Provably Secure and Anonymous V2I and V2V Authentication Protocol for VANETs

Qi Xie, Zixuan Ding, and Panpan Zheng

***Abstract*— Vehicular Ad-hoc Networks (VANETs) enable the connection and information exchange between vehicles and transportation infrastructure (V2I), vehicle and vehicle (V2V) to improve the safety and efficiency of the transportation system. In previous protocols, V2I and V2V authentication protocols based on bilinear pairings or identity-based cryptography are computationally heavy or difficult to protect the user's identity and privacy. In addition, lightweight authentication protocols have not achieve both V2I and V2V authentication, and may suffer from Onboard Unit (OBU) intrusion attacks, Roadside Unit (RSU) captured attacks, and difficult to track malicious vehicles. Therefore, a lightweight and anonymous V2I and V2V authentication protocol with batch verification based on Elliptic Curves Cryptography (ECC) is proposed. We use Physical Unclonable Function (PUF) and biological key to avoid RSU captured attacks and OBU intrusion attacks, design a feature embedding strategy with dynamic pseudo-identity to recover the malicious vehicle's identity by the Trusted Authority (TA). In the application test simulating the actual scenario, our protocol is more efficient because of lower overhead and batch authentication strategy. The semantic security of the protocol is formally proved under the random oracle model. The comparative analysis and security proof results show that our protocol is more superior to others.**

***Index Terms*— Authentication protocol, V2I, V2V, VANETs, privacy protection, ECC, PUF.**

I. Introduction

With the increasing level of urbanization, the number of motor vehicles is increasing rapidly. The Intelligent Transportation System (ITS) is proposed to realize the interaction between infrastructure, vehicles, and people [1]. Vehicle Ad-hoc Network is the kernel of the ITS. With the participation of the new wireless communication technology, real-time communication between vehicles and X (vehicles, people, roads, infrastructure, clouds, etc.) is realized by VANETs, which can intelligently monitor, schedule, and manage infrastructures, vehicles, and roads, providing users with a safe, comfortable, and intelligent driving experience and traffic services [2].

The main purpose of introducing VANETs is to enhance the driving experience by improving road safety, convenience and transportation efficiency, and reducing traffic accidents. However, VANETs have many challenges of security risks and privacy disclosure in ITS. In particular, with a large amount of information exchange between vehicles, vehicles and traffic infrastructure through wireless channels, they are vulnerable to passive and active attacks. At the same time, potential malicious users and malicious nodes also threaten the security of VANETs. V2I and V2V are two common communication methods in VANETs [3], so it is a challenge to design a secure and lightweight V2I and V2V authentication and session key agreement protocol.

A. Motivation and Contributions

After analyzing the existing protocols for VANETs, we found that V2I and V2V authentication protocols based on bilinear pairings or identity-based cryptography are computationally heavy or difficult to protect the user's identity and privacy. In addition, lightweight authentication protocols have not achieve both V2I and V2V authentication, and may suffer from OBU intrusion attacks, RSU captured attacks, and difficult to track malicious vehicles. Therefore, a lightweight and anonymous V2I and V2V authentication protocol with batch verification based on ECC is proposed. The main contributions of this paper are summarized as follows:

- Without the participation of TA, the proposed protocol achieves both V2I and V2V authentication and session key negotiation. Multiple V2I authentications can be batch executed, and the mutual authenticated vehicles can communicate in any RSU domain or different RSU domains or in scenarios lack of traffic infrastructure without repeated authentication.
- A feature embedding strategy with dynamic pseudo-identity is designed to recover the identity of the malicious vehicle by the TA. The update of pseudo-identity does not require the participation of third parties, thus avoiding the desynchronization attack and traceability.
- We integrate PUF and biological key into RSU and the OBU respectively to resist the RSU captured attack and the OBU intrusion attack. In addition, the semantic security of the proposed protocol is formally proved under the random oracle model. The comparative analysis shows that our protocol has low computation and communication costs.

The rest of this paper is organized as follows. Sections II and III introduce the related works and preliminaries, respectively. Section IV presents models and design goals. A lightweight and anonymous V2I and V2V authentication

Manuscript received 2 October 2022; revised 18 January 2023; accepted 3 March 2023. Date of publication 16 March 2023; date of current version 7 July 2023. This work was supported in part by the National Natural Science Foundation of China under Grant U21A20466. The Associate Editor for this article was V. Chamola. *(Corresponding author: Qi Xie.)*

The authors are with the Key Laboratory of Cryptography of Zhejiang Province, Hangzhou Normal University, Hangzhou 311121, China (e-mail: qixie68@126.com).

Digital Object Identifier 10.1109/TITS.2023.3253710

protocol for VANETs is proposed in Section V. Sections VI and VII provide the formal security proof under the random oracle model and informal security analysis, respectively. In Section VIII, we compare and analyze the proposed scheme and related schemes in terms of security, multi-request processing, and overhead. Section IX concludes this paper.

II. Related Works

IEEE1609.2 [4] uses Public Key Infrastructure (PKI) to regulate the entities' security services of Wireless Access in Vehicular Environments and the communication mechanism between entities, which can be applied to VANETs. Cui et al. [5] thought that the PKI-based system is a good choice to realize safe information exchange in VANETs, which can realize the identity authentication of entities and the verification of message integrity. Xie et al. [6] proposed a PKI-based vehicle message broadcasting authentication protocol for VANETs. Joshi et al. [7] designed an efficient scheme based on event trigger mechanism for VANETs, which uses PKI-based signature to test the validity of the broadcast beacon. Asghar et al. [8] proposed a PKI-based authentication protocol for VANETs. However, with the increase of revoked vehicles, the efficiency of finding revoked vehicles from the Certificate Revocation Lists (CRL) is relatively low. Liu et al. [9] introduced a conditional privacy protection authentication scheme based on short-term regional certificates, but the authentication process needs certificates exchange is a defect.

Since Identity-based Cryptography (IBC) can solve the problem of certificate management, in 2015, He et al. [10] proposed an identity-based authentication scheme for V2V and V2I communication. In addition, they used batch verification to process multiple requests simultaneously. However, it may reveal the original identity or privacy. Cui et al. [11] proposed a security privacy-preserving authentication scheme based on cuckoo filter. Their scheme utilizes a cuckoo filter and binary search to improve the batch verification. In addition, Qi et al. [12] proposed an identity-based authentication scheme that utilizes pseudonyms to ensure the privacy. However, IBC based authentication protocols for VANETs have the defect of the key escrow problem [13].

Designing authentication protocol based on lightweight cryptography has important application value in ITS. Recently, Liu et al. [14] proposed a lightweight V2I authentication protocol, which TA establishes a group including vehicles and RSUs, and the authentication is executed rapidly with the help of the secret key. Li et al. [15] proposed a lightweight V2I authentication protocol based on symmetric key cryptosystems. The protocol shares a secret key between the vehicle and RSU to allow them to communicate after the successful authentication with the help the TA. However, the disadvantages of the scheme are that it needs secure channels and can't realize the non-repudiation. Tan et al. [16] proposed a certificateless authentication scheme, but the computation cost is heavy because the scheme uses Chinese Remainder Theorem (CRT) and ECC. Benyamina et al. [17] proposed a lightweight authentication protocol based on the Message Authentication Code (MAC), but its computation capability is constrained using two classes for upgrading keys. Based on the self-certified public keys and Schnorr signatures, Li et al. [18] proposed a hierarchical authentication protocol for VANETs. Zhang et al. [19] proposed a privacy-preserving authentication protocol using bilinear pairings for VANETs, which supports batch authentication. Yadav and Vijayakumar [20] proposed a signature-based authentication protocol for VANETs, which provides an authentication solution for vehicle, RSU, and TA. Nath and Choudhury [21] proposed a privacy-preserving authentication scheme for VANETs, the authenticated vehicles can communicate based on the group key. To resist trace attack, the vehicle has to ask TA for pseudonym updating. Azees et al. [22] proposed a bilinear pairings based anonymous authentication scheme, including misbehaving vehicles tracking mechanism and the authentication mechanism of vehicles in different RSUs, which has high guidance value in similar articles.

