Route Privacy-Preserving Authentication Scheme Based on PUF in VANETs

Hanwen Deng[1,2], Yining Liu[1,2(✉)], and Dong Wang[1,2]

[1] School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin 541004, China
lyn7311@sina.com

[2] School of Mathematics and Computing Science, Guilin University of Electronic Technology, Guilin 541004, China

Abstract. Due to the exposure of transmitted messages in public channels within Vehicular Ad-Hoc Network (VANET), many authentication schemes have been proposed to safeguard security and privacy. And in existing schemes, to expedite the authentication process for Vehicle-to-Infrastructure (V2I) communication, vehicles requesting authentication information from Certification Authority (CA) regarding the RSUs they are expected to encounter before the journey is recommended. However, the viability of the aforementioned schemes rely on two challenging prerequisites: complete trustworthiness of CA and the assurance that the Onboard Units (OBUs), which store secret keys permanently, remain impervious to physical attacks and cloning attempts. Hence in this paper, we propose a route privacy-preserving authentication scheme based on PUF in VANETs. Basing on Oblivious Transfer (OT) method, we let CA complete authentication keys distribution without knowing the route plan of a vehicle. We utilize Physically Unclonable Function (PUF) to minimize the exposure of private key. And as the output of a PUF is easily affected by objective factors, Fuzzy Extractor (FE) is used in our scheme to correct the challenge-response pair of it. In addition, the detailed security analysis proves that our scheme can meet the security requirements. Finally, the experimental analysis suggests that our scheme is lower than the other schemes in terms of time complexity.

Keywords: VANETs · Route Privacy · Oblivious Transfer · Physically Unclonable Function · Fuzzy Extractor

1 Introduction

In modern society, personal vehicles have become increasingly essential for not only convenience but also for easy mobility. Nonetheless, they give rise to issues such as traffic congestion and car accidents. To address these concerns, Vehicular Ad-Hoc Networks (VANETs) have been devised to provide safe and comfortable travel for passengers. They enable communication between different entities

J. Cai et al. (Eds.): SPNCE 2023, LNICST 525, pp. 278–296, 2025.
https://doi.org/10.1007/978-3-031-73699-5_20

using Wi-Fi technology and, as a result, have become a widely researched technology [2]. VANETs use Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communication, primarily relying on Dedicated Short Range Communication (DSRC) protocol [1]. The three entities taking part in VANETs are Certification Authorities (CAs), Road Side Units (RSUs), and vehicles.

As security is an issue that can not be ignored because transmitted messages are exposed to public channels, requirements such as authentication and integrity must be achieved [8]. Moreover, In most cases, present solutions provide unforgeability and non-repudiation of messages for ensuring message legitimacy [3]. However, traditional security requirements are insufficient for VANETs because of the features of exposed wireless communication, privacy preserving is critical in VANETs [9].

In order to preserve identity privacy, anonymous identity is proposed to hide the real identity of a vehicle. As some adversaries are able to link the content of message if the anonymous identity is fixed [5], many existing authentication schemes in VANETs suggest to generate different and temporary pseudonyms before every communication, which means that unlinkablility is achieved. Meanwhile, aiming at achieving traceability, Conditional Privacy-Preserving Authentication (CPPA) schemes have been proposed to curtail interference by malicious users by reveal their true identities [4].

However, as real time authentication between RSUs and high-speed vehicles is intolerable for the delay-sensitive applications in VANETs [7], route planning is introduced in VANETs to speed up V2I authentication process [6]. For privacy protection, sensitive information like vehicle's route must not be disclosed, even to entities. Due to both CA and RSUs are semi-trusted, additional measures are needed to preserve route privacy. Moreover, the effectiveness of the existing route privacy-preserving authentication schemes depends on two demanding prerequisites which are hard to guarantee: the absolute trustworthiness of CA and the guarantee that OBUs, responsible for permanently storing secret keys, remain impervious to physical attack and cloning attempts. Consequently, this paper proposes an authentication scheme in VANETs that is able to preserve route privacy and resist physical attacks.

1.1 Motivation and Contributions

In order to tackle the challenges associated with maintaining route privacy and countering physical attacks in VANETs, we propose a route privacy-preserving authentication scheme based on PUF in VANETs. Our scheme incorporates a k-out-of-n Oblivious Transfer method, allowing a vehicle to securely request authentication keys for RSUs it will encounter while keeping its route plan confidential from CA. Furthermore, we employ a combination of PUFs and fuzzy extraction techniques to effectively safeguard the private key from physical attack. Our key contributions are summarized below.

– We propose a route privacy-preserving authentication scheme based on PUF in designed to fulfill the security and privacy requirements of vehicles in

VANETs. In our scheme, the V2I authentication process is able to sped up with the guarantee that the private key will not be exposed by physical attacks and the achievement of route privacy when CA is not considered to be fully trusted.
– We conducted a detailed analysis of our scheme while ensuring that it meets the necessary security requirements. Our findings suggest that the proposed scheme effectively preserves the privacy of vehicles, even in complex and harsh conditions. Additionally, our scheme is characterized by low time complexity.

1.2 Outline of the Rest Paper

Related work is outlined in Sect. 2 In Sect. 3, we introduce the system model and threat model, meanwhile, a overview of Group Rings, Oblivious Transfer Protocol, Physical Unclonable Function and Fuzzy Extractor is provided. We introduce the proposed scheme detailedly in Sect. 4. Next, Sect. 5 evaluates the security of the route privacy-preserving authentication scheme based on PUF in VANETs while Sect. 6 offers a performance evaluation of it. At last, the conclusion of the paper is done by us.

2 Related Work

In this section, we provide an overview of different authentication schemes that address privacy and security concerns in VANETs. We examine each protocol individually, discussing their respective pros and cons.

Security is a crucial concern that cannot be overlooked since transmitted messages are vulnerable to public channels. Therefore, it is imperative to ensure that certain requirements, such as authentication and integrity, are met in order to safeguard the confidentiality and accuracy of the information being transmitted [3]. As Traditional security requirements are inadequate for VANETs due to the unique characteristics of exposed wireless communication, privacy preservation is widely research [9]. Aiming at preserving identity privacy, Mundhe et al. [11] utilize ring signature to generate identities to prevent property of vehicles from leakage. Ahamed et al. [12] proposed an efficient anonymous mutual and batch authentication scheme in VANETs, which is able to perform anonymous batch authentication. However, the problem is, the achievements of these existing schemes are not enough for the stability of the system. Because of the lack of the tracing and punishment mechanism, the adversary can disrupt the system without any price.

