PCP: A Pseudonym Change Scheme for Location Privacy Preserving in VANETs

Xinyang Deng 1, Tianhan Gao 1, Nan Guo 2,*, Cong Zhao 1 and Jiayu Qi 1

1 Software College, Northeastern University, Shenyang 110819, China; xinyang1121@sina.com (X.D.); gaotb@mail.neu.edu.cn (T.G.); cc598487409@gmail.com (C.Z.); yoonagoogoo@gmail.com (J.Q.)
2 Computer Science and Engineering College, Northeastern University, Shenyang 110819, China
* Correspondence: guonan@mail.neu.edu.cn

Abstract: In vehicular ad hoc networks (VANETs), pseudonym change is considered as the vital mechanism to support vehicles’ anonymity. Due to the complicated road conditions and network environment, it is a challenge to design an efficient and adaptive pseudonym change protocol. In this paper, a pseudonym change protocol for location privacy preserving (PCP) is proposed. We first present the requirements of pseudonym change in different scenarios. According to variable network states and road conditions, vehicles are able to take different pseudonym change strategies to resist the tracking by global passive adversaries. Furthermore, the registration protocol, authentication protocol, pseudonym issuance protocol, and pseudonym revocation protocol are introduced for the pseudonym management mechanism. As a consequence, it is not feasible for global passive adversaries to track a vehicle for a long time and obtain the trajectory of the vehicle. The analysis results show that the security and performance of PCP are improved compared with the traditional ones.

Keywords: VANETs; pseudonym change; location privacy

1. Introduction

The intelligent transportation system (ITS) is regarded as an important part of next-generation urban transport, which integrates a variety of advanced technologies (e.g., sensor technology, intelligent control technology) to improve convenience for drivers and pedestrians [1]. Being able to keep a stable network connection and provide a diversity of services, vehicular ad hoc networks (VANETs), as the essential part of the ITS, have had increasing attention paid to them [2]. According to the current features of urban traffic (e.g., rapid vehicle movement, uneven traffic distribution), VANETs have formed the standard in line with the future development of intelligent transportation [3], while still facing the following challenges: (1) Fast topology change: The fast-changing network topology caused by the instability of vehicle velocity has put forward more requirements for VANETs to provide stable network communication services, such as routing algorithms and congestion prediction mechanisms. (2) Non-static network density: The fast topology change causes the continuous change of the service intensity of roadside units (RSUs), which leads to a delay in responding to requests from vehicles. In addition, the instability of the signal-to-noise ratio caused by network density also affects the stability of communication. (3) Wireless communication environment: Owing to the wireless medium’s nature, it is difficult to protect the security of communication. (4) Limited communication duration: Vehicles need to avoid performing high calculations or storing excessive data to complete the authentication and data transmission as soon as possible.

Figure 1 shows the framework of VANETs. RSUs, as the roadside infrastructure, are deployed on both sides of the road. RSUs are able to collect the driving state of the surrounding vehicles, predict the traffic flow situation nearby, provide certain driving suggestions for vehicles, and support the road condition warning service. In addition, RSUs support providing network services for vehicles by connecting with the base station.
Vehicles equipped with on-board units (OBUs) can communicate with surrounding vehicles and RSUs to obtain a variety of application services. In addition, each vehicle is also secured with a GPS receiver to have an accurate location and time [4].

Figure 1. The framework of VANETs.

In order to ensure the driving safety of vehicles, vehicles are required to send the message related to their driving status regularly to surrounding vehicles and RSUs [5], e.g., basic safety message (BSM) [6]. The BSM guarantees that vehicles are aware of the danger so as to make appropriate decisions in time. However, the adversaries in the communication range are able to collect and aggregate received data through eavesdropping on the BSM. Consequently, the location privacy of vehicles and the individual privacy of vehicles owners are threatened. For the purpose of protecting vehicle location privacy, the IEEE 1609.2 standard suggests using a pseudonym instead of the real identity [7]. Accordingly, it becomes impossible to obtain the private information of the vehicle owners through utilizing the real identity of vehicles. However, if there is no effective strategy to support pseudonym change, the adversaries can still link the pseudonym and the real identity through tracking vehicles for a long time, thus invading the location privacy of vehicles [8].

Figures 2 and 3 depict the syntactic linking scenario and the semantic linking scenario of VANETs, respectively [9].

In the syntactic linking scenario, if a vehicle changes from pseudonym \( PS_1 \) to pseudonym \( PS_2 \) while other vehicles decide not to change their pseudonyms at the same time, it is obvious that the adversaries are able to determine that \( PS_1 \) and \( PS_2 \) are from the same vehicle. In the semantic linking scenario, vehicles at the intersections are required to change their pseudonyms. However, if the vehicle (holding \( PS_1 \)) does not change its trajectory or there is no vehicle with a similar driving status around the vehicle, the adversaries are still able to utilize advanced tracking algorithms to predict the location of the vehicle according to the BSM regularly sent by the vehicle. As a result, the semantic linking attack makes adversaries believe that \( PS_1 \) and \( PS_2 \) belong to the same vehicle.