III. Preliminaries

In this section, we introduce preliminaries, including ECC, PUF and Fuzzy extractor.

A. Elliptic Curve Cryptography

Let F_p be a finite field and a large prime number p is the order. E is an elliptic curve defined as: $y^2 = x^3 + ax + b \bmod p$, where $a, b \in F_p$ are constants. There is a multiplicative cyclic group G of order q, and P is the generator point. The set contains an infinity point O.

Definition 1: Elliptic curve scalar multiplication: Let $n \in Z_q^*$, then the scalar multiplication is $n \cdot P = P + P + \cdots + P$ (for a total of n times).

Definition 2: Elliptic Curve Discrete Logarithm Problem (ECDLP): There are two random points $P, Q \in G$ and $Q = x \cdot P$. It is hard to compute x from Q in the probabilistic polynomial-time t.

Definition 3: Elliptic Curve Computational Diffie-Hellman Problem (ECCDH): for the given values $\{P, a \cdot P, b \cdot P\}$, where $a, b \in Z_q^*$, there exists no probabilistic polynomial-time algorithm to compute the value $a \cdot b \cdot P$.

B. Physical Unclonable Function

PUF is a hardware function implementation circuit that depends on the characteristics of the chip. It has uniqueness and randomness. By extracting the inevitable process parameter deviation in the process of chip manufacturing, it realizes the only corresponding function between the challenge signal and the response signal. A basic difference between PUF and traditional technology is that PUF is essentially not affected by reverse engineering technology. That is, when the chip encrypted by PUF is analyzed by an attacker, the response of PUF will change, so the encrypted information cannot be obtained.

PUF is a circuit operation at the hardware level, and the time cost of a single operation is generally less than 1 nanosecond (ns). In the case of equal computing power, the

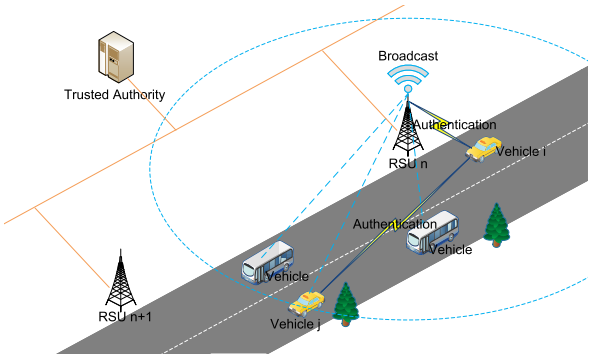

Fig. 1. System model.

cost of a single hash operation is at the millisecond (ms) level, which is 1000 times that of PUF. Therefore, the computation and communication costs of PUF are usually ignored.

In this paper, PUF is used in RSUs to protect the stored message. Even if the attacker captures RSU, he cannot analyze any information from the RSU. Therefore, our protocol can resist RSU captured attacks.

C. Fuzzy Extractor

This function allows the input with a certain noise, and the outputs obtained from the inputs within a threshold is the same, so it can be used for the extraction and recovery of the biological key.

The generation of the biological key can be described as $(\sigma, \tau) = Gen\,(bio)$, where bio is the biological information and $Gen\,(.)$ is generating function, σ is the biological key, τ is the recovery parameter to be saved. The recovery process of the biological key is $\sigma = Rep\left(bio', \tau\right)$, $Rep\,(.)$ is the recovery function, and there is a certain error between the new bio-information bio' and the original bio.

IV. Models and Design Goals

A. System Model

In this paper, an ECC-based anonymous authentication protocol was proposed for VANET. The system model is shown in Fig.1, which contains the TA, RSUs and vehicles.

TA is fully trusted with powerful computation and storage resources, which realizes the generation of system parameters and registrations for RSUs and vehicles. TA is the only entity that can reveal the real identity of a vehicle to track malicious vehicles with the assistance of RSUs once a dispute happens.

RSUs are roadside units as transportation infrastructure, which can verify and anonymously authenticate the message from vehicles. RSUs are independent of each other for security in the face of RSU captured and compromised. RSUs are connected to the TA for malicious vehicle tracking.

Without the help of TA, vehicles can authenticate with RSU mutually and information exchange safely, and RSU can batch authenticate vehicles. In addition, vehicles in the same RSU domain can authenticate each other, and can communicate in any RSU domain or different RSU domains or in scenarios without traffic infrastructure without repeated authentication.

B. Threat Model

According to Dolev-Yao threat model [23] and the security survey on VANETs [24], we define the threat model is as follows.

- The adversary A can eavesdrop, intercept, modify or delete the messages transmitted publicly.
- A could be a registered vehicle or internal attacker, which means that the attacker may send malicious messages or launch internal attack.
- A can launch the side-channel attacks on OBU and RSU, but it is difficult to obtain biological keys and crack PUF.
- The trusted authority (TA) is fully trusted and considered to have adequate storage space for vehicle data set, its secret key is secure.

C. Design Goals

1) The proposed protocol can realize both V2I and V2V authentication, establish session key and communication safely. The authentication process must be efficient, and V2I authentication supports batch verification.
2) The privacy of vehicle needs to be protected, and the update of the temporary identity of the vehicle does not require the participation of third parties.
3) The proposed protocol can resist various known attacks including RSU captured attacks and OBU intrusion attacks, and can achieve several known advantages, such as perfect forward secrecy, session key secrecy, etc.
4) In the case of dispute, the identity of the malicious message sender can be recovered by TA.

V. The Proposed Scheme

The proposed scheme consists of seven phases: (1) System initialization. (2) RSU registration. (3) Vehicle registration. (4) V2I authentication and key agreement. (5) V2V authentication and key agreement. (6) Pseudo-identity update. (7) Malicious vehicle tracing. The notations used in our protocol is shown in Table I.

A. System Initialization

TA selects an elliptic curve $E(GF_q)$ and a base point P, then selects its private key $x_c \in Z_q^*$, and calculates $X_c = x_c \cdot P$ as its public key. TA selects the symmetric encryption/decryption function $E_{SK}(.)/D_{SK}(.)$ and one-way hash functions $h(.)$. Finally, TA keeps x_c secret and publishes the system parameters $\{q, P, E_{SK}(.), D_{SK}(.), X_c, h(.)\}$.

B. RSU Registration

Step 1: RSU_i selects its identity ID_{Ri} and secret parameter x_{Ri}, then calculates $X_{Ri} = x_{Ri} \cdot P$, and sends $\{X_{Ri}, ID_{Ri}\}$ to the TA via a secure channel.

Step 2: Then TA verifies ID_{Ri}'s legitimacy and uniqueness and selects a random integer a_{Ri} and calculates

$$A_{Ri} = a_{Ri} \cdot P,$$
$$\text{and } C_{Ri} = h(ID_{Ri} \parallel X_{Ri} \parallel A_{Ri}) x_c + a_{Ri},$$

then sends $\{A_{Ri}, C_{Ri}\}$ to RSU_i via a secure channel.