Therefore, in order to reveal the real identity of adversary, the conditional privacy-preserving authentication is widely researched in the last decades. Based on public key infrastructure (PKI), Khodaei et al. [18] check the certificate to verify the identity of a vehicle. However, as the use of digital certificates can result in increased transmission and storage overhead, CPPA schemes based on identity are proposed. Utilizing bilinear pairing, Zhang et al. [19] proposed to use multiple certificate authorities to achieve conditional privacy. Because there are

some disadvantages in performance of bilinear pairing-based schemes which is unacceptable in delay-sensitive scenes, another cryptography tool Elliptic Curve Cryptosystem (ECC) is often used by authentication schemes in VANETs. Based on ECC, Lin et al. [13] proposed a scheme that organizes the vehicles into several groups managed by group leaders so as to reveal the real identities of malicious vehicles. Nevertheless, the high velocity of the vehicle during the journey renders it unsuitable for delay-sensitive applications [7], route planning is introduced in VANETs to speed up V2I authentication process [6]. As it is hard to guarantee the reliability of CA, Liang et al. [22] proposed a route planning authentication scheme aimed at safeguarding the privacy of vehicle routes while acquiring authentication keys from CA. Based on China's remaining theorem, in the route privacy scheme of Yan et al. [23], the malicious vehicles can be revoked efficiently.

While the aforementioned schemes appear to prioritize security and privacy, it is important to acknowledge that the security of OBUs is often perceived as excessively idealistic due to their inherent resource limitations. Given that OBUs frequently store private keys of associated entities, the system's security may be compromised by cloning or physical attacks [24]. In an environment lacking physical security, it is crucial to urgently develop a solution that not only has low cost implications but also effectively mitigates the risk of adversarial compromise of remote unmonitored devices. Baseing on unavoidable variations in the manufacturing process, the Physical Unclonable Function (PUF) is specifically designed to offer a hardware-unique mapping [25]. Renault et al. [26] utilized PUF to spread secret keys by RSUs. According to their scheme, vehicles have the capability to receive emergency tokens from RSUs, and only authorized vehicles possess the decryption capability. Likewise, based on PUF, Umar et al. [28] proposed a identity-based anonymous authentication scheme in VANETs. They employed fundamental cryptographic operations to reduce costs, while also incorporating PUF as a countermeasure against physical attacks. However the schemes mentioned above ignored the fact that chip aging, environmental variations such as temperature, and other factors can introduce noise, which can result in bit flipping and potentially impact the response of PUF. Additional methods should be figured to solve the problem.

In conclusion, the practicality of numerous schemes falls short, prompting our objective to propose an authentication scheme for VANETs that not only safeguards the privacy of vehicle routes but also effectively thwarts physical attacks on the system. Furthermore, we analyze the differences between the related schemes, which are shown in Table 1.

3 Preliminaries

In this section, the System Model, Threat Model, Group Rings, Oblivious Transfer Protocol, Physical Unclonable Function, Fuzzy Extractor and Design Goals of the proposed scheme are described respectively.

Table 1. Existing Schemes: A Comparative Summary

Scheme	Year	Methods	Strenghts	Limitations
[11]	2018	Ring signature	Providing signature unforgeability	Lack of providing traceability and protection for physical attack
[12]	2018	Bilinear pairing	Providing mutual authentication and data integrity	Lack of providing traceability and unlinkability. High computational overheads
[18]	2021	PKI	Providing reduction on certificate revocation lists distribution overhead	High storage overheads. Lack of providing protection for physical attack
[19]	2017	Bilinear pairing	Providing simultaneous verification of many messages	Lack of unlinkability. High computational overheads
[26]	2021	PUF	Providing protection against physical attack	Lack of providing methods to correct the noisy response of PUF. Storing response of PUF in RSUs which is unsafe
[28]	2021	ECC and PUF	Providing low-cost authentication and rotection against physical attack	Lack of providing methods to correct the noisy response of PUF
[23]	2022	ECC and Chinese remainder theorem	Providing route privacy and malicious vehicles revocation	Lack of providing protection for physical attack

3.1 System Model

Figure 1 illustrates the system model of out route privacy-preserving authentication scheme based on PUF in VANTEs. There are three entities in the model: Certification Authority (CA), Road Side Unit (RSU), and vehicle.

– **CA:** CA plays a crucial role in the proposed scheme by utilizing its exceptional computing and storage capabilities to perform two primary tasks: storing information related to RSUs and vehicles, and facilitating the authentication process between them. Although CA is expected to follow established protocols, it cannot be entirely relied upon. This is due to the fact that CA has an inherent interest in obtaining sensitive privacy information about vehicles, including real-time location and routes.

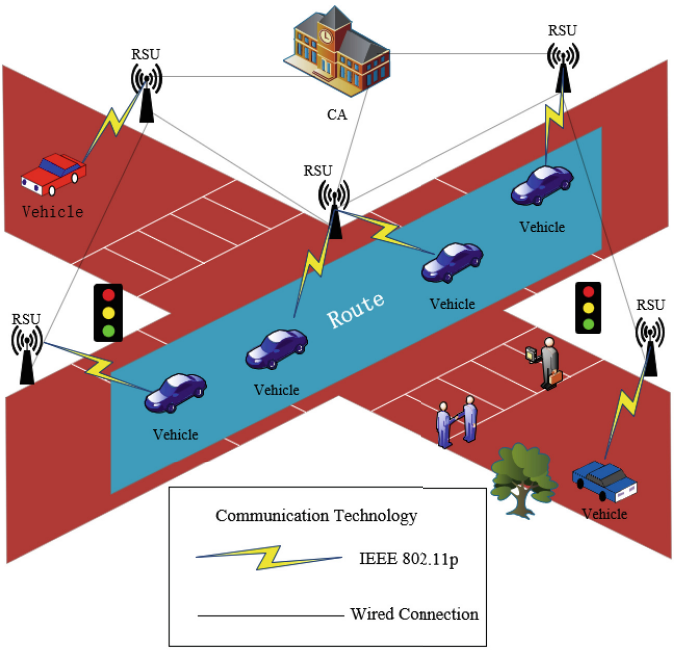

Fig. 1. System model.

