + h\left(J_m \parallel AC \parallel PID_i \parallel RID_m \parallel T_4 \parallel T_5\right) * j_m.$$

RSU_m broadcasts $\{AC, PID_i, T_4, RID_m, l_m, J_m, T_5\}$ and uploads it onto the blockchain. The record indicates that the vehicle PID_i has passed the handover authentication of RID_m at T_5 and the announcement AC of the vehicle was issued by RID_m. Any vehicle can check the validity of AC by checking whether $l_m \cdot P = PK_{Rm} + h(J_m \parallel AC \parallel PID_i \parallel RID_m \parallel T_4 \parallel T_5) \cdot J_m$ is right. This phase is shown in Fig. 6.



Vehicle i

$\{P, V_i, S_{i1}, S_{i2}, S_{i3}, A_i, PK_{Vi}, PK_{TA}, PID_i, Rep(.), VaI_i, \tau_i\}$

Vehicle j

$\{P, V_j, S_{j1}, S_{j2}, S_{j3}, A_j, PK_{Vj}, PK_{TA}, PID_j, Rep(.), VaI_j, \tau_j\}$

Input $Bio_i^{'}$

$\sigma_i^{'} = Rep(Bio_i^{'}, \tau_i)$

If $V_i \neq h(\sigma_i^{'} \parallel VaI_i)$, abort it. Else, compute

$b_i = S_{i1} \oplus h(\sigma_i^{'} \parallel V_i)$

$SK_{Vi} = S_{i2} \oplus h(V_i \parallel \sigma_i^{'})$

Generate a random number o_i, accident report AC, and timestamp T_6.

$O_i = o_i \cdot P$

$w_i = b_i + SK_{Vi} + h(AC \parallel O_i \parallel VaI_i \parallel T_6) * o_i$

$\xrightarrow[\text{(public channel)}]{\{w_i, PID_i, AC, A_i, O_i, PK_{Vi}, VaI_i, T_6\}}$

Check the freshness of T_6

Verify if $w_i \cdot P =?\, h(PID_i \parallel PK_{Vi} \parallel A_i) \cdot PK_{TA} + A_i + PK_{Vi} + h(AC \parallel O_i \parallel VaI_i \parallel T_6) \cdot O_i$

If not, abort the session. Else, the message source is trusted. Vehicle j reacts to AC.

Fig. 7. V2V message broadcast phase.

E. V2V Message Broadcast Phase

If there is no RSU around the vehicle i, the vehicle i can broadcast the accident reports to other vehicles.

Step BR1: The user inputs the biological information Bio'_i, and the vehicle i computes $\sigma'_i = Rep(Bio'_i, \tau_i)$. If $V_i \neq h(\sigma'_i \parallel VaI_i)$, the vehicle i refuses the login requestion, else, computes

$$b_i = S_{i1} \oplus h\left(\sigma'_i \parallel V_i\right),$$
$$\text{and } SK_{Vi} = S_{i2} \oplus h\left(V_i \parallel \sigma'_i\right).$$

The vehicle i generates a random number o_i, accident report AC, and timestamp T_6. Then, computes

$$O_i = o_i \cdot P,$$
$$\text{and } w_i = b_i + SK_{Vi} + h\left(AC \parallel O_i \parallel VaI_i \parallel T_6\right) * o_i.$$

The vehicle i broadcasts $\{w_i, PID_i, AC, A_i, O_i, PK_{Vi}, VaI_i, T_6\}$ to other vehicles.

Step BR2: Assumes the vehicle j receives the message $\{w_i, PID_i, AC, A_i, O_i, PK_{Vi}, VaI_i, T_6\}$. The vehicle j first checks the freshness of T_6 and verifies if $w_i \cdot P = h(PID_i \parallel PK_{Vi} \parallel A_i) \cdot PK_{TA} + A_i + PK_{Vi} + h(AC \parallel O_i \parallel VaI_i \parallel T_6) \cdot O_i$ is right. if not, the vehicle j aborts it, else, the vehicle j trusts the message source. In case of dispute or malicious message, the vehicle j can send PID_i and VaI_i to TA, then TA can compute $D_{h(SK_{TA})}(PID_i) = (VID_i, VaI_i, r_i)$ and obtain the identity of vehicle i. The steps of the broadcasting phase are shown in Fig. 7.

F. Pseudo-Identity of Vehicle Updates Phase

If the vehicle i has completed the current transaction, it requests TA by performing the following steps to update pseudo-identity.

Step IU1: The user inputs the biological information Bio'_i, and the vehicle i computes $\sigma'_i = Rep(Bio'_i, \tau_i)$. If $V_i \neq h(\sigma'_i \parallel VaI_i)$, the vehicle i refuses the login requestion, else, computes $r_i = S_{i3} \oplus h(VID_i \parallel \sigma'_i)$. The vehicle i generates a new secret number SK_{Vi}^{*}, a timestamp T_6, and computes

$$PK_{Vi}^{*} = SK_{Vi}^{*} \cdot P,$$
$$\text{and } M_1 = E_{r_i}\left(VID_i, PK_{Vi}^{*}, PID_i, T_6\right).$$

The vehicle i sends $\{PID_i, M_1, T_6\}$ to TA through the public channel.

Step IU2: TA first checks if T_6 is fresh, then computes

$$(VID_i, VaI_i, r_i) = D_{h(SK_{TA})}\left(PID_i\right),$$
$$\text{and } \left(VID_i^{*}, PK_{Vi}^{*}, PID_i^{*}, T_6^{*}\right) = D_{r_i}\left(M_1\right).$$

If $VID_i^{*} \neq VID_i$ or $PID_i^{*} \neq PID_i$ or $T_6^{*} \neq T_6$, TA aborts it, else, TA generates random numbers r_i^{*}, a_i^{*}, and computes

$$A_i^{*} = a_i^{*} \cdot P,$$
$$PID_i^{*} = E_{h(SK_{TA})}\left(VID_i \parallel VaI_i \parallel r_i^{*}\right),$$
$$\text{and } b_i^{*} = h\left(PID_i^{*} \parallel PK_{Vi}^{*} \parallel A_i^{*}\right) * SK_{TA} + a_i^{*}.$$

TA generates a timestamp T_7, and computes $M_2 = E_{r_i}$ $(VID_i, A_i^{*}, PID_i^{*}, b_i^{*}, r_i^{*}, T_7)$. The message $\{PID_i, M_2, T_7\}$ is sent to the vehicle i through the public channel.