TABLE I
NOTATIONS

Notations	Description
TA	Trusted-authority
$Vehicle_j$	j-th vehicle
RSU_t	t-th roadside unit
RID_t	Unique identity of RSU_t
V_{Ni}	Real identity of $Vehicle_i$
TV_{Ni}	Pseudonym identity of $Vehicle_i$
P	The generator of the elliptic curve
x_c, X_c	Private and public key of TA, $X_c = x_c \cdot P$
x_{Ri}, X_{Ri}	Private and public key of RSU_i, $X_{Ri} = x_{Ri} \cdot P$
a_{Ri}, a_{ri}, d_{vi}	Random integers
SK_{viri}	The session key between Vehicle and RSU
SK_{vivj}	The session key between Vehicles
T_1, T_2, T_3, T_4	Timestamps
$h(.)$	Hash function
$\|$	Concatenation
$\oplus$	XOR operation
$\triangle T$	Time threshold
$E_{SK()}/D_{SK()}$	Symmetric encryption/decryption function
$PUF()$	Physical unclonable function
Cha_i, Res_i	The challenge and response of the $PUF()$
Bio_i	The biological information of user
$Gen(.), Rep(.)$	The generation and reproduction functions of Fuzzy extractor
α_i, β_i	Biological key and reproduction parameter

Step 3: RSU_i verifies if $C_{Ri} \cdot P = h(ID_{Ri} \parallel X_{Ri} \parallel A_{Ri}) \cdot X_c + A_{Ri}$. If not, abort it, else RSU_i generates a challenge Cha_i and computes

$$Res_i = PUF(Cha_i),$$
$$\text{and } Sx = Res_i \oplus x_{Ri},$$

then stores $\{Sx, X_{Ri}, ID_{Ri}, C_{Ri}, A_{Ri}, Cha_i, PUF()\}$. The steps are shown in Fig. 2.

C. Vehicle Registration

Step 1: $Vehicle_i$ sends its real identity V_{Ni} and the registration request to TA via a secure channel.

Step 2: On receiving the request from $Vehicle_i$, TA verifies the legitimacy and uniqueness of the identity and generates a random integer a_{vi}, then computers

$$A_{vi} = a_{vi} \cdot P,$$
$$\text{and } C_{vi} = h(V_{Ni} \parallel A_{vi}) x_c + a_{vi}.$$

TA stores $\{A_{vi}, C_{vi}\}$ into the smart card SC and sends it to $Vehicle_i$ via the secure channel. In addition, TA stores $\{V_{Ni}, h(V_{Ni})^{-1} A_{vi}\}$ in Vehicle's Identity Mapping (VIM) table.

Step 3: After obtaining SC, $Vehicle_i$ verifies if $C_{vi} \cdot P = h(V_{Ni} \parallel A_{vi}) X_c + A_{vi}$. If not, abort it, otherwise $Vehicle_i$ generates a temporary identity TV_{Ni}, and computes

$$t = h(TV_{Ni})(h(V_{Ni} \parallel A_{vi}))^{-1},$$
$$C_{vi}^* = tC_{vi},$$
$$\text{and } D_{vi} = tA_{vi}.$$

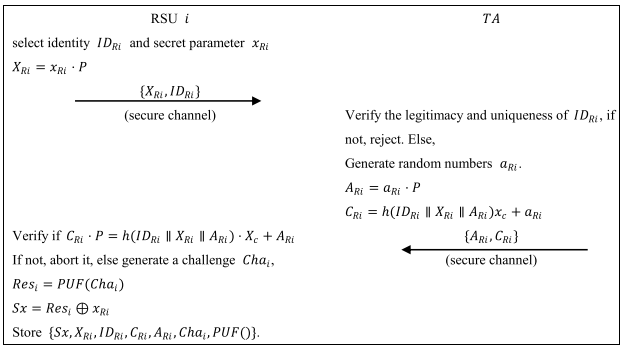

Fig. 2. RSU registration.

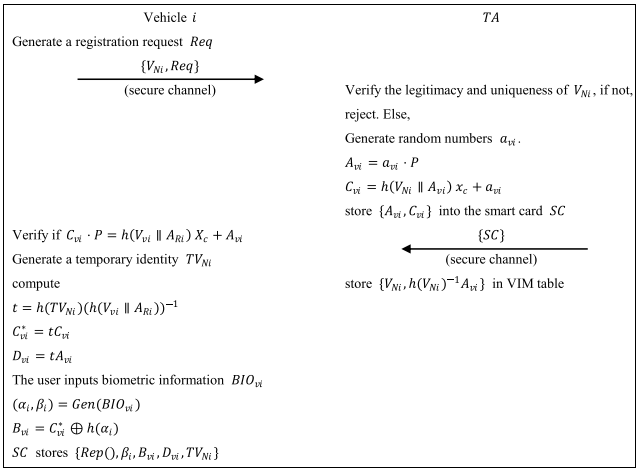

Fig. 3. Vehicle registration.

Then the user inputs the biometric information BIO_{vi} and calculates

$$(\alpha_i, \beta_i) = Gen(BIO_{vi}),$$
$$\text{and } B_{vi} = C_{vi}^* \oplus h(\alpha_i),$$

then replaces A_{vi} and C_{vi} with D_{vi} and B_{vi}. That is, SC contains $\{Rep(), \beta_i, B_{vi}, D_{vi}, TV_{Ni}\}$. The steps are shown in Fig. 3.

D. V2I Authentication and Key Agreement

Step 1: When $Vehicle_i$ enters the range of RSU_i, it receives the broadcast message $\{ID_{Ri}, X_{Ri}, C_{Ri}, A_{Ri}\}$ from RSU_i. $Vehicle_i$ verifies whether $C_{Ri} \cdot P = h(ID_{Ri} \parallel X_{Ri} \parallel A_{Ri}) \cdot X_c + A_{Ri}$. If not, reject it. Otherwise, the user inserts the smart card SC, inputs the biometric information BIO_{vi}^*, and generates a random number d_{vi} and a timestamp T_1, then $Vehicle_i$ calculates

$$\alpha_i = Rep\left(BIO_{vi}^*, \beta_i\right),$$
$$C_{vi}^* = B_{vi} \oplus h(\alpha_i),$$
$$C_{vi1} = d_{vi} \cdot P,$$
$$C_{vi2} = C_{vi}^* + d_{vi},$$
$$\text{and } C_{vi3} = h(d_{vi} \cdot X_{Ri} \parallel T_1) \oplus TV_{Ni}.$$

$Vehicle_i$ sends $\{D_{vi}, C_{vi1}, C_{vi2}, C_{vi3}, T_1\}$ to RSU_i.

Step 2: After receiving the message $\{D_{vi}, C_{vi1}, C_{vi2}, C_{vi3}, T_1\}$, RSU_i first verifies the freshness of T_1,

then calculates

$$x_{Ri} = PUF(Cha_i) \oplus Sx,$$
$$\text{and } TV_{Ni} = C_{vi3} \oplus h(x_{Ri} \cdot C_{vi1} \parallel T_1).$$

then verifies if $C_{vi2} \cdot P = h(TV_{Ni}) \cdot X_c + C_{vi1} + D_{vi}$, where

$$\begin{aligned} &C_{vi2} \cdot P \\ &= C^*_{vi} \cdot P + d_{vi} \cdot P \\ &= t \cdot C_{vi} \cdot P + d_{vi} \cdot P \\ &= t \cdot h(V_{Ni}) \cdot x_c \cdot P + t \cdot a_{vi} \cdot P + C_{vi1} \\ &= h(TV_{Ni}) \cdot X_c + t \cdot A_{vi} + C_{vi1} \\ &= h(TV_{Ni}) \cdot X_c + D_{vi} + C_{vi1}. \end{aligned}$$

If not, RSU_i rejects it. Otherwise, RSU_i generates a random number d_{Ri} and a timestamp T_2, then calculates

$$C_{Ri1} = d_{Ri} \cdot P,$$
$$SK_{rivi} = h(d_{Ri} \cdot C_{vi1} \parallel C_{vi1} \parallel C_{Ri1} \parallel TV_{Ni} \parallel ID_{Ri}),$$
$$\text{and } R_{vi} = h(SK_{rivi} \parallel TV_{Ni} \parallel ID_{Ri} \parallel T_2).$$

RSU_i sends the message $\{TV_{Ni}, C_{Ri1}, R_{vi}, T_2\}$ to $Vehicle_i$.