- **RSU:** RSUs are strategically placed along the roadside and serve as intermediaries between CA and vehicles. Their primary function is to provide driving convenience to vehicles within their coverage area, including information on road conditions. Furthermore, RSUs also facilitate communication between vehicles that are situated within their range.
- **Vehicles:** Each vehicle is equipped with an OBU. OBU is in charge of communicating with other entities: CA, RSUs and OBUs.

3.2 Threat Model

In the proposed scheme, the Initial phase and registration phase are performed in a secure channel while the security of the communications between vehicles and the other entities (CA, RSUs, vehicles) could not be guaranteed. What calls for special attention is that although both CA and RSUs should adhere to defined protocols strictly, they are curious about the sensitive privacy of vehicles such as routes and speed. Additionally, the time of all entities is kept in sync and the identities of all RSUs are public. The assumptions of the adversary model are described as follows:

- It is assumed that an attacker has the ability to intercept, modify, delete, and replay any information transmitted over the public channel. This includes all forms of communication that are not securely encrypted or protected.

– The entities of the system are facing the risk of physical attacks, secret parameters of them are likely to be stolen.
– Besides executing the protocol honestly, both CA and RSUs are likely to obtain the privacy of the individual vehicles by analyzing legally received messages.

3.3 Group Rings

For a Given group G and a commutative ring R. The $R[G]$ denote a set of $\sum_{g_i \in G} r_i g_i$, where $r_i \in R$. In which we have $\sum_{g_i \in G} a_i g_i + \sum_{g_i \in G} b_i g_i = \sum_{g_i \in G} (a_i + b_i) g_i$ and $\sum_{g_i \in G} a_i g_i \cdot \sum_{g_i \in G} b_i g_i = \sum_{g_i \in G} \left(\sum_{g_i g_k = g_i} a_j b_k \right) g_i$ [17]. In this paper, we denote $Z_q [S_m]$ for $R = Z_q$ and G is the m-degree symmetric group. What's more, $M_l (Z_q [S_m])$ denote a set of $l * l$ matrices that is considered as a semi-group over $Z_q [S_m]$.

3.4 Oblivious Transfer Protocol

An Oblivious Transfer (OT) protocol [17] is a cryptographic method utilized to safeguard the privacy of users in electronic commerce. Through the use of OT, the receiver is able to obtain the desired information without the sender being made aware of the specific selection. In k-out-n OT scheme, we denote Alice has n messages and Bob wants to get k of them. Specifically, Bob can only get what he has chosen, meanwhile, Alice knows nothing about Bob's choice [10]. Figure 2 shows the process of the mentioned k-out-n OT scheme.

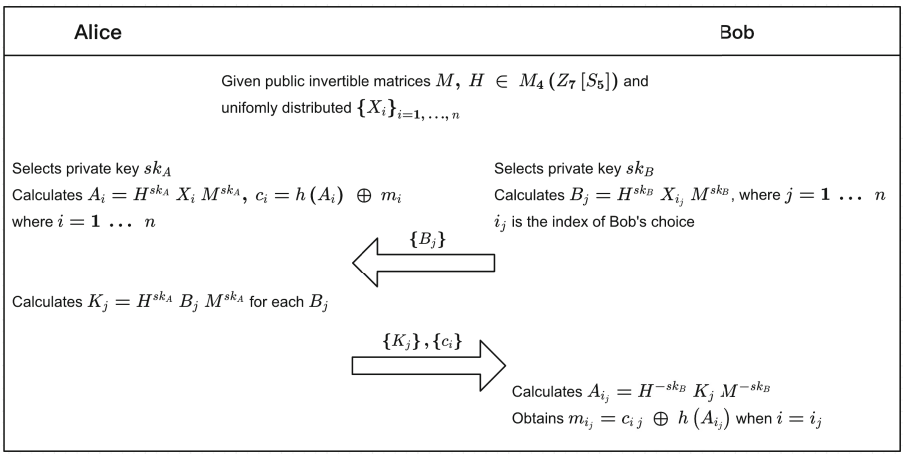

Fig. 2. k-out-n OT scheme.

3.5 Physical Unclonable Function

A Physical Unclonable Function (PUF) is a device that transforms an input bit-string, also known as a challenge, into an output bit, which is referred to as a response. This transformation is achieved by utilizing a specialized microelectronic circuit within the PUF that is highly responsive to variations in signal propagation delay. Variations in manufacturing processes result in slight delays among the fabricated circuits. These delays, combined with the intentional design of the delay-sensitive PUF circuit, impact the response to identical challenge bits across different instances of circuit fabrication. As the delay cannot be controlled, the PUF becomes unclonable, providing a means for unique authentication in devices that incorporate such embedded PUFs [20]. Let Cha and RE denote challenge and the response respectively, in this paper, a PUF function can be described as $RE = PUF(Cha)$.

3.6 Fuzzy Extractor

It's worth noting that chip aging, environmental variations such as temperature and some other factors can introduce noise, leading to bit flipping and potentially affecting the PUF response. Consequently, the demand for helper data algorithms becomes imperative to address errors in PUF responses and ensure the independence and uniform distribution of response bits. These algorithms play a crucial role in fulfilling the requirements of PUF-based authentication and key generation processes [21]. In this paper, we introduce Fuzzy Extractor(FE) to generate the reproduction parameter to correct the noisy response. The two algorithms in FE are denoted as $Rep()$ and $Gen()$ respectively. Specifically, let RE denote the input parameter, $(SK, RP) = Gen(RE)$, where SK is secret key and RP is reproduction parameter to be saved. The recovery process is $SK^* = Rep(RE^*, RP)$ where there is a certain error between RE and RE^*.