Step IU3: On receiving the message, the vehicle i first checks the freshness of T_7 and computes $(VID_i^{**}, A_i^{*}, PID_i^{*}, b_i^{*}, r_i^{*}, T_7) = D_{r_i}(M_2)$. If $b_i^{*} \cdot P \neq h(PID_i^{*} \parallel PK_{Vi}^{*} \parallel A_i^{*}) * PK_{TA} + A_i^{*}$ or $VID_i^{**} \neq VID_i$ or $T_7^{*} \neq T_7$, the vehicle aborts it, else computes

$$S_{i1}^{*} = b_i^{*} \oplus h\left(\sigma_i \parallel V_i\right),$$
$$S_{i2}^{*} = SK_{Vi}^{*} \oplus h\left(V_i \parallel \sigma_i\right),$$
$$\text{and } S_{i3}^{*} = r_i^{*} \oplus h\left(VID_i \parallel \sigma_i\right).$$

$\{P, V_i, S_{i1}^{*}, S_{i2}^{*}, S_{i3}^{*}, A_i^{*}, PK_{Vi}^{*}, PK_{TA}, PID_i^{*}, Rep(.),$ $VaI_i, \tau_i\}$ is stored in the vehicle's OBU. The above steps are shown in Fig. 8.

VI. Formal Security Proof

In this section, we provide the formal security proof under the random oracle model to prove the security of the proposed protocol.

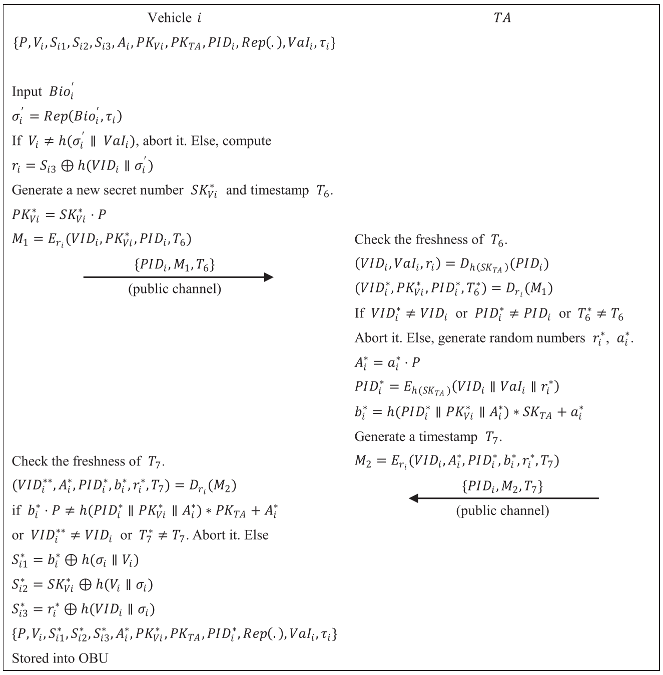
A. Definition of Random Oracle Model

Definition 1 (Participants & partnering): The participants of the scheme are composed of Trusted Authority (TA), Vehicle (V), and roadside unit (RSU). In the *i*-th instance, the participants are denoted as Π_{TA}^{i}, $\Pi_{Vi}^{i}(\Pi_{Vj}^{i})$, and Π_{RSUt}^{i}, respectively. The state of the oracle is $Accept$ if it receives a correct request.

If the oracle Π_{Vi}^{i} and Π_{RSUt}^{i} are in $Accept$ and the session key SK_{ti}^{i} (SK_{it}^{i}) has been agreed, the oracle Π_{Vi}^{i} (Π_{RSUt}^{i}) gets its session identity SID_{Vi}^{i} (SID_{RSUt}^{i}) and participant identity PID_{Vi}^{i} (PID_{RSUt}^{i}). the oracles Π_{Vi}^{i} and Π_{RSUt}^{i} can be considered partners if the following conditions are satisfied.

(1) The session key $SK_{ti}^{i} = SK_{it}^{i}$. (2) The session identity $SID_{Vi}^{i} = SID_{RSUt}^{i}$. (3) The participant identities $PID_{Vi}^{i} = \Pi_{RSUt}^{i}$, $PID_{RSUt}^{i} = \Pi_{Vi}^{i}$.

Definition 2 (Queries): the queries are defined to simulate various attacks.



Vehicle i

TA

$\{P, V_i, S_{i1}, S_{i2}, S_{i3}, A_i, PK_{Vi}, PK_{TA}, PID_i, Rep(.), VaI_i, \tau_i\}$

Input $Bio_i^{'}$

$\sigma_i^{'} = Rep(Bio_i^{'}, \tau_i)$

If $V_i \neq h(\sigma_i^{'} \parallel VaI_i)$, abort it. Else, compute

$r_i = S_{i3} \oplus h(VID_i \parallel \sigma_i^{'})$

Generate a new secret number SK_{Vi}^{*} and timestamp T_6.

$PK_{Vi}^{*} = SK_{Vi}^{*} \cdot P$

$M_1 = E_{r_i}(VID_i, PK_{Vi}^{*}, PID_i, T_6)$

$\{PID_i, M_1, T_6\}$

(public channel)

Check the freshness of T_6.

$(VID_i, VaI_i, r_i) = D_{h(SK_{TA})}(PID_i)$

$(VID_i^{*}, PK_{Vi}^{*}, PID_i^{*}, T_6^{*}) = D_{r_i}(M_1)$

If $VID_i^{*} \neq VID_i$ or $PID_i^{*} \neq PID_i$ or $T_6^{*} \neq T_6$

Abort it. Else, generate random numbers r_i^{*}, a_i^{*}.