RSU_i utilizes batch verification to check a large number of messages from many vehicles at a simultaneous, if the equation $\left(\sum_{i=1}^{n} C_{vi2}\right) \cdot P = (\sum_{i=1}^{n} h_1(TV_{Ni})) \cdot X_c + \sum_{i=1}^{n} (D_{vi} + C_{vi1})$ holds, RSU_i can calculate the session key between RSU_i and $Vehicle_i$.

The correctness of the above equation can be proved by:

$$\begin{aligned} &\left(\sum_{i=1}^{n} C_{vi2}\right) \cdot P \\ &= \left(\sum_{i=1}^{n} C^*_{vi}\right) \cdot P + \sum_{i=1}^{n} d_{vi} \cdot P \\ &= \left(\sum_{i=1}^{n} t \cdot C_{vi}\right) \cdot P + \sum_{i=1}^{n} d_{vi} \cdot P \\ &= (\sum_{i=1}^{n} t \cdot h(V_{Ni}) \cdot x_c) \cdot P \\ &\quad + (\sum_{i=1}^{n} t \cdot a_{vi}) \cdot P + \sum_{i=1}^{n} C_{vi1} \\ &= (\sum_{i=1}^{n} h(TV_{Ni})) \cdot X_c + \sum_{i=1}^{n} t \cdot A_{vi} + \sum_{i=1}^{n} C_{vi1} \\ &= (\sum_{i=1}^{n} h(TV_{Ni})) \cdot X_c + \sum_{i=1}^{n} (D_{vi} + C_{vi1}). \end{aligned}$$

Step 3: On receiving the message $\{TV_{Ni}, C_{Ri1}, R_{vi}, T_2\}$, $Vehicle_i$ verifies the freshness of T_2, and calculate $SK_{viri} = h(d_{vi} \cdot C_{Ri1} \parallel C_{vi1} \parallel C_{Ri1} \parallel TV_{Ni} \parallel ID_{Ri})$ and verifies if $h(SK_{viri} \parallel TV_{Ni} \parallel ID_{Ri} \parallel T_2) = R_{vi}$. If not, $Vehicle_i$ rejects it. Otherwise, authentication is completed. The steps are shown in Fig. 4.

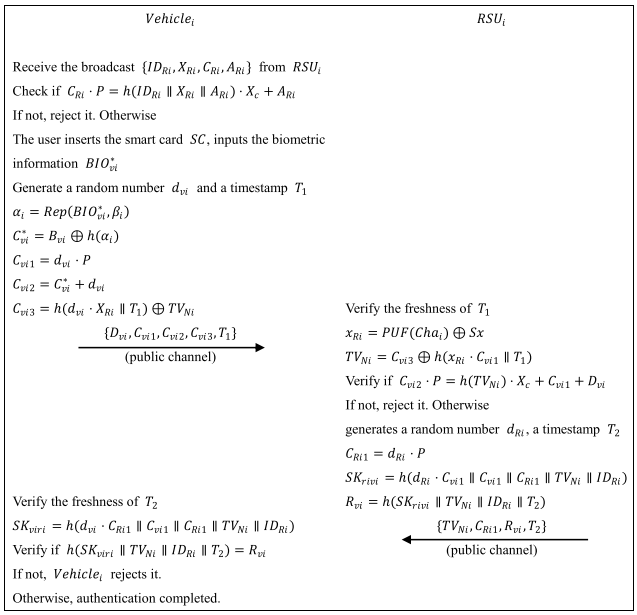

Fig. 4. V2I authentication and key agreement.

E. V2V Authentication and Key Agreement

RSU_i broadcasts the temporary identity $\{TV_{N1}, TV_{N2}, \cdots\cdots, TV_{Nn}\}$ of all authenticated vehicles in the public region area of RSU_i, $Vehicle_i$ and $Vehicle_j$ in the same RSU_i domain can authenticate each other and establish session key, then they can communicate in any RSU domain or no traffic infrastructure without repeated authentication. The steps are shown in Fig. 5.

Step 1: If $Vehicle_i$ wants to communicate with $Vehicle_j$, The $Vehicle_i$ calculates $D_1 = E_{SK_{viri}}(C_{vi1}, TV_{Ni}, TV_{Nj}, T_3)$ where T_3 is a timestamp. Then sends $\{C_{vi1}, D_1, T_3\}$ to RSU_i.

Step 2: After receiving the message $\{C_{vi1}, D_1, T_3\}$, RSU_i verifies the freshness of T_3, calculates $(C'_{vi1}, TV_{Ni}, TV_{Nj}, T'_3) = D_{SK_{rivi}}(D_1)$. If $C'_{vi1} \neq C_{vi1}$ or $T'_3 \neq T_3$, reject it. Otherwise RSU_i generates a timestamp T_4, and calculates

$$D_2 = E_{SK_{rivi}}(TV_{Ni}, TV_{Nj}, C_{Vj1}, T_4),$$
$$\text{and } D_3 = E_{SK_{riv_j}}(TV_{Nj}, TV_{Ni}, C_{Vi1}, T_4).$$

Then RSU_i sends $\{D_2, T_4, TV_{Ni}\}$ to $Vehicle_i$ and $\{D_3, T_4, TV_{Nj}\}$ to $Vehicle_j$.

Step 3: On receiving $\{D_2, T_4, TV_{Ni}\}$, $Vehicle_i$ first verifies the freshness of T_4, then calculates $(TV_{Ni}, TV_{Nj}, C_{vj1}, T_4) = D_{SK_{viri}}(D_2)$. If TV_{Ni}, TV_{Nj}, and T_4 are wrong, $Vehicle_i$ rejects it, otherwise generates a timestamp T_5, and calculates

$$SK_{vivj} = h(d_{vi} \cdot C_{vj1} \parallel TV_{Ni} \parallel TV_{Nj} \parallel C_{vi1} \parallel C_{vj1}),$$
$$\text{and } C_{vivj} = h(SK_{vivj} \parallel TV_{Ni} \parallel TV_{Nj} \parallel C_{vi1} \parallel C_{vj1} \parallel T_5).$$

Then $Vehicle_i$ sends $\{C_{vivj}, TV_{Ni}, TV_{Nj}, T_5\}$ to $Vehicle_j$.

On receiving $\{D_3, T_4, TV_{Nj}\}$, $Vehicle_j$ first verifies the freshness of T_4, then calculates $(TV_{Nj}, TV_{Ni}, C_{vi1}, T_4) = D_{SK_{vjri}}(D_3)$. If TV_{Nj}, TV_{Ni}, and T_4 are wrong, $Vehicle_j$ rejects it, otherwise generates a timestamp T_6, and calculates

$$SK_{vjvi} = h(d_{vj} \cdot C_{vi1} \parallel TV_{Ni} \parallel TV_{Nj} \parallel C_{vi1} \parallel C_{vj1}),$$
$$\text{and } C_{vjvi} = h(SK_{vjvi} \parallel TV_{Ni} \parallel TV_{Nj} \parallel C_{vi1} \parallel C_{vj1} \parallel T_6).$$

Then $Vehicle_j$ sends $\{C_{vjvi}, TV_{Nj}, TV_{Ni}, T_6\}$ to $Vehicle_i$.