3.7 Design Goals

- **Route Privacy:** Under the assumption that CA is partially untrusted, we are supposed to ensure that the routes of vehicles remain undisclosed to any entity.
- **Mutual identity authentication:** In order to ensure the validity of the messages transmitted in the public channel, We need to guarantee that only the senders of the messages could prove that who they are claimed to be.
- **Identity Traceability:** Once a malicious vehicle is detected, its real identity could be revealed by the RSU cluster even though all the vehicles use pseudonyms through the communications.
- **Identity Unlinkability:** This implies that neither attackers nor any other entities can deduce the identity of a specific vehicle by linking two authentication messages transmitted by that vehicle.
- **Physical Attack Resistance:** It means that even if the OBUs of vehicles are under physical attack, for instance, being captured by adversaries, the secret key cannot be obtained by them.

– **Replay Attack Resistance:** This implies that the replayed messages are unable to pass the verification process of any entity within the system.

4 The Proposed Scheme

In this section, we introduce our route privacy-preserving authentication scheme. Meanwhile, we list the main notations in proposed scheme as Table 2.

Table 2. Main Notations

Notations	Descriptions
h_0, h_1	Secure hash functions
M, H	Invertible matrices
E_{sym}	Symmetry encryption algorithm
RSU_i	The i-th RSU
v_j	The j-th vehicle
sk_{CA}, sk_{v_j}	Private key of each entity
K_i	Authentication key of RSU_i
K_R	Symmetric key of all RSUs
RID_j	Real identity of v_j
AID_j	Associated identity of v_j
PID_j	Pseudonym of v_j
PUF	Physical unclonable function
Gen, Rep	Generation and reproduction functions of fuzzy extractor

4.1 Initial Phase

In this phase, CA is supposed to set necessary parameters of system with the coordination of RSUs.

1. CA chooses a random number $sk_{CA} \in Z_q^*$ as private key, it then selects a secure parameter λ and generates two collision-resistance hash functions $h_0 : \{0,1\}^* \rightarrow Z_q^*$ and $h_1 : M_4 \left(Z_7 \left[S_5\right]\right) \rightarrow \{0,1\}^\lambda$.
2. To meet the requirements of the system, CA selects a symmetric encryption algorithm denoted as E_{sym}. This algorithm is utilized to encrypt the plaintext message m by performing the operation $c = E_{sym}(k, m)$, where c represents the resulting cipher and k is the secret key. Subsequently, the received cipher c is decrypted by executing the operation $m = D_{sym}(k, c)$ to obtain the original plaintext message.
3. We assmue that there are n RSUs in the jurisdiction of CA which indicated as $\{RSU_i\}_{i=1,2,\cdots,n}$. CA assigns n authentication keys $\{K_i\}_{i=1,2,\cdots,n}$ for them and select one symmetric key K_R.

4. CA randomly chooses invertible matrices $M, H \in M_4\left(Z_7\left[S_5\right]\right)$ and uniformly distributed $\{X_i\}_{i=1,\ldots,n}$. Then, CA calculates $A_i = H^{sk_{CA}} X_i M^{sk_{CA}}$ and the ciphers $c_i = h_1\left(A_i\right) \oplus K_i$ for $i = 1, \ldots, n$.
5. CA securely retains the values sk_{CA} and $\{c_i\}\, i = 1, 2, \cdots, n$. It transmits the symmetric key K_R to all RSUs through a secure channel. Additionally, CA publicly broadcasts the following elements: $\left\{h_0, h_1, E_{sym}, M, H, \{X\}_{i=1,\ldots,n}\right\}$.

4.2 Registration Phase

Every vehicle needs to register into the system through the registration Phase. Figure 3 reflects the registration process.

1. Let us assume that there will be a maximum of m vehicles. When a vehicle, denoted as v_j $(j = 1, 2, \cdots, m)$, signs up, it generates a challenge Cha_j and computes response R_j using PUF as $R_j = PUF(Cha_j)$. Subsequently, in order to obtain the reproduction parameter RP_j, v_j calculates $(sk_{v_j}, RP_j) = Gen(R_j)$. It is worth mentioning that sk_{v_j} will not be stored. Finally, it sends its real identity $RID_j \in Z_q^*$ to CA.
2. Upon receiving the RID_j from v_j, CA chooses a random number r_j for v_j and generates its corresponding associated identity as $AID_j = RID_j \oplus h_0(sk_{CA}||r_j)$. It is important to note that CA has the capability to periodically update the value of AID_j. Then, the pseudonym of v_j is generated by calculating $PID_j = E_{sym}(K_R, AID_j)$. Subsequently, CA transmits the associated identity and pseudonym $\{AID_j, PID_j\}$to the respective vehicle.

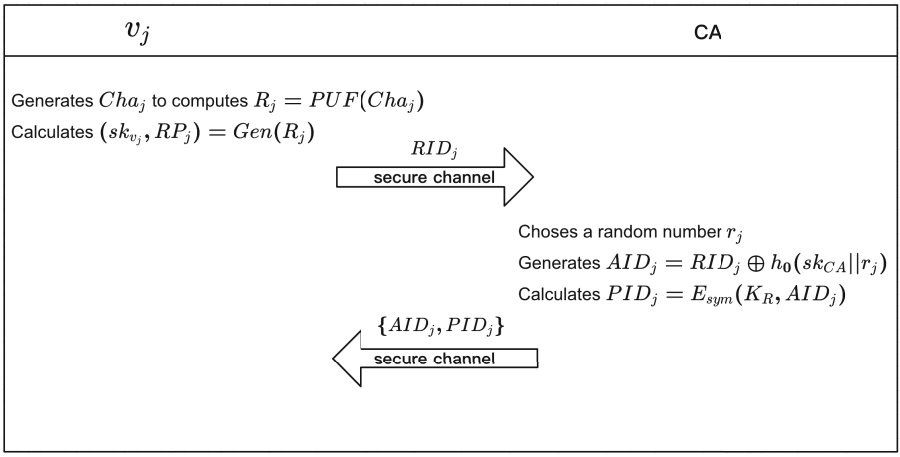

Fig. 3. Registration phase.