$A_i^{*} = a_i^{*} \cdot P$

$PID_i^{*} = E_{h(SK_{TA})}(VID_i \parallel VaI_i \parallel r_i^{*})$

$b_i^{*} = h(PID_i^{*} \parallel PK_{Vi}^{*} \parallel A_i^{*}) * SK_{TA} + a_i^{*}$

Generate a timestamp T_7.

$M_2 = E_{r_i}(VID_i, A_i^{*}, PID_i^{*}, b_i^{*}, r_i^{*}, T_7)$

$\{PID_i, M_2, T_7\}$

(public channel)

Check the freshness of T_7.

$(VID_i^{**}, A_i^{*}, PID_i^{*}, b_i^{*}, r_i^{*}, T_7) = D_{r_i}(M_2)$

if $b_i^{*} \cdot P \neq h(PID_i^{*} \parallel PK_{Vi}^{*} \parallel A_i^{*}) * PK_{TA} + A_i^{*}$

or $VID_i^{**} \neq VID_i$ or $T_7^{*} \neq T_7$. Abort it. Else

$S_{i1}^{*} = b_i^{*} \oplus h(\sigma_i \parallel V_i)$

$S_{i2}^{*} = SK_{Vi}^{*} \oplus h(V_i \parallel \sigma_i)$

$S_{i3}^{*} = r_i^{*} \oplus h(VID_i \parallel \sigma_i)$

$\{P, V_i, S_{i1}^{*}, S_{i2}^{*}, S_{i3}^{*}, A_i^{*}, PK_{Vi}^{*}, PK_{TA}, PID_i^{*}, Rep(.), VaI_i, \tau_i\}$

Stored into OBU

Fig. 8. Pseudo-identity of vehicle updates phase.

$Execute(\Pi_{Vi}^{i}, \Pi_{RSUt}^{i}, \Pi_{Vj}^{i})$ *:* All the messages exchanged between Π_{Vi}^{i}, Π_{RSUt}^{i}, and Π_{Vj}^{i} are intercepted by the adversary.

$Send(\Pi_{Vi}^{i}, \Pi_{RSUt}^{i}, m)$ *:* A sends a message m to Π_{Vi}^{i} or Π_{RSUt}^{i}, if the message is correct, Π_{Vi}^{i} or Π_{RSUt}^{i} response A.

$Reveal(\Pi_{Vi}^{i}, \Pi_{RSUt}^{i})$ *:* A can get the agreed session key through this query.

$Test(\Pi_{Vi}^{i}, r)$ *:* Which is allowed to be executed at most once. This query generates a random bit r, if $r = 1$, the real session key is returned, else, returns a random number.

$Corrupt(\Pi_{Vi}^{i})$*:* Which simulates the attack of intercepting OBU, and returns the stored information $\{P, V_i, S_{i1},$ $S_{i2}, S_{i3}, A_i, PK_{Vi}, PK_{TA}, PID_i, Rep(.), VaI_i, \tau_i\}$ in OBU.

$CorruptRSU(RSU_t)$*:* Which simulates the attack of capturing RSU, and returns the stored information $\{RID_t, P, K_{t1}, K_{t2}, Z_t, PK_{Rt}, PK_{TA}, Cha_t\}$.

Definition 3 (Freshness): A instance can be regarded as fresh if it satisfies the following conditions:

(1) Π_{Vi}^{i} and Π_{Vj}^{i} or Π_{RSUt}^{i} are in $Accept$. (2) A has not executed $Reveal(\Pi_{Vi}^{i}, \Pi_{RSUt}^{i})$ to obtain the session key.

Definition 4 (Semantic security): After executing at most once $Test(\Pi_{Vi}^{i})$ and multiple $Execute(\Pi_{Vi}^{i}, \Pi_{RSUt}^{i}, \Pi_{Vj}^{i})$, $Send(\Pi_{Vi}^{i}, \Pi_{RSUt}^{i}, m)$, and $Reveal(\Pi_{Vi}^{i}, \Pi_{RSUt}^{i})$ queries. A guesses the generated random bit r. The possibility of success is $Adv_P^A = |2\Pr[suc(A)] - 1|$, if $Adv_P^A > \eta$, the protocol is not secure, where η is sufficiently small.

B. Formal Proof

Theorem 1: The advantage of obtaining the session key in polynomial time by A *is*$Adv_P^A \leq \frac{q_{HA}^2}{2^{l_{HA}}} + \frac{(q_{SE}+q_{EX})^2}{n} + \frac{q_{SE}}{2^{l_{bio}-1}} + Adv_{PUF}^A + 2Adv_{ECDLP}^A$.

Where q_{HA}, q_{SE}, and q_{EX} represents the times of executing Hash, Send, and Execute, respectively. l_{HA}, n, and l_{bio} are the length of hash, transcripts, and biological key, respectively. The advantage of breaking PUF and ECDLP by A are Adv_{PUF}^{A} and Adv_{ECDLP}^{A}, respectively.