Step 4: $Vehicle_i$ checks the freshness of T_6 and verifies if $h(SK_{vivj} \parallel TV_{Ni} \parallel TV_{Nj} \parallel C_{vi1} \parallel C_{vj1} \parallel T_6) = C_{vjvi}$. At the same time, $Vehicle_j$ checks the freshness of T_5 and verifies if $h(SK_{vjvi} \parallel TV_{Ni} \parallel TV_{Nj} \parallel C_{vi1} \parallel C_{vj1} \parallel T_5) = C_{vivj}$. If correct, the session key between $Vehicle_i$ and $Vehicle_i$ is $SK_{vivj} = SK_{vjvi}$.

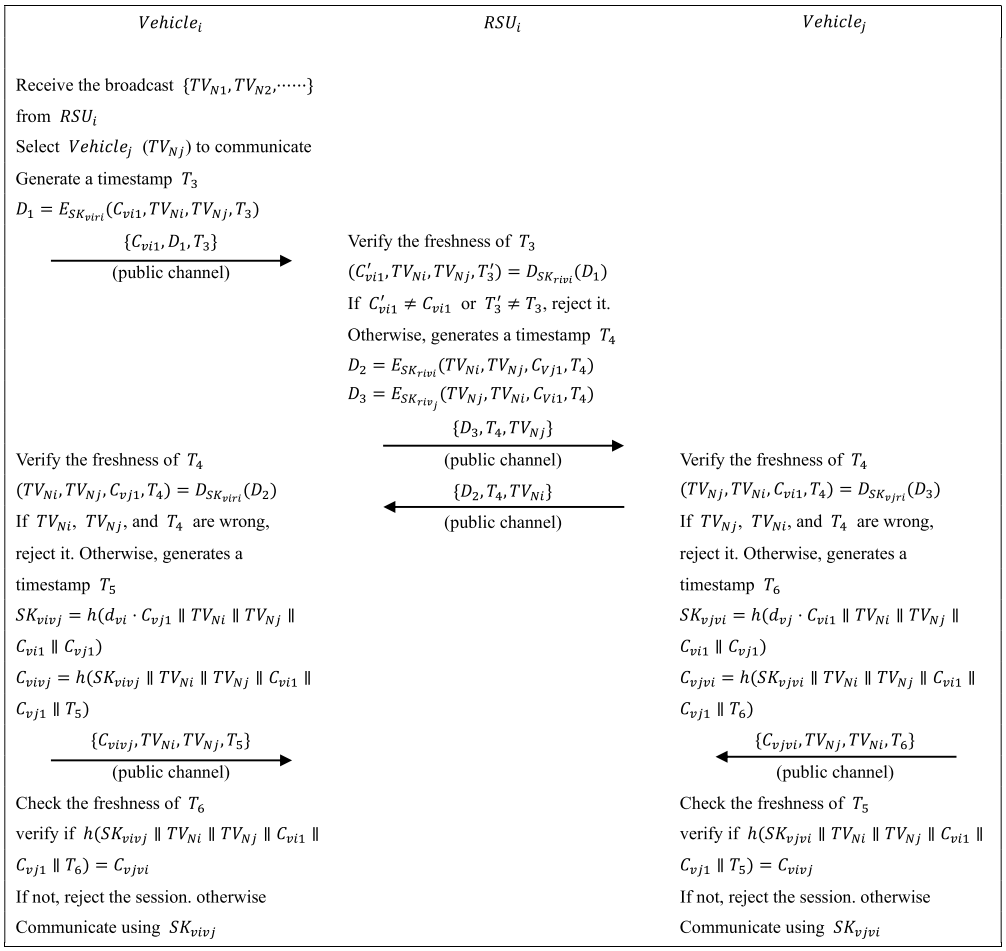

Fig. 5. V2V authentication and key agreement.

F. Pseudo-Identity Update

To resist identity tracking attacks and protect vehicle privacy, the temporary pseudo-identity of the vehicle can be updated. The vehicle generates a new temporary identity TV_{Ni}^{new}, and computes

$$D_{vi}^{new} = h(TV_{Ni}^{new})(h(TV_{Ni}))^{-1} D_{vi},$$
$$\text{and } B_{vi}^{new} = h(TV_{Ni}^{new})(h(TV_{Ni}))^{-1} B_{vi}.$$

The smart card SC replaces B_{vi}, D_{vi}, and TV_{Ni} with B_{vi}^{new}, D_{vi}^{new}, and TV_{Ni}^{new}, respectively.

G. Malicious Vehicle Tracing

In the proposed authentication protocol, the vehicles use pseudonyms to realize anonymous privacy preservation. If there is a vehicle sending malicious messages, TA can expose its real identity. The steps are as follows:

RSU calculates $TK = h(TV_{Ni})^{-1} D_{vi}$ and sends it to TA, where $TK = h(TV_{Ni})^{-1} D_{vi} = h(V_{Ni})^{-1} A_{vi}$, TA can realize the conditional privacy preservation of VANET according to lookup its VIM to find the real identity of the vehicle.

VI. Formal Security Proof

We use the random oracle model to formally prove the semantic security of the proposed protocol.

A. Definition of the Random Oracle Model

Definition 4: (Participants & partnering): The participants are composed of Vehicle (V) and Roadside Unit (RSU). In the i-th instance, the participants are denoted as $In_{Vi}^i(In_{Vj}^i)$, and In_{RSUi}^i, respectively. The state $Accept$ represents that an oracle receives a correct message.

If two oracles are in $Accept$ and the session keys have been agreed, the oracles get their session identities and participant identities. The oracles can be considered partners if the following conditions are satisfied.

1) Their session keys are the same.
2) Their session identities are the same.
3) The participant identity is equal to each other's identity.

Definition 5: (Queries): the queries simulate the capabilities of attackers.

$Execute(In_{Vi}^i, In_{RSUi}^i, In_{Vj}^i)$: All the messages transmitted openly can be intercepted by the adversary A.

$Send(In_{Vi}^i, In_{RSUi}^i, In_{Vj}^i, m)$:

A forges and sends the message m to In_{Vi}^i, In_{RSUi}^i, or In_{Vj}^i, if m is correct, In_{Vi}^i, In_{RSUi}^i, or In_{Vj}^i responses A.

$Reveal(In_{Vi}^i, In_{RSUi}^i, In_{Vj}^i)$:

A can get the session keys between In_{Vi}^i, In_{RSUi}^i, and In_{Vj}^i.

$Test(In^i_{Vi}, In^i_{RSUi}, In^i_{Vj}, r)$: This query is allowed to be executed at most once. which generates a random bit r, if $r = 1$, the real session key is returned, else, return a random number.

$Corrupt(In^i_{Vi}, In^i_{Vj})$: Which simulates the side-channel attack on the smart card, and returns the stored information $\{Rep(), \beta_i, B_{vi}, D_{vi}, TV_{Ni}\}$.

$CorruptRSU(In^i_{RSUi})$: Which simulates the attack of capturing RSU, and returns the stored information $\{Sx, X_{Ri}, ID_{Ri}, C_{Ri}, A_{Ri}, Cha_i, PUF()\}$.

Definition 6: (Freshness): An instance can be regarded as fresh if it satisfies:

1) In^i_{Vi}, In^i_{RSUi}, and In^i_{Vj} are in $Accept$.
2) The query $Reveal(In^i_{Vi}, In^i_{RSUi}, In^i_{Vj})$ has not been executed.
3) The queries $Corrupt(In^i_{Vi}, In^i_{Vj})$ and $CorruptRSU(In^i_{RSUi})$ have been executed at most once.

Definition 7: (Semantic security): A is allowed to execute at most once $Test(In^i_{Vi}, In^i_{RSUi}, In^i_{Vj}, r)$ and multiple other queries to determine the correctness of the return value of $Test(In^i_{Vi}, In^i_{RSUi}, In^i_{Vj}, r)$. That is A guesses the random bit r generated by $Test$. The possibility is $Adv^A_P = |2Pr[suc(A)] - 1|$, $Adv^A_P < \eta$ represents the protocol is secure, where η is sufficiently small.