4.3 Route Planning Phase

In this phase, we introduce the route planning phase before a journey of v_j. Figure 4 reflects the route planning process

1. The vehicle v_j chooses an appropriate shortest path algorithm such as SPFA algorithm. Suppose that the result of the shortest path algorithm suggests that v_j would pass $Path_j = \{RSU_1, RSU_2, \cdots, RSU_a, \cdots, RSU_w\}$ $(w <= n)$. Then it obtains $R_j^* = PUF(Cha_j)$ and generates it secret key by calculating $sk_{v_j} = Rep(R_j^*, RP_j)$.
2. According to the $Path_j$, the vehicle v_j keeps its choice ch $(ch = 1, \cdots, w)$, and calculates $B_{ch} = H^{sk_{v_j}} X_{j_i} M^{sk_{v_j}}$ for $1 \leq j_i \leq n$. In addition, v_j generates the timestamp t_0 and constructs $\iota_{j,1} = h_0(AID_j || t_0)$, $\iota_{j,2} = h_1(B_{ch})$ and sends $\{\iota_{j,1}, \iota_{j,2}, t_0, \{B_{ch}\}, AID_j\}$ to CA.
3. On receiving message from v_j, CA checks the legality of AID_j and verifies $\iota_{j,1}$, $\iota_{j,2}$ and t_0. If the checking process succeeds, CA computes $R_{ch} = H^{sk_{CA}} B_{ch} M^{sk_{CA}}$ for $ch = 1, 2, \cdots, w$, generates the timestamp t_1 to constructs $\mu_1 = \{h_0(t_1 || c_i)\}_{i \in \{1,2,\ldots,n\}}$, $\mu_2 = \{h_1(R_{ch})\}_{ch \in \{1,2,\ldots,w\}}$ and sends them back to v_j with all ciphers $\{c_i\}_{i \in \{1,2,\ldots,n\}}$.
4. In order to get the authentication keys of wanted RSUs in $Path_j$, v_j first verifies μ_1, μ_2 and t_1. If the verification succeeds, it computes $A_{j_i} = H^{-sk_{v_j}} R_{ch} M^{-sk_{v_j}}$. Finally, v_j could obtain $K_{ch} = c_{j_i} \oplus h_1(A_{j_i})$ while CA could not know which c_i the v_j has chosen.

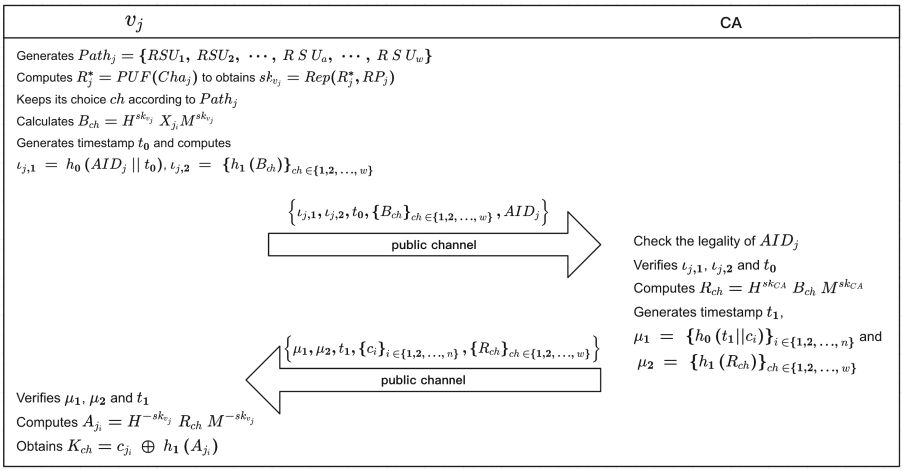

Fig. 4. Route Planning phase.

4.4 Mutual Authentication Phase

As both of the vehicles and RSUs are probably attacked, before they share information with each other, they have to do the mutual authentication. Figure 5 reflects the mutual authentication process.

1. When the vehicle v_j enters the coverage of RSU_i, both of them need to prove their validation. The vehicle v_j selects a random number $r_{j_i} \in Z_q^*$. Then, v_j generates the timestamp t_2 and message m_0, to calculates $sm_{j_i} = E_{sym}(K_i, AID_j \| t_2 \| m_0 \| PID_j \| r_{j_i})$, $\phi_j = h_0(PID_j \| AID_j \| sm_{j_i} \| t_2)$, where $j_i \in \{1, \ldots, n\}$. Finally, $\{sm_{j_i}, \phi_j, t_2, PID_j, AID_j\}$ is sent to RSU_i.
2. After RSU_i receives, it first calculates $content_{j_i} = D_{sym}(K_i, sm_{j_i})$ to decrypt the cipher. The checking process is to judge whether ϕ_j is valid using hash function h_0. If it passes, then it calculates $AID_j^* = D_{sym}(K_R, PID_j)$, only if the equation $AID_j^* = AID_j$ holds, it means that the authentication of v_j is complete, otherwise, RSU_i rejects the request. Next, RSU_i generates the timestamp t_3 and message m_1, calculates $sm_{i_j} = E_{\mathbf{sym}}(K_i, h_0(r_{j_i} + 1) \| t_3 \| m_1)$ and $\sigma_i = h_0\left(i \| t_3 \| m_1 \| sm_{i_j}\right)$. It sends $\left\{sm_{i_j}, \sigma_i, t_3, i\right\}$ back to v_j at last.
3. On receiving the response, v_j calculates $content_{i_j} = D_{sym}\left(K_i, sm_{i_j}\right)$. It then verifies the validation of σ_i from $content_{i_j}$, if it passes, the communication between v_j and RSU_i is finally established.

5 Security Analysis

In this section, the security analysis is provided to demonstrate that the proposed scheme has meets all of out design goals.

Theorem 1. *The proposed scheme can achieve route privacy.*

Proof. During the route planning phase, vehicle v_j obtains authentication keys through Oblivious Transfer (OT). The only relevant parameter for v_j in CA's possession is $B_{ch} = H^{sk_{v_j}} X_{j_i} M^{sk_{v_j}}$. If CA intends to determine the route, it must deduce X_{j_i} by factoring B_{ch} into $H^{sk_{v_j}}$, X_{j_i}, and $M^{sk_{v_j}}$, then identify the value of j_i by comparing X_{j_i} with other matrices. However, this task cannot be accomplished due to the protection provided by $H^{sk_{v_j}}$ and $M^{sk_{v_j}}$, as it is based on the Group Factorization Problem [29].