Proof: The games $Game_i (0 \leq i \leq 4)$ are defined to simulate the attacks launched by A. $Win_i (0 \leq i \leq 4)$ means A guesses the random bit r in the $Game_i$. The games are defined as:

$Game_0$ *:* This game simulates the real attack first launched by A. According to the definition, we get:

$$Adv_P^A = |2 \Pr [Win_0] - 1| \tag{1}$$

$Game_1$ *:* This game simulates the eavesdropping attack. A gets all the parameters $\{PID_i, A_i, D_i, PK_{Vi}, c_i, T_1, f_t, PK_{Rt}, E_t, Z_t, N_1, T_2, RID_t\}$ transmitted between Π_{Vi}^i and Π_{RSUt}^i by executing $Execute$. Then, A executes $Test(\Pi_{Vi}^i)$ and guesses if its result is the session key. However, because of the random number and ECDLP, the attacker cannot discover any valuable information about the session key from the transmission message. Therefore, we get:

$$\Pr [Win_0] = \Pr [Win_1] \tag{2}$$

$Game_2$ *:* This game simulates the collision attack on the transcripts and hash results, according to the definition of the birthday paradox, we have:

$$Pr [Win_2] - Pr [Win_1] \leq \frac{q_{HA}^2}{2^{l_{HA}+1}} + \frac{(q_{SE} + q_{EX})^2}{2n} \tag{3}$$

$Game_3$ *:* This game simulates A executes corruption attacks $Corrupt(\Pi_{Vi}^i)$ and $CorruptRSU(RSU_t)$ to obtain the stored information $\{P, V_i, S_{i1}, S_{i2}, S_{i3}, A_i, PK_{Vi}, PK_{TA}, PID_i, Rep(.), VaI_i, \tau_i\}$ in OBU and $\{RID_t, P, K_{t1}, K_{t2}, Z_t, PK_{Rt}, PK_{TA}, Cha_t\}$ in RSU, where $V_i = h(\sigma_i \parallel VaI_i)$, $S_{i1} = b_i \oplus h(\sigma_i \parallel V_i)$, $S_{i2} = SK_{Vi} \oplus h(V_i \parallel \sigma_i)$, and $S_{i3} = r_i \oplus h(VID_i \parallel \sigma_i), \sigma_i$ is the biometric key. The probability of obtaining valuable information about the vehicle is $\frac{q_{SE}}{2^{l_{bio}}}$. In addition, $Res_t = PUF(Cha_t)$, $K_{t1} = K_{RSU} \oplus h(Res_t)$, and $K_{t2} = (y_t \parallel SK_{Rt}) \oplus h(Res_t \parallel K_{t1})$. The probability of breaking PUF by A is Adv_{PUF}^A. Therefore, we have:

$$Pr [Win_3] - Pr [Win_2] \leq \frac{q_{SE}}{2^{l_{bio}}} + Adv_{PUF}^A \tag{4}$$

$Game_4$ *:* The parameters $D_i = d_i \cdot P$ and $E_t = e_t \cdot P$ are transmitted publicly, which are used for session key agreement. This game simulates that A calculates the session key according to the messages transmitted publicly. We have:

$$Pr [Win_4] - Pr [Win_3] \leq Adv_{ECDLP}^A \tag{5}$$

The session keys are generated independently and randomly. Hence, the advantage of guessing r is equal to guessing the session key. We have:

$$Pr [Win_4] = \frac{1}{2} \tag{6}$$

Combining the above formulas, we have:

$$\frac{1}{2} Adv_P^A = \left| \Pr [Win_0] - \frac{1}{2} \right|$$

$$\leq \frac{q_{HA}^2}{2^{l_{HA}+1}} + \frac{(q_{SE}+q_{EX})^2}{2n} + \frac{q_{SE}}{2^{l_{bio}}} + Adv_{PUF}^A + Adv_{ECDLP}^A$$

That is:

$$Adv_P^A \leq \frac{q_{HA}^2}{2^{l_{HA}}} + \frac{(q_{SE} + q_{EX})^2}{n} + \frac{q_{SE}}{2^{l_{bio}-1}} + Adv_{PUF}^A + 2Adv_{ECDLP}^A$$

VII. Informal Security Analysis

In this section, we discuss the security of the proposed scheme.

A. Stolen-Verifier Attack

In the proposed scheme, TA and RSU do not store the verification tables. Therefore, the proposed protocol can resist stolen-verifier attack.

B. Replay Attack

Suppose an adversary A intercepts and replays the messages sent by the vehicle i. In the authentication phase, the sent message is $\{PID_i, A_i, D_i, PK_{Vi}, c_i, T_1\}$, where $c_i = h(PID_i \parallel PK_{Vi} A_i) * SK_{TA} + a_i + SK_{Vi} + h(PID_i \parallel T_1 \parallel D_i) * d_i$. Because of the timestamp T_1 and without knowing the secret parameters SK_{TA} and SK_{Vi}, the replayed message cannot pass the authentication of RSU. In addition, A cannot calculate the secret value $SK_{it} = h(d_i \cdot E_t)$ that based on ECDLP according to the returned message $\{f_t, PK_{Rt}, E_t, Z_t, N_1, T_2, PID_i, RID_t\}$.

In the V2I announcement phase, the sent message is $\{PID_i, AC, N_2, T_4\}$, where $N_2 = h(PID_i \parallel RID_t \parallel h(SK_{it}) \parallel T_4 \parallel h(AC))$. A cannot forge the accident report or timestamp to pass the verification. Meanwhile, because of the timestamps and the random numbers, the replay attacks in the V2V broadcasting phase and vehicle pseudo-identity updating cannot work too.

C. Forgery Attack/Impersonation Attack

Suppose the adversary A impersonates the vehicle i to authenticate, announce, or broadcast. In the authentication phase, A has to forge $\{PID_i, A_i, D_i, PK_{Vi}, c_i, T_1\}$, where $c_i = h(PID_i \parallel PK_{Vi} \parallel A_i) * SK_{TA} + a_i + SK_{Vi} + h(PID_i \parallel T_1 \parallel D_i) * d_i$. A cannot forge c_i because the secret parameters SK_{TA} and SK_{Vi} are unobtainable. Meanwhile, w_i in V2V broadcast message $\{w_i, PID_i, AC, A_i, O_i, PK_{Vi}, VaI_i, T_6\}$ cannot be forged too. In V2I announcement phase, A cannot forge N_2, where $N_2 = h(PID_i \parallel RID_t \parallel h(SK_{it}) \parallel T_4 \parallel h(AC))$, $h(SK_{it})$ is unavailable. Therefore, the vehicle cannot be forged.