B. Formal Proof

Theorem 1: The advantage of obtaining the session key in polynomial time by A is $Adv^A_P \le \frac{q^2_{HA}}{2^{l_{HA}}} + \frac{(q_{SE}+q_{EX})^2}{n} + \frac{q_{SE}}{2^{l_{bio}-1}} + 2q_{SE}Adv^A_{PUF} + 2Adv^A_{ECDLP}$.

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^A_{PUF} and Adv^A_{ECDLP}, respectively.

Proof: The games $Game_i (0 \le i \le 4)$ are defined to simulate the attacks launched by A. $Win_i (0 \le i \le 4)$ 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:

$$Adv^A_P = |2\ Pr[Win_0] - 1| \tag{1}$$

$Game_1$: This game simulates the eavesdropping attack. A gets all the messages transmitted publicly. Then, A guesses the random bit r. However, because of the ECDLP, the attacker cannot judge the association between the captured messages and the session keys. 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, the probability of hash collision is less than $\frac{q^2_{HA}}{2^{l_{HA}+1}}$, and the collision probability of other transcripts is less than $\frac{(q_{SE}+q_{EX})^2}{2n}$. Therefore, we have:

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

$Game_3$: This game simulates A executes $Corrupt(In^i_{Vi}, In^i_{Vj})$ and $CorruptRSU(In^i_{RSUi})$ to obtain the stored information $\{Rep(), \beta_i, B_{vi}, D_{vi}, TV_{Ni}\}$ in the smart card and $Sx, X_{Ri}, ID_{Ri}, C_{Ri}, A_{Ri}, Cha_i, PUF()\}$ in RSU, where $B_{vi} = C^*_{vi} \oplus' h(\alpha_i)$, α_i is the biometric key, $Sx = PUF(Cha_i) \oplus x_{Ri}$. If Awants to obtain the valuable parameters, he must guess α_i or break PUF. Suppose the probability of breaking PUF by A is Adv^A_{PUF}. Therefore, we have:

$$Pr[Win_3] - Pr[Win_2] \le q_{SE}(\frac{1}{2^{l_{bio}}} + Adv^A_{PUF}) \tag{4}$$

$Game_4$:

A can obtain $C_{vi1} = d_{vi} \cdot P$, $C_{Ri1} = d_{Ri} \cdot P$, and $C_{vj1} = d_{vj} \cdot P$ publicly, which are used for session keys agreements. This game simulates that A calculates the session keys according to the transcripts. We have:

$$Pr[Win_4] - Pr[Win_3] \le Adv^A_{ECDLP} \tag{5}$$

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:

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

$$\le \frac{q^2_{HA}}{2^{l_{HA}+1}} + \frac{(q_{SE}+q_{EX})^2}{2n} + \frac{q_{SE}}{2^{l_{bio}}} + q_{SE}Adv^A_{PUF} + Adv^A_{ECDLP},$$

$$Adv^A_P \le \frac{q^2_{HA}}{2^{l_{HA}}} + \frac{(q_{SE}+q_{EX})^2}{n} + \frac{q_{SE}}{2^{l_{bio}-1}} + 2q_{SE}Adv^A_{PUF} + 2Adv^A_{ECDLP}.$$

VII. Informal Security Analysis

A. Stolen-Verifier Attack

TA stores $\{V_{Ni}, h(V_{Ni})^{-1}A_{vi}\}$ for mapping vehicle's real identities, where V_{Ni} is the vehicle's real identity, $A_{vi} = a_{vi} \cdot P$ is a public parameter. The leakage of the mapping table cannot affect the security of the proposed protocol.

B. Replay Attack

The timestamps and the random numbers are combined with the public messages. The replayed messages cannot pass the verification of freshness and integrity. The proposed protocol can resist the replay attack.

C. Forgery Attack/Impersonation Attack

Suppose an adversary impersonates the vehicles to authenticate with RSU and forges the message $\{D_{vi}, C_{vi1}, C_{vi2}, C_{vi3}, T_1\}$, where $C_{vi1} = d_{vi} \cdot P$, $C_{vi2} = C^*_{vi} + d_{vi} = B_{vi} \oplus' h(\alpha_i) + d_{vi} = h(TV_{Ni})(h(V_{Ni} \parallel A_{vi}))^{-1}(h(V_{Ni} \parallel A_{vi})x_c + a_{vi}) + d_{vi} = h(TV_{Ni})x_c + h(TV_{Ni})(h(V_{Ni} \parallel A_{vi}))^{-1}a_{vi} + d_{vi}$, $C_{vi3} = h(d_{vi} \cdot X_{Ri} \parallel T_1) \oplus' TV_{Ni}$, x_c is TA's secret key, a_{vi} and d_{vi} are random numbers, $A_{vi} = a_{vi} \cdot P$, V_{Ni} and TV_{Ni} are the vehicle's identity and pseudo-identity, $D_{vi} = tA_{vi} = h(TV_{Ni})(h(V_{Ni} \parallel A_{vi}))^{-1}A_{vi}$ and α_i is the biometric key. TV_{Ni} will be updated after authentication. Therefore, the adversary cannot forge or replay TV_{Ni} and calculate C_{vi2} without knowing TA's secret key x_c.

Suppose the adversary impersonates the vehicle to authenticate with the vehicle, he/she forges $\{C_{vi1}, D_1, T_3\}$ or $\{C_{vjvi}, TV_{Nj}, TV_{Ni}, T_6\}$, where $C_{vi1} = d_{vi} \cdot P$, $D_1 = E_{SK_{viri}}(C_{vi1}, TV_{Ni}, TV_{Nj}, T_3)$, and $C_{vjvi} = h(SK_{vjvi} \parallel TV_{Ni} \parallel TV_{Nj} \parallel C_{vi1} \parallel C_{vj1} \parallel T_6)$. The agreements of the session keys SK_{viri} and SK_{vjvi} are based on ECDLP, the session keys cannot be obtained by the adversary without knowing the secret random numbers. Therefore, C_{vjvi} and D_1 cannot be forged.

Suppose the adversary impersonates the RSU to authenticate vehicles, he/she forges $\{TV_{Ni}, C_{Ri1}, R_{vi}, T_2\}$, where $C_{Ri1} = d_{Ri} \cdot P$, $R_{vi} = h(SK_{rivi} \parallel TV_{Ni} \parallel ID_{Ri} \parallel T_2)$, TV_{Ni} is vehicle's pseudo-identity and $TV_{Ni} = C_{vi3} \oplus' h(x_{Ri} \cdot C_{vi1} \parallel T_1)$, x_{Ri} is RSU's secret key and $x_{Ri} = PUF(Cha_i) \oplus Sx$. Because of PUF, x_{Ri} cannot be obtained by the adversary, therefore, the message cannot be forged by the adversary.

D. Smart Card Lost (OBU Intrusion) Attack

The smart card stores $\{Rep(), \beta_i, B_{vi}, D_{vi}, TV_{Ni}\}$, where $Rep()$ is the reproduction functions of fuzzy extractor, β_i is the reproduction parameter, $B_{vi} = C^*_{vi} \oplus' h(\alpha_i)$, α_i is the biometric key, $D_{vi} = tA_{vi} = h(TV_{Ni})(h(V_{Ni} \parallel A_{vi}))^{-1}A_{vi}$, the valuable parameter C^*_{vi} cannot be obtained by the adversary without knowing α_i. Therefore, even if the adversary obtains the stored information in the smart card, he/she cannot launch attacks based on it.