Theorem 2. *The proposed scheme can achieve mutual identity authentication.*

Proof. In the proposed scheme, since RSUs are semi-trusted, RSUs and vehicles have to complete identity authentication with each other before establishing communication channel.

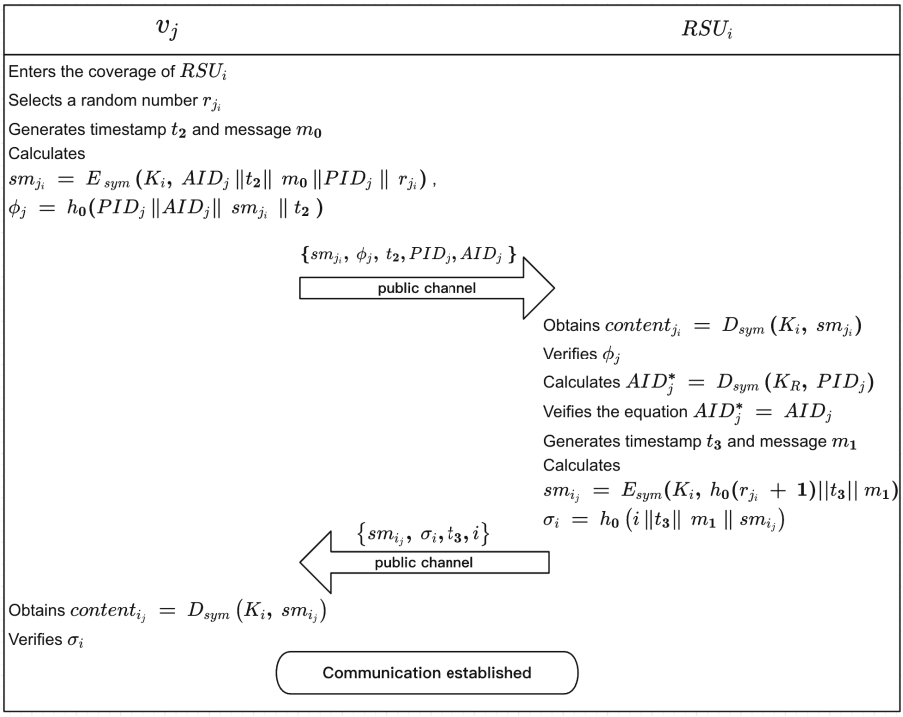

Fig. 5. Mutual authentication phase.

- On the one hand, the vehicle v_j obtains the authentication key K_i of RSU_i in the route planning phase. If the adversary wants to disguise as a legal vehicle, it needs to obtain the matrix X_{j_i} to get K_i to encrypt message using E_{sym} . However, it is tough for it as the proof of **Theorem 1** mentioned above. If the adversary wants to tamper the message of v_j, RSU_i can penetrate the attack by the hash function h_0 and reject it.
- On the other hand, RSU_i has access to the random number r_{j_i} generated by v_j. In order to establish its legitimacy, RSU_i is required to respond with $h_0(r_{j_i}+1)$. Importantly, only the authorized RSU possesses the authentication key necessary to decrypt the cipher transmitted by v_j.

Theorem 3. *The proposed scheme can achieve identity traceability.*

Proof. In our proposed scheme, when a malicious vehicle v_j is detected, CA is able to reveal its real identity because $AID_j = RID_j \oplus h_0(sk_{CA}||r_j)$ and CA is responsible to store sk_{CA} and r_j. Moreover, in order to guarantee that the associate identity can be traced, RSU_i is supposed to verifies the availability of the pseudonyms by calculating $AID_j^* = D_{sym}(K_R, PID_j)$, only if the equation $AID_j^* = AID_j$ holds, it means that the authentication of v_j is complete. In the event that a malicious vehicle v_j is detected, CA has the capability to disclose

its real identity. This is possible because $AID_j = RID_j \oplus h_0(sk_{CA}||r_j)$, and CA is responsible for securely storing both sk_{CA} and r_j. Furthermore, to ensure traceability of the pseudonyms sent by v_j, RSU_i is required to verify the validity of it by computing $AID_j^* = D_{sym}(K_R, PID_j)$. Only when the equation $AID_j^* = AID_j$ holds true, it signifies that the authentication of v_j is successful.

Theorem 4. *The proposed scheme can achieve unlinkability.*

Proof. Due to the periodic updating of vehicle pseudonyms, it becomes impossible for an adversary to establish a connection between multiple messages originating from the same vehicle.

Theorem 5. *The proposed scheme can resist physical attack and cloning.*

Proof. The private key sk_{v_j} of vehicle v_j is not directly stored in OBU. To derive its private key, v_j is required to compute the noisy results as $skn_j = PUF(Cha_j)$. Subsequently, it calculates sk_{v_j} using the reproduction parameter RP_j as $sk_{v_j} = Rep(skn_j, RP_j)$. As a result, even if OBU becomes a target of physical attacks or cloning attempts, adversaries are unable to obtain sk_{v_j} and exert influence on other entities.

Theorem 6. *The proposed scheme can resist replay attack.*

Proof. Each time an entity intends to transmit messages via the public channel, timestamps and random numbers are integrated into the public messages. Consequently, adversaries are unable to successfully pass the verification process due to the inclusion of freshness indicators.

6 Performance Evaluation

This section presents a comprehensive analysis of the computational and communication workload associated with the proposed scheme, along with a comparative assessment against several recent schemes. To assess the computation overhead, we implemented the proposed scheme using Java 15 on a desktop computer featuring an Apple M1 Pro processor with a clock frequency of 3.20 GHz, running on macOS 13 operating system. The average operation time of the simulation, calculated over 1000 iterations, is displayed in Table 3. It is important to note that the computational burden of certain operations, such as XOR, has been disregarded due to their relatively minor impact on efficiency when compared to other operations.