Suppose the adversary A captures and impersonates RSU to respond to the vehicles or upload information onto the blockchain. A has to forge $\{f_t, PK_{Rt}, E_t, Z_t, N_1, T_2, PID_i, RID_t\}$ or $\{RID_t, PID_i, K_{ViRt}, N_1, l_t, J_t, T_3\}$, where $f_t = y_t + SK_{Rt} + h(E_t \parallel RID_t \parallel T_2) * e_t$ and $l_t = SK_{Rt} + h(N_1 \parallel h(SK_{ti}) \parallel RID_t \parallel PID_i \parallel J_t \parallel T_3) * j_t$. Because of the PUF, SK_{Rt} cannot be obtained. Therefore, forging RSU cannot work.

Therefore, the proposed protocol can resist impersonation attacks.

D. OBU Intrusion Attack

The vehicle authentication parameters are usually stored in the OBU, but the OBU of the vehicle is not completely safe. Attackers can obtain stored data through the side-channel attack, etc. In some protocols [13], [16], [18], authentication parameters are stored in plain text or encrypted with passwords, but attackers can still use offline password guessing to recover the decrypted parameters. Therefore, the OBU intrusion attack will cause serious impacts, such as privacy disclosure, impersonation attacks, and message forgery.

In the proposed scheme, suppose an adversary A intrudes OBU and obtains $\{P, V_i, S_{i1}, S_{i2}, S_{i3}, A_i, PK_{Vi}, PK_{TA}, PID_i, Rep(.), VaI_i, \tau_i\}$ stored in it, where $S_{i1} = b_i \oplus h(\sigma_i \parallel V_i)$, $S_{i2} = SK_{Vi} \oplus h(V_i \parallel \sigma_i)$, $S_{i3} = r_i \oplus h(VID_i \parallel \sigma_i)$. σ_i is the biometric key of the user. When A does not have σ_i, he/she cannot obtain any valuable parameters. Therefore, even if A intrudes the OBU of the vehicle, A cannot launch any attacks.

E. RSU Captured Attack

In the authentication of VANETs, RSU is an important infrastructure for authenticating vehicles, which can verify the user's real identity, issue messages, and send the vehicle's authentication credentials to other RSUs. RSU usually stores important secret parameters for authentication. Once RSU is captured, it may lead to adverse consequences such as privacy disclosure, impersonation attacks, message forgery, illegal registration, and so on. Most protocols lack RSU protection [10], [13], [15], [16], [18], so they cannot resist RSU captured attacks.

In our scheme, each RSU stores $\{RID_t, P, K_{t1}, K_{t2}, Z_t, PK_{Rt}, PK_{TA}, Cha_t\}$, where $K_{t1} = K_{RSU} \oplus h(Res_t)$, $K_{t2} = (y_t \parallel SK_{Rt}) \oplus h(Res_t \parallel K_{t1})$, and $Res_t = PUF(Cha_t)$. PUF is the physically unclonable function. According to the characteristics of PUF, once RSU is captured or the adversary analyzes the data stored in RSU, the output of $PUF(Cha_t)$ will change. Therefore, the attacker cannot obtain $(y_t \parallel SK_{Rt})$ and K_{RSU}. In other words, capturing a RSU cannot influence other entities or the system.

F. Known-Key Security

The session key $SK_{ti} = SK_{it} = h(d_i \cdot E_t) = h(e_t \cdot D_i) = h(e_t \cdot d_i \cdot P)$, where d_i and e_t are random numbers and are different in each session. Because of the computational Diffie-Hellman problem (CDHP) and one-way hash function, an adversary cannot obtain any valuable information even if he/she gets the session key.

G. Perfect Forward Secrecy

In the proposed protocol, the session key $SK_{ti} = SK_{it} = h(d_i \cdot E_t) = h(e_t \cdot D_i) = h(e_t \cdot d_i \cdot P)$, d_i and e_t are random numbers generated in each session by the vehicle and RSU, respectively. Assuming that the adversary knows all the long-term keys, he/she cannot obtain or calculate the former or current session keys due to CDHP and hash function. The proposed protocol has perfect forward secrecy.

TABLE II
COMPARISON OF SECURITY AND PROPERTIES

Attacks/Properties	[10]	[13]	[15]	[16]	[18]	Ours
Privileged-Insider Attack	×	✓	×	×	×	✓
Off-line Password Guessing Attack	✓	-	-	×	-	✓
Impersonation Attack	×	✓	×	×	✓	✓
Replay Attack	✓	✓	✓	✓	✓	✓
Man-in-Middle Attack	✓	✓	×	✓	✓	✓
OBU Intrusion Attack	✓	×	✓	×	×	✓
RSU Captured Attack	×	×	×	×	×	✓
Stolen-Verifier Attack	✓	✓	✓	✓	×	✓
Update Asynchronous Attack	✓	✓	✓	✓	✓	✓
Identity Anonymity	✓	×	✓	✓	×	✓
Mutual Authentication	✓	×	×	✓	✓	✓
Session Key Secrecy	-	-	✓	✓	✓	✓
Know Session Key Attack	-	-	✓	✓	✓	✓
Perfect Forward Secrecy	-	-	✓	✓	✓	✓
Handover Authentication	✓	✓	✓	✓	✓	✓
Malicious Message Tracking	×	×	×	✓	✓	✓
Unlinkability	×	✓	✓	✓	×	✓

✓:Resist(Attacks)/Possess(Properties) ×:Suffer(Attacks)/No(Properties)
-: Not considered

H. Anonymity and Unlinkability

In the proposed protocol, the pseudo-identity of the vehicle is $PID_i = E_{h(SK_{TA})}(VID_i, VaI_i, r_i)$, r_i is a random number generated by TA in each pseudo-identity updating phase. The pseudo-identities of the vehicle are different and unlinkable. Only TA can recover the real identity by computing $(VID_i, VaI_i, r_i) = D_{h(SK_{TA})}(PID_i)$. The adversaries cannot obtain the real identity or trace the vehicle based on PID_i. Therefore, the proposed protocol maintains anonymity and unlinkability.