E. RSU Captured Attack

RSU stores $\{Sx, X_{Ri}, ID_{Ri}, C_{Ri}, A_{Ri}, Cha_i, PUF()\}$, where $Sx = PUF(Cha_i) \oplus x_{Ri}$, $X_{Ri} = x_{Ri} \cdot P$, ID_{Ri} is RSU's identity, $C_{Ri} = h(ID_{Ri} \parallel X_{Ri} \parallel A_{Ri})x_c + a_{Ri}$, $A_{Ri} = a_{Ri} \cdot P$, Cha_i is the challenge of the PUF. Even if a RSU is captured by the adversary, he/she cannot obtain the secret key x_{Ri} and influence other entities.

F. Known-Key Security

The session keys $SK_{rivi} = SK_{viri} = h(x_{Ri} \cdot d_{vi} \cdot P \parallel C_{vi1} \parallel C_{Ri1} \parallel TV_{Ni} \parallel ID_{Ri})$, $SK_{vivj} = SK_{vjvi} = h(d_{vi} \cdot d_{vj} \cdot P \parallel TV_{Ni} \parallel TV_{Nj} \parallel C_{vi1} \parallel C_{vj1})$. The agreements of the session keys are based on the ECDLP and one-way hash function. Even if the adversary obtains the session keys, he cannot recover any long-term keys.

TABLE II
COMPARISON OF SECURITY AND PROPERTIES

Scheme		[15]	[18]	[19]	[20]	[21]	Ours
Techniques		$T_{3,4}$	$T_{2,3,8}$	$T_{2,3,4,8}$	$T_{2,3,4,8}$	$T_{2,3,4,5,8}$	$T_{2,3,4,5,6,7,8}$
Attacks/ Properties	A_1	×	✓	✓	✓	✓	✓
	A_2	-	-	×	-	-	✓
	A_3	×	✓	×	×	×	✓
	A_4	✓	✓	×	✓	✓	✓
	A_5	✓	✓	✓	✓	✓	✓
	A_6	×	×	×	×	×	✓
	A_7	×	✓	✓	×	×	✓
	A_8	×	✓	✓	×	×	✓
	A_9	✓	×	✓	✓	✓	✓
	A_{10}	✓	✓	✓	✓	✓	✓
	P_1	✓	✓	✓	✓	✓	✓
	P_2	✓	✓	✓	✓	✓	✓
	P_3	✓	✓	✓	✓	✓	✓
	P_4	×	✓	✓	✓	×	✓
	P_5	×	✓	×	×	×	✓
	P_6	✓	×	✓	✓	✓	✓
	P_7	✓	×	✓	×	✓	✓

✓:Resist(Attacks)/Possess(Properties) ×:Suffer(Attacks)/No(Properties) -: N/A
Techniques: T_1: Chaotic maps; T_2: Diffie-Hellman Algorithm; T_3: Hash; T_4: XOR; T_5: Symmetric Encryption; T_6: Fuzzy Extractor; T_7: PUF; T_8:ECC.
Attacks/Properties: A_1: Privileged-Insider Attack; A_2: Off-line Password Guessing Attack; A_3: Impersonation Attack; A_4: Replay Attack; A_5: Man-in-Middle Attack; A_6: OBU Intrusion Attack; A_7: RSU Captured Attack; A_8: Stolen-Verifier Attack; A_9: Update asynchronous Attack; A_{10}: Know Session Key Attack; P_1: Mutual Authentication; P_2: Session Key Secrecy; P_3: Identity Anonymity; P_4: Perfect Forward Secrecy; P_5: Batch Authentication; P_6: Malicious Message Tracking; P_7: Unlinkability.

G. Perfect Forward Secrecy

Suppose the adversary knows all the long-term keys in the protocol. However, he/she still cannot obtain the random numbers used for session key agreements, which are not transmitted publicly. Therefore, even if the adversary knows long-term keys he/she cannot recover the previous session keys.

H. Anonymity and Unlinkability

In each session, the vehicle generates a novel pseudo-identity, the pseudo-identities are unlinkable and anonymous. In addition, the transmitted messages are combined with timestamps and random numbers, which are also unlinkable.

I. Desynchronization Attack

The pseudo-identities are generated by the vehicle individually. Therefore, the proposed protocol can resist desynchronization attack.

VIII. Performance Analysis

In this section, we compare the performance between the proposed protocol and the related protocols [15], [18], [19] [20], [21].

First, we analyze the security of the related protocols. In Li et al.'s protocol [15], TA stores RSUs' identities and secret keys. The secret parameter k_j is shared among RSUs and TA, and will affect the system security once it is leakaged. The vehicle's registration parameters are stored in OBU plainly, the adversary can obtain them by the side-channel attack and impersonate the vehicle. The session key agreement is based on the random numbers and one-way hash function, which cannot provide perfect forward secrecy. In Li et al.'s [18]

TABLE III
COMPARISON OF COMPUTATIONAL COSTS

Scheme	V2I Authentication			Time(ms)	Multiple Authentications	Time(ms)
	Vehicle	RSU	TA		RSU&TA (n Vehicle)	
[15]	$6T_H$	$4T_H$	$15T_H$	$0.475ms$	$19nT_H$	$0.361nms$
[18]	$6T_H + 6T_{ECC}$	$6T_H + 6T_{ECC}$	-	$31.548ms$	$6nT_H + (4n+2)T_{ECC}$	$10.554n + 5.22ms$
[19]	$5T_H + T_{ECC}$	$2T_H + T_{ECC}$	$7T_H + 2T_{ECC}$	$10.706ms$	$9nT_H + 3nT_{ECC}$	$8.001nms$
[20]	$5T_H + 3T_{ECC}$	$5T_H + 5T_{ECC}$	$6T_H + 6T_{ECC}$	$36.844ms$	$11nT_H + 11nT_{ECC}$	$28.919nms$
[21]	$2T_H + 4T_{ECC} + T_{SE}$	$3T_H + 5T_{ECC} + T_{SE}$	-	$24.607ms$	$3nT_H + 5nT_{ECC} + nT_{SE}$	$13.618nms$
Ours	$5T_H + 5T_{ECC}$	$4T_H + 5T_{ECC}$	-	$26.271ms$	$4nT_H + (2n+2)T_{ECC}$	$5.296n + 5.22ms$

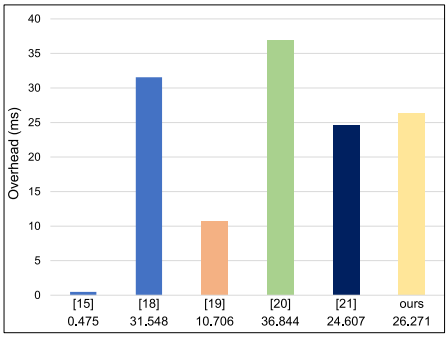

Fig. 6. Single authentication overhead.

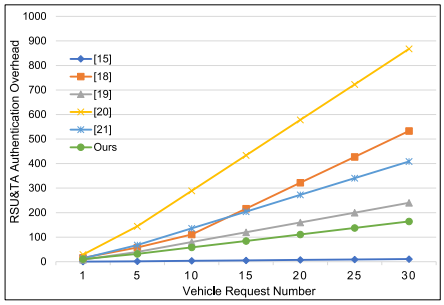

Fig. 7. Overhead in multiple authentication requests.

authentication protocol, the vehicles and RSUs authenticate each other using the time keys, which need to be updated by the registration authority, the update process is unreliable. In addition, the vehicle's pseudo-identity is fixed and can be traced. In Zhang et al.'s [19] authentication protocol, the vehicles authenticate in RSU and TA for obtaining the RSU's local master key, which is used for the message signing. In Yadav and Vijayakumar's [20] protocol and Nath and Choudhury's [21] protocol, TA stores the verification table for identity verification. The vehicle stores the registration parameters plainly, which can be impersonated after launching the side-channel attack. The captured RSU can influence other entities. We found that all relevant protocols could not resist OBU intrusion attacks and subsequent impersonation attacks. In addition, RSU captured attacks will also have a serious impact on some protocols. Table II shows the comparison of security and properties between ours and above protocols.