6.1 Computational Overhead

In the proposed scheme, as the registration phase is an one-time process, we ignore the computation burden of it in this subsection. In route planning phase, as we assume that the total number of RSUs is n and the path of the vehicles would include w RSUs. To begin with, in order to obtain its secret key, the

Table 3. Execution

Notation	Description	Execution time (ms)
T_h	Hash function execution	0.001
T_a^{ecc}	Point addition execution on ECC	0.016
T_m^{ecc}	Scalar multiplication execution on ECC	0.669
T_i^{mtx}	Matrix inverse execution	0.002
T_m^{mtx}	Matrix multiplication execution	0.003
T_e	Encrytion of AES	0.037
T_d	Decryption of AES	0.016
T_{PUF}	PUF simulation	0.113
T_{fe}	Fuzzy extractor execution	0.417

vehicle is supposed to perform PUF and FE once, then it needs to execute matrix multiplication $2\log sk_{v_j}+2w$ times, hash function $w+1$ times to prepare for the request. On receiving the response from CA, the vehicle v_j is supposed to perform 2 matrix inverse, $2w$ matrix multiplications and $w+n$ hash evaluations. Therefore, $(2\log sk_{v_j}+4w)T_m^{mtx}+(n+2w+1)T_h+2T_i^{mtx}+T_{PUF}+T_{fe}=0.006\log sk_{v_j}+0.014w+0.001n+0.58ms$ is cost by v_j. As for CA, it needs to perform hash function $2w+n+1$ times and matrix multiplication $2w$ times. The total cost of CA is $0.008w+0.001n+0.001ms$. Figure 6 reflects the relationship between the system computation burden, the number of RSUs in the route of vehicle and the total computation burden in this phase.

Table 4. Comparison of computation overheads in authentication phase

Scheme	Computation overheads
[10]	$8T_h+11T_m^{ecc}+4T_a^{ecc}$
[14]	$11T_h+4T_m^{ecc}$
[15]	$2T_h+5T_m^{ecc}$
[16]	$10T_h+10T_m^{ecc}+3T_a^{ecc}$
Our scheme	$5T_h+2T_e+3T_d$

In the mutual authentication phase, the vehicle v_j ought to Before sending message, the vehicle v_j ought to perform AES encryption and hash function once respectively. On receiving the response from RSU_i, in order to verify the validation of RSU_i, it has to perform AES decryption once and hash function once finally. Thus, the computation burden of v_j in mutual authentication phase is $2T_h+T_e+T_d=0.054ms$. As mentioned above, in order to check the validation of v_j, RSU_i has to obtain PID_j and then deduce AID_j. Double AES decryption and a hash operation would be done. Then RSU_i needs to execute AES

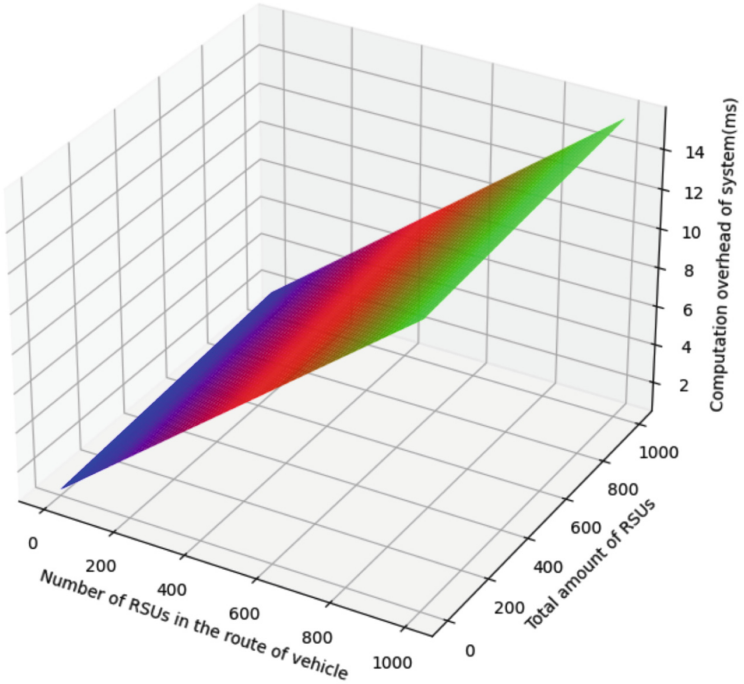

Fig. 6. Relationship between system computation overheads, number of RSUs in the route of vehicle and total computation overheads.

decryption once and hash function twice respectively to response. The total cost of RSU_i is $3T_h + T_e + 2T_d = 0.072ms$. In Table 4, we list the comparison of computation burden between other related schemes as they could be implemented in the same way.

6.2 Communication Overhead

In this subsection, our focus is solely on analyzing the communication cost associated with the mutual authentication process, as the route planning phase occurs only occasionally. To estimate the communication overhead, we make reasonable assumptions regarding the bit-lengths of the output of hash function (SHA-128) and symmetric encryption (AES-128) are both 128bits. The length of an ECC point, a timestamp are 160bits and 32bits respectively. We calculate and compare the communication overhead of the protocols in Table 5.

Hence, our scheme not only offers enhanced security compared to other relevant schemes but also maintains a lower overhead, making it more suitable for the requirements of VANETs.

Table 5. Comparison of communication overhead in authentication phase

Scheme	Communication overhead
[10]	1216bits
[14]	2784bits
[15]	1280bits
[16]	864bits
Our scheme	832bits

7 Conclusion

In VANETs, the implementation of most privacy-preserving schemes relies on the complete trustworthiness of CA and the availability of OBUs. Obviously, guaranteeing these two prerequisites is tough in practical environment. As the route of a vehicle may be obtained by CA and the secret keys stored in OBUs might be leaked when physical attack and cloning occurs, security and privacy can not be safeguarded. To address this issue, we propose a route privacy-preserving authentication scheme based on PUF in VANETs. While preserving route privacy, our scheme accelerates V2I authentication speed and defends against physical attacks. To implement our scheme, a vehicle can plan its route and request authentication keys from CA for the RSUs it will encounter. We use OT to ensure that CA has no knowledge of which authentication keys the vehicle has chosen. Furthermore, a vehicle's secret key must be generated by PUF using its challenge. And as s the output of a PUF is easily affected by objective factors, fuzzy extractor is used in our scheme to correct the noise. Finally, our scheme has a lower computation burden compared to other relevant schemes.