I. Desynchronization Attack

Suppose the adversary A launches attacks that interfere with vehicle pseudo-identity updates. In the pseudo-identity updating phase, the attacker interferes with the vehicle to receive the correct message $\{PID_i, M_2, T_7\}$ from TA utilizing tampering and interception, where $M_2 = E_{r_i}(VID_i, A_i^*, PID_i^*, b_i^*, r_i^*, T_7)$. Therefore, the vehicle cannot update the pseudo-identity and the data stored in the OBU. However, this will not affect the vehicle's authentication and message broadcasting, which can still be done using the vehicle's existing pseudo-identity $PID_i = E_{h(SK_{TA})}(VID_i, VaI_i, r_i)$. Likewise, the vehicle can continue to attempt to request TA to update the pseudo-identity.

J. Malicious Message Tracking

In VANETs, the malicious messages of legitimate users are often difficult to prevent, and they are generally handled by tracking the identity of the sender. However, the anonymity policy protects privacy and prevents trace attacks but it increases the difficulty of legal accountability. Some protocols cannot recover the real identity of the user who sent the malicious message [10], [13], [15].

TABLE III
COMPARISON OF COMPUTATIONAL COSTS

Scheme	First Authentication		Time(ms)	Handover Authentication		Time(ms)
	Vehicle	RSU		Vehicle	RSU	
[10]	$6T_H + 4T_{ME}$	$3T_H + 4T_{ME}$	$40.379ms$	$3T_H + 2T_{ME}$	$2T_H + T_{ME}$	$15.173ms$
[13]	$T_{AS} + T_{Sig}$	$T_H + T_{AS} + T_{Sig}$	$74.339ms$	T_H	$2T_H$	$0.057ms$
[15]	$2T_H + T_{BP} + T_{ME}$	$2T_H + T_{BP} + T_{ME}$	$99.162ms$	$T_H + T_{BP}$	$T_{BP} + T_{ME}$	$94.079ms$
[16]	$9T_H + 3T_{ECC}$	$8T_H + 3T_{ECC} + T_{Sig}$	$33.607ms$	$6T_H$	$10T_H + 2T_{Sig}$	$35.552ms$
[18]	$2T_H + 3T_{ECC} + 3T_{BP}$	$2T_H + 2T_{ECC} + 4T_{BP}$	$324.745\ ms$	$3T_H + 4T_{ECC}$	$2T_H + 2T_{ECC} + 3T_{BP}$	$149.306\ ms$
Ours	$9T_H + 5T_{ECC}$	$10T_H + 6T_{ECC}$	$29.071ms$	$3T_H$	$7T_H + 2T_{ECC}$	$5.41ms$

TABLE IV
COMPARISON OF COMMUNICATION OVERHEAD

Scheme	First Authentication		Handover Authentication		Total($bits$)
	Vehicle	RSU	Vehicle	RSU	
[10]	1524	2524	512	2024	$6584bits$
[13]	1472	2240	288	320	$4320bits$
[15]	-	$256^2 + 32$	-	$256^2 + 2 \times 256^4$	$2(256^2 + 256^4) + 32bits$
[16]	704	704	800	800	$3008bits$
[18]	736	4160	832	-	$5728bits$
Ours	1088	1440	608	-	$3136bits$

In our protocol, the temporary identity PID_i of a legal user is granted by TA, where $PID_i = E_{h(SK_{TA})}(VID_i, VaI_i, r_i)$, VID_i is the real identity of the vehicle, VaI_i is the appearance information, r_i is the random number, and SK_{TA} is TA's secret key. PID_i is combined with identity authentication parameters b_i, where $b_i = h(PID_i \parallel PK_{Vi} \parallel A_i) * SK_{TA} + a_i$. Therefore, PID_i cannot be forged and cannot be linked. When a legitimate user publishes a malicious message, TA can discover the user's real identity VID_i by decrypting PID_i.

VIII. PERFORMANCE COMPARISON

Table II is the comparison of the security and properties between the proposed scheme with some related schemes [10], [13], [15], [16], [18], which shows that ours has higher security than others.

We use the environment of Raspberry Pi 4B to simulate the computational cost of each operation of OBU and RSU in practical applications. Compared with high-performance computers, the performance of Raspberry Pi is closer to the OBU, so the results we get are more practical. The specification of Raspberry Pi 4B is quad-core 64bits ARM Cortex-A72, 1.5GHz, 2GB LPDDR4 SDARM.

Let T_H, T_{AS}, T_{Sig}, T_{ME}, T_{BP}, and T_{ECC} be the time spent by the operations of Hash (SHA-256), asymmetric encryption/decryption (RSA-1024), asymmetric encryption-based signature (DSA-1024), modular exponentiation, bilinear pairing, and elliptic curve multiplication. According to the computation result of Raspberry Pi, $T_H \approx 0.019$ ms, $T_{AS} \approx 19.536$ ms, $T_{Sig} \approx 17.624$ ms, $T_{ME} \approx 5.026$ ms, $T_{BP} \approx 44.517$ ms, $T_{ECC} \approx 2.610$ ms, respectively.

Table III and Fig. 9 show the comparison of computation costs between ours and some related protocols for VANETs, the first and handover authentication efficiencies have increased by 13.50% to 91.05% and 64.34% to 96.38%, respectively. The sum of first authentication and handover authentication is 34.481 ms, the efficiency is 37.93% higher than the existing most efficient protocol [10].

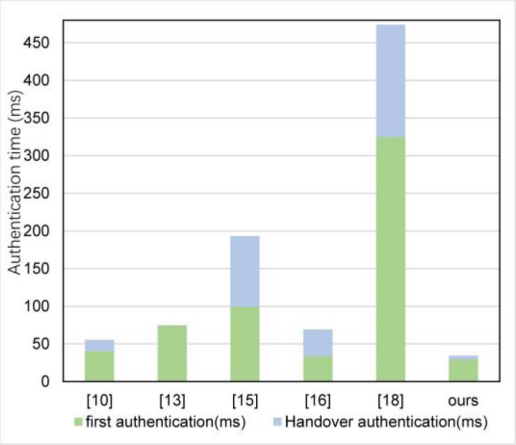


Fig. 9. The comparison of computation times.