To simulate the computing performance of mobile devices in VANETs environment, we use Raspberry Pi 4B quad-core 64bits ARM Cortex-A72, 1.5GHz, 2GB LPDDR4 SDARM to simulate the computing of on-board computers.

Let T_H, T_{SE}, and T_{ECC} be the time spent of Hash (SHA-256), symmetric encryption/decryption (AES), and elliptic curve multiplication. According to the computing power of Raspberry Pi 4B, $T_H \approx 0.019ms$, $T_{SE} \approx 0.511ms$, $T_{ECC} \approx 2.610ms$.

Table III and Fig. 6 show that the single authentication overhead of the proposed protocol is low. However, in practical application scenarios, RSU has to process the authentication requests of multiple vehicles at the same time. As shown in Fig. 7, when the number of authentication requests increases, the batch authentication strategy allows our scheme to maintain a lower time overhead.

TABLE IV
COMPARISON OF COMMUNICATION OVERHEAD

Scheme	Authentication		Total ($bits$)
	Vehicle	RSU&TA	
[15]	1888	2976	4864*bits*
[18]	1248	1248	2496*bits*
[19]	832	1792	2624*bits*
[20]	960	2656	3616*bits*
[21]	1376	640	2016*bits (V2I)*
	1504	-	1504*bits (V2V)*
Ours	864	480	1344*bits (V2I)*
	1152	640	1792*bits (V2V)*

In Table IV, we calculate and compare the communication overhead of the protocols. The lengths of the outputs of Hash (SHA-256), one block symmetric encryption (AES-128), one ECC point, and random number are 256bits, 128bits, 160bits, and 256bits, respectively. The lengths of identity, the password, and the timestamp are 32bits. The communication cost of our scheme keeps low among the related schemes.

Therefore, our scheme is not only safer than the relevant schemes but also maintains a lower overhead, which is more suitable for the needs of VANETs.

IX. CONCLUSION

In this paper, we propose a lightweight and anonymous authentication protocol for VANETs, which achieves both V2I and V2V authentication. The vehicle and RSU can realize mutual authentication and exchange information safely without the help of TA. When many vehicles are authenticated with RSU at the same time, batch authentication can be carried out. Once the vehicles in the same RSU domain have completed mutual authentication, they can communicate in any RSU domain or different RSU domains or in scenarios lack

of traffic infrastructure without repeated authentication. The dynamic pseudo-identities are used to protect the privacy and an embedding strategy of dynamic verification parameter is utilized to recover the real identity of the malicious message sender. We use PUF and biological key to resist the RSU captured attacks and the OBU intrusion attacks. Our scheme is efficient and formal provably secure under the random oracle model, which can be applied to VANETs. In the future, we will design traffic accident handling protocol for VANETs.

REFERENCES

[1] D. Y. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen, "A survey on platoon-based vehicular cyber-physical systems," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 263–284, 1st Quart., 2016.

[2] S. S. Moni and D. Manivannan, "A scalable and distributed architecture for secure and privacy-preserving authentication and message dissemination in VANETs," *Internet Things*, vol. 13, Mar. 2021, Art. no. 100350.

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

[4] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015.

[5] J. Cui, L. Wei, J. Zhang, Y. Xu, and H. Zhong, "An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 5, pp. 1621–1632, May 2018.

[6] 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, May 2022, doi: 10.1155/2022/3372489.

[7] A. Joshi, P. Gaonkar, and J. Bapat, "A reliable and secure approach for efficient car-to-car communication in intelligent transportation systems," in *Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET)*, Mar. 2017, pp. 1617–1620.

[8] M. Asghar, R. R. M. Doss, and L. Pan, "A scalable and efficient PKI based authentication protocol for VANETs," in *Proc. 28th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Nov. 2018, pp. 1–3.

[9] Z.-C. Liu, L. Xiong, T. Peng, D.-Y. Peng, and H.-B. Liang, "A realistic distributed conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Access*, vol. 6, pp. 26307–26317, 2018.

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

[11] J. Cui, J. Zhang, H. Zhong, and Y. Xu, "SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10283–10295, Nov. 2017.

[12] J. Qi and T. Gao, "A privacy-preserving authentication and pseudonym revocation scheme for VANETs," *IEEE Access*, vol. 8, pp. 177693–177707, 2020.

[13] I. Ali, Y. Chen, N. Ullah, R. Kumar, and W. He, "An efficient and provably secure ECC-based conditional privacy-preserving authentication for Vehicle-to-Vehicle communication in VANETs," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1278–1291, Feb. 2021.

[14] 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, p. e3317, Nov. 2017.

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

[16] H. Tan, Z. Gui, and I. Chung, "A secure and efficient certificateless authentication scheme with unsupervised anomaly detection in VANETs," *IEEE Access*, vol. 6, pp. 74260–74276, 2018.

[17] Z. Benyamina, K. Benahmed, and F. Bounaama, "ANEL: A novel efficient and lightweight authentication scheme for vehicular ad hoc networks," *Comput. Netw.*, vol. 164, Dec. 2019, Art. no. 106899.

[18] X. Li, Y. Han, J. Gao, and J. Niu, "Secure hierarchical authentication protocol in VANET," *IET Inf. Secur.*, vol. 14, no. 1, pp. 99–110, Jan. 2020, doi: 10.1049/IET-IFS.2019.0249.

[19] J. Zhang, Q. Zhang, X. Lu, and Y. Gan, "A novel privacy-preserving authentication protocol using bilinear pairings for the VANET environment," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–13, Jun. 2021, doi: 10.1155/2021/6692568.

[20] K. A. Yadav and P. Vijayakumar, "LPPSA: An efficient lightweight privacy-preserving signature-based authentication protocol for a vehicular ad hoc network," *Ann. Telecommun.*, vol. 77, pp. 1–17, Dec. 2021.

[21] H. J. Nath and H. Choudhury, "A privacy-preserving mutual authentication scheme for group communication in VANET," *Comput. Commun.*, vol. 192, pp. 357–372, Aug. 2022, doi: 10.1016/J.COMCOM.2022.06.024.

[22] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 9, pp. 2467–2476, Sep. 2017, doi: 10.1109/TITS.2016.2634623.

[23] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

[24] M. Azees, P. Vijayakumar, and L. J. Deborah, "Comprehensive survey on security services in vehicular ad-hoc networks," *IET Intell. Transp. Syst.*, vol. 10, no. 6, pp. 379–388, 2016, doi: 10.1049/IET-ITS.2015.0072.

Qi Xie received the Ph.D. degree in applied mathematics from Zhejiang University, China, in 2005. He was a Visiting Scholar at the Department of Computer Science, University of Birmingham, U.K., from 2009 to 2010, and a Visiting Scholar at the Department of Computer Science, City University of Hong Kong, in 2012. He is a Professor with Hangzhou Normal University and the Director of the Key Laboratory of Cryptography of Zhejiang Province. He has published over 80 research papers in international journals and conferences, such as IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. His research interests include applied cryptography, including digital signatures, authentication, and key agreement protocols. He served as a reviewer for over 40 international journals. He served as the General Co-Chair for ISPEC2012 and ACM ASIACCS2013.

Zixuan Ding received the bachelor's degree from Nantong University in 2020. He is currently pursuing the master's degree with Hangzhou Normal University. He mainly studies authentication protocols and cryptography.

Panpan Zheng is currently pursuing the M.S. degree with the School of Information Science and Technology, Hangzhou Normal University, Hangzhou, China. Her research interests include authentication and key agreement protocols.