References

1. Cui, J., Wei, L., Zhang, J., et al.: An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks. IEEE Trans. Intell. Transp. Syst. **20**(5), 1621–1632 (2018)
2. Khan, A.A., Abolhasan, M., Ni, W., et al.: A hybrid-fuzzy logic guided genetic algorithm (H-FLGA) approach for resource optimization in 5G VANETs. IEEE Trans. Veh. Technol. **68**(7), 6964–6974 (2019)
3. Wei, L., Cui, J., Xu, Y., et al.: Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs. IEEE Trans. Inf. Forensics Secur. **16**, 1681–1695 (2020)
4. Wang, Y., Liu, Y., Tian, Y.: ISC-CPPA: improverd-security certificateless conditional privacy-preserving authentication scheme with revocation. IEEE Trans. Veh. Technol. **71**(11), 12304–12314 (2022)
5. Saini, K., Namdev, K., Rai, K.: TMAPS: a trust-based mutual authentication and privacy in VANET. In: 2022 3rd International Conference for Emerging Technology (INCET), pp. 1–7. IEEE (2022)

6. Ahmad, A., Din, S., Paul, A., et al.: Real-time route planning and data dissemination for urban scenarios using the internet of things. IEEE Wirel. Commun. **26**(6), 50–55 (2019)
7. Zhang, H., Yu, J., Obaidat, M.S., et al.: Secure edge-aided computations for social internet-of-things systems. IEEE Trans. Comput. Soc. Syst. **9**(1), 76–87 (2020)
8. Song, J., Liu, Y., Shao, J., et al.: A dynamic membership data aggregation (DMDA) protocol for smart grid. IEEE Syst. J. **14**(1), 900–908 (2019)
9. Lin, C., He, D., Huang, X., et al.: BCPPA: a blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks. IEEE Trans. Intell. Transp. Syst. **22**(12), 7408–7420 (2020)
10. Zhang, X., Zhong, H., Cui, J., et al.: LBVP: a lightweight batch verification protocol for fog-based vehicular networks using self-certified public key cryptography. IEEE Trans. Veh. Technol. **71**(5), 5519–5533 (2022)
11. Mundhe, P., Yadav, V.K., Verma, S., et al.: Efficient lattice-based ring signature for message authentication in VANETs. IEEE Syst. J. **14**(4), 5463–5474 (2020)
12. Ahamed, A.B.S., Kanagaraj, N., Azees, M.: EMBA: an efficient anonymous mutual and batch authentication schemes for vanets. In: 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), pp. 1320–1326. IEEE (2018)
13. Lin, X., Sun, X., Ho, P.H., et al.: GSIS: a secure and privacy-preserving protocol for vehicular communications. IEEE Trans. Veh. Technol. **56**(6), 3442–3456 (2007)
14. Wei, L., Cui, J., Zhong, H., et al.: Proven secure tree-based authenticated key agreement for securing V2V and V2I communications in VANETs. IEEE Trans. Mob. Comput. **21**(9), 3280–3297 (2021)
15. Kumar, V., Ahmad, M., Mishra, D., et al.: RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing. Veh. Commun. **22**, 100213 (2020)
16. Wang, J., Zhu, Y.: Secure two-factor lightweight authentication protocol using self-certified public key cryptography for multi-server 5G networks. J. Netw. Comput. Appl. **161**, 102660 (2020)
17. Wang, X., Kuang, X., Li, J., et al.: Oblivious transfer for privacy-preserving in VANET's feature matching. IEEE Trans. Intell. Transp. Syst. **22**(7), 4359–4366 (2020)
18. Khodaei, M., Papadimitratos, P.: Efficient, scalable, and resilient vehicle-centric certificate revocation list distribution in VANETs. In: Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks, pp. 172–183 (2018)
19. Zhang, L., Wu, Q., Domingo-Ferrer, J., et al.: Distributed aggregate privacy-preserving authentication in VANETs. IEEE Trans. Intell. Transp. Syst. **18**(3), 516–526 (2016)
20. Millwood, O., Miskelly, J., Yang, B., et al.: PUF-phenotype: a robust and noise-resilient approach to aid group-based authentication with DRAM-PUFs using machine learning. IEEE Trans. Inf. Forensics Secur. **18**, 2451–2465 (2023)
21. Badshah, A., Waqas, M., Muhammad, F., et al.: AAKE-BIVT: anonymous authenticated key exchange scheme for blockchain-enabled internet of vehicles in smart transportation. IEEE Trans. Intell. Transp. Syst. **24**(2), 1739–1755 (2022)
22. Liang, Y., Liu, Y., Gupta, B.B.: PPRP: preserving-privacy route planning scheme in VANETs. ACM Trans. Internet Technol. **22**(4), 1–18 (2022)
23. Yan, Z., Zhang, J.: Path privacy-preserving scheme based on oblivious transfer protocol. In: 2022 10th International Conference on Intelligent Computing and Wireless Optical Communications (ICWOC), pp. 6–10. IEEE (2022)

24. Alfadhli, S.A., Lu, S., Chen, K., et al.: MFSPV: a multi-factor secured and lightweight privacy-preserving authentication scheme for VANETs. IEEE Access **8**, 142858–142874 (2020)
25. Wallrabenstein, J.R.: Practical and secure IoT device authentication using physical unclonable functions. In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), pp. 99–106. IEEE (2016)
26. Renault, É., Mühlethaler, P., Boumerdassi, S.: Communication security in vanets based on the physical unclonable function. In: ICC 2021-IEEE International Conference on Communications, pp. 1–6. IEEE (2021)
27. Umar, M., Islam, S.K.H., Mahmood, K., et al.: Provable secure identity-based anonymous and privacy-preserving inter-vehicular authentication protocol for VANETS using PUF. IEEE Trans. Veh. Technol. **70**(11), 12158–12167 (2021)
28. Habeeb, M., Kahrobaei, D., Koupparis, C., Shpilrain, V.: Public key exchange using semidirect product of (semi)groups. In: Jacobson, M., Locasto, M., Mohassel, P., Safavi-Naini, R. (eds.) ACNS 2013. LNCS, vol. 7954, pp. 475–486. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38980-1_30
29. Habeeb, M.E., Kahrobaei, D., Koupparis, C., et al.: Public key exchange using semidirect product of (semi)groups. In: Applied Cryptography and Network Security (2013)