In Table IV, we calculate and compare the communication overhead of the protocols. The lengths of the outputs of Hash (SHA-256), asymmetric encryption/decryption (RSA-1024), asymmetric encryption-based signature (DSA-1024), one block symmetric encryption (AES-128), one ECC point, and random number are 256bits, 1024bits, 1024bits, 128bits, 160bits, and 256bits, respectively. The lengths of identity, the password, and the timestamp are 32bits. According to the security standard of Diffie-Hellman key exchange, the length of large prime number p is 500 bits. In scheme [10] and [16], vehicles and Smart Cards (SC) are both used as storage devices, so we combine the storage costs in Table V. In scheme [15], because the message sent by RSU has no modulus calculation, the transmission cost is quite large. In [18], T is the number of the edge nodes (ENs) in an

TABLE V
COMPARISON OF STORAGE OVERHEAD

Scheme	Storage overhead (*bits*)	
	Vehicle&SC	RSU
[10]	2024 *bits*	1012 *bits*
[13]	2592 *bits*	-
[15]	-	-
[16]	768 *bits*	704 *bits*
[18]	257 *bits*	4160 *bits*
Ours	1920 *bits*	1248 *bits*

ENs set. To achieve better security, Yang et al. [18] suggested that $T \geq 10$, so we take T = 10 in Tables IV and V. It can be concluded that the communication overhead of our scheme is at a lower level in the relevant protocols.

The comparison of the storage overhead is shown in Table V. Because many previous protocols cannot resist RSU captured attacks and OBU intrusion attacks, in order to resist these attacks, our protocol uses biological key and PUF to protect the secret information stored in OBU and RSU, which directly leads to the storage costs of our proposed protocol is slightly higher than that of some other protocols. However, the security and efficiency of authentication protocol in VANETs are more important for driving safety. In addition, the storage cost of the proposed protocol is kept within 2Kb, which is at the same level as that of the relevant protocols less than 4KB. According to our survey of RSU and OBU products and literature [30], the storage capacity of OBU and RSU exceeds 2Gb (for example, the OBU of SPV 10 model) and 8Gb (for example, the RSU of FET1012A-C model) respectively. Therefore, the impact of storage capacity increase of no more than 1Kb on the system can be ignored.

IX. Conclusion

In this article, we first analyze the problems and challenges in the current application scenarios of VANETs and point out that the existing authentication protocols for VANETs cannot be applied to the scenarios with different RSU domains or without traffic infrastructure. In addition, few protocols are secure enough to resist RSU captured attack, OBU intrusion attack, and recover the real identity of the malicious message sender. Therefore, we propose a novel protocol to achieve V2I authentication, V2I handover authentication, and V2V broadcasting authentication, which can be used in any scenarios. PUF and biological key are used in RSU and OBU to resist the RSU captured attack and the OBU intrusion attack. The dynamic anonymity strategy is used to avoid privacy disclosure and tracking attacks. We also design an embedding strategy of pseudo-identity and vehicle feature to recover the real identity of the malicious message sender by TA. The proposed protocol is proved secure under the random oracle model. Compared with related V2I handover authentication protocols, our protocol can resist various attacks, the sum of first and handover authentication efficiencies has increased by 37.93% compared with the existing most efficient protocol. Therefore, the proposed protocol is safe and effective.

References

[1] H. Liu, H. Li, and Z. Ma, "Efficient and secure authentication protocol for VANET," in *Proc. IEEE Int. Conf. Comput. Intell. Secur.*, 2010, pp. 523–527.

[2] X. Xue and J. Ding, "LPA: A new location-based privacy-preserving authentication protocol in VANET," *Secur. Commun. Netw.*, vol. 5, no. 1, pp. 69–78, 2012.

[3] Y. Liu, Z. He, S. Zhao, and L. Wang, "An efficient anonymous authentication protocol using batch operations for VANETs," *Multimedia Tools Appl.*, vol. 75, no. 24, pp. 17689–17709, 2016.

[4] S. Wang and N. Yao, "LIAP: A local identity-based anonymous message authentication protocol in VANETs," *Comput. Commun.*, vol. 112, pp. 154–164, 2017.

[5] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on HMAC for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 8, pp. 2193–2204, Aug. 2016.

[6] C. Zhang, X. Xue, L. Feng, X. Zeng, and J. Ma, "Group-signature and group session key combined safety message authentication protocol for VANETs," *IEEE Access*, vol. 7, pp. 178310–178320, 2019.

[7] X. Li, Y. Han, J. Gao, and J. Niu, "Secure hierarchical authentication protocol in VANET," *Inst. Eng. Technol. Inf. Secur.*, vol. 14, no. 1, pp. 99–110, 2019.

[8] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 2, pp. 722–735, Mar./Apr. 2021.

[9] H. Xiong, J. Chen, Q. Mei, and Y. Zhao, "Conditional privacy-preserving authentication protocol with dynamic membership updating for VANETs," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 3, pp. 2089–2104, May/Jun. 2022.

[10] C. Wang, R. Huang, J. Shen, J. Liu, P. Vijayakumar, and N. Kumar, "A novel lightweight authentication protocol for emergency vehicle avoidance in VANETs," *IEEE Internet Things J.*, vol. 8, no. 18, pp. 14248–14257, Sep. 2021.

[11] P. Wang and Y. Liu, "SEMA: Secure and efficient message authentication protocol for VANETs," *IEEE Syst. J.*, vol. 15, no. 1, pp. 846–855, Mar. 2021.

[12] Q. Xie, P. Zheng, Z. Ding, X. Tan, and B. Hu, "Provable secure and lightweight vehicle message broadcasting authentication protocol with privacy protection for VANETs," *Secur. Commun. Netw.*, vol. 2022, pp. 1–10, 2022.

[13] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preservation in VANETs," *IEEE Access*, vol. 7, pp. 117716–117726, 2019.

[14] Z. Ma, J. Zhang, Y. Guo, Y. Liu, X. Liu, and W. He, "An efficient decentralized key management mechanism for VANET with blockchain," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5836–5849, Jun. 2020.

[15] C. Wang, J. Shen, J.-F. Lai, and J. Liu, "B-TSCA: Blockchain assisted trustworthiness scalable computation for V2I authentication in VANETs," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 3, pp. 1386–1396, Jul./Sep. 2021.

[16] S. Son, J. Lee, Y. Park, Y. Park, and A. K. Das, "Design of blockchain-based lightweight V2I handover authentication protocol for VANET," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 3, pp. 1346–1358, May/Jun. 2022.

[17] K. N. Qureshi, G. Jeon, M. M. Hassan, M. R. Hassan, and K. Kaur, "Blockchain-based privacy-preserving authentication model intelligent transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 7, pp. 7435–7443, Jul. 2023.

[18] A. Yang, J. Weng, K. Yang, C. Huang, and X. Shen, "Delegating authentication to edge: A decentralized authentication architecture for vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 2, pp. 1284–1298, Feb. 2022.

[19] Q. Mei, H. Xiong, Y. C. Chen, and C. M. Chen, "Blockchain-enabled privacy-preserving authentication mechanism for transportation CPS with cloud-edge computing," *IEEE Trans. Eng. Manage.*, early access, Apr. 14, 2022, doi: 10.1109/TEM.2022.3159311.

[20] Q. Li, D. He, Z. Yang, Q. Xie, and K.-K. R. Choo, "A Lattice-based conditional privacy-preserving authentication protocol for the vehicular Ad Hoc network," *IEEE Trans. Veh. Technol.*, vol. 71, no. 4, pp. 4336–4347, Apr. 2022.

[21] Y. Liu, W. Guo, Q. Zhong, and G. Yao, "LVAP: Lightweight V2I authentication protocol using group communication in VANETs," *Int. J. Commun. Syst.*, vol. 30, no. 16, 2017, Art. no. e3317.

[22] X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar, and N. Kumar, “A lightweight privacy-preserving authentication protocol for VANETs,” *IEEE Syst. J.*, vol. 14, no. 3, pp. 3547–3557, Sep. 2020.

[23] T. Nandy, M. Y. I. B. Idris, R. M. Noor, I. Ahmedy, and S. Bhattacharyya, “An enhanced two-factor authentication protocol for V2V communication in VANETs,” in *Proc. 3rd Int. Conf. Inf. Sci. Syst.*, 2020, pp. 171–176.

[24] P. R. Babu, A. G. Reddy, B. Palaniswamy, and S. K. Kommuri, “EV-Auth: Lightweight authentication protocol suite for dynamic charging system of electric vehicles with seamless handover,” *IEEE Trans. Intell. Veh.*, vol. 7, no. 3, pp. 734–747, Sep. 2022.

[25] D. Dolev and A. Yao, “On the security of public key protocols,” *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.

[26] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online]. Available: https://assets.pubpub.org/d8wct41f/31611263538139.pdf

[27] I.-C. Lin and T.-C. Liao, “A survey of blockchain security issues and challenges,” *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, 2017.

[28] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, “Physical unclonable functions and applications: A tutorial,” *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.

[29] M. Potkonjak and V. Goudar, “Public physical unclonable functions,” *Proc. IEEE*, vol. 102, no. 8, pp. 1142–1156, Aug. 2014.

[30] Z. Hu, Z. Zheng, T. Wang, L. Song, and X. Li, “Roadside unit caching: Auction-based storage allocation for multiple content providers,” *IEEE Trans. Wireless Commun.*, vol. 16, no. 10, pp. 6321–6334, Oct. 2017, doi: 10.1109/TWC.2017.2721938.

Qi Xie received the Ph.D. degree in applied mathematics from Zhejiang University, Hangzhou, China, in 2005. Between 2009 and 2010, he was a Visiting Scholar with the Department of Computer Science, University of Birmingham, Birmingham, U.K., and Visiting Scholar with the Department of Computer Science, City University of Hong Kong, Hong Kong, in 2012. He has authored or coauthored more than 80 research papers in international journals and conferences, such as IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. His research interests include applied cryptography, digital signatures, authentication and key agreement protocols. He was the General Co-Chair of ISPEC2012 and ACM ASIACCS2013, and a Reviewer of more than 40 international journals.

Zixuan Ding received the bachelor’s degree from Nantong University, Nantong, China, in 2020. He is currently working toward the master’s degree with Hangzhou Normal University, Hangzhou, China. He mainly studies authentication protocols and cryptography.

Wen Tang is currently working toward the M.S. degree with the School of Information Science and Technology, Hangzhou Normal University, Hangzhou, China. She mainly studies authentication and key agreement protocols.

Debiao He (Member, IEEE) received the Ph.D. degree in applied mathematics from the School of Mathematics and Statistics, Wuhan University, Wuhan, China, in 2009. He is currently a Professor with the School of Cyber Science and Engineering. He has authored or coauthored more than 100 research papers in refereed international journals and conferences, such as IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, and Usenix Security Symposium. His work has been cited more than 10 000 times at Google Scholar. His main research interests include cryptography and information security, in particular, cryptographic protocols. He was the recipient of the 2018 IEEE Systems Journal Best Paper Award and 2019 IET Information Security Best Paper Award. He serves on the Editorial Board of several international journals, such as *Journal of Information Security and Applications*, *Frontiers of Computer Science*, and *Human-centric Computing and Information Sciences*.

Xiao Tan received the B.S. and M.S. degrees from Fudan University, Shanghai, China, in 2007 and 2010, respectively, and the Ph.D. degree from the City University of Hong Kong, Hong Kong, in 2013. He is currently a Lecturer with Hangzhou Normal University, Hangzhou, China, and Researcher with the Key Laboratory of Cryptography of Zhejiang Province. His main research interests include cryptography and information security, in particular, digital signatures, authenticated key agreement, and encryption schemes.