Moreover, the frequency of pseudonym change is the important factor that affects the location privacy degree. The higher the frequency of pseudonym change, the better the degree of privacy protection. However, due to limited bandwidth, the frequency should not seriously hinder the performance. Consequently, it is crucial to design a secure and efficient pseudonym change scheme to guarantee that any adversaries can not associate the same vehicle with two different pseudonyms or track a certain vehicle for a long time.
Up to the present moment, a large number of pseudonym change strategies have been proposed, such as mix zones and silent periods. The core idea of these strategies is to find or create opportunities to break the continuous tracking of vehicles. However, in the silent period mechanism, the time window is limited by the interval of the BSMs. In the mix zone mechanism, the security of the pseudonym change depends on the number of pseudonyms changed synchronously in the mix zone. Moreover, the glaring issue is that the strength of the privacy protection of the above schemes heavily depends on the vehicle density within the communication range. Under low-density conditions, it is difficult to keep high location privacy. In order to address the above issues, we propose a novel pseudonym change scheme for location privacy preserving in VANETs (PCP):

(1) We improve the ID-based linearly homomorphic signature scheme and construct a pseudonym generation and aggregate protocol, where vehicles are able to calculate legitimate pseudonym certificates without the participation of the RSUs. Meanwhile, vehicles can judge the conditions for pseudonym change independently and obtain the necessary information through vehicle-to-vehicle (V2V) communication to enhance the safety of the subsequent pseudonym change protocol.

(2) The vehicle registration protocol, authentication protocol, and pseudonym revocation protocol are proposed, which guarantee that all legal vehicles are able to communicate with surrounding entities and compromised vehicles can be revealed in time.

(3) The computational cost and communication cost are adopted to evaluate the performance of the V2I authentication protocol in PCP. In addition, the vehicles in network simulation framework (Veins) is introduced to simulate the pseudonym change protocol of the proposed scheme to verify the effectiveness.

The remainder of the paper is organized as follows. Section 2 discusses the related works on pseudonym change. Section 3 revisits the preliminaries and presents the improved identity-based signature mechanism. The details of the proposed scheme (PCP) are given in Section 4. Sections 5 and 6 analyze the security and performance of PCP, respectively. Finally, we conclude the work and present the future work in Section 7.
2. Related Works

In recent years, a large number of pseudonym change schemes have been proposed. Generally, the taxonomy of pseudonym change strategies includes mix-zone-based strategies and silent-period-based strategies.

2.1. Mix-Zone-Based Strategies

This strategy requires that vehicles change their pseudonyms in fixed areas, called mix zones, where the location of the mix zones is usually determined by the RSUs. Ref. [10] proposed cryptographic mix zones (CMIX zones). In a CMIX zone, the BSMs are transmitted as ciphertext. External adversaries cannot obtain any useful information related to the pseudonym change. However, the proposed scheme does not consider the size of the anonymity set. If there are few vehicles in a CMIX zone, adversaries still have the ability to track the target vehicle with high probability. In order to solve the problem, Lu et al. suggested a mix zone that is deployed at social spots [11], such as intersections or a spot near a shopping mall. The most feasible case is the intersection with high traffic flow and traffic lights, where there are a large number of slow-moving vehicles that have enough time to change their pseudonyms. Refs. [12–14] utilized roadside infrastructure to support vehicle pseudonym changing. Ref. [12] suggested building the vehicular location privacy zone, where two infrastructures called the router and aggregator are deployed at both ends of the vehicular location privacy zone (VLPZ), which are responsible for ensuring the unlinkability of the pseudonym changing, respectively. When a vehicle arrives at the router in the VLPZ, the vehicle stops broadcasting the BSM. The router selects a lane for the vehicle randomly, and the vehicle is required to change its pseudonym before reaching the aggregator. As the exit order is different from the entering order due to random residency periods, it is difficult to link the same vehicle. Ref. [13] depended on fog computing to provide the pseudonym change service for vehicles. Different from ref. [12], the new pseudonyms for all vehicles in the mix zone are provided by the RSUs. Ref. [13] alleviated the computational cost and storage cost of the central authority to improve the efficiency of updating pseudonyms. In the above schemes, the shared key is usually adopted to resist external attacks. However, if a vehicle is compromised, the adversaries can eavesdrop on the communication message from the vehicle inside the mix zone and still be able to track the target vehicle. In order to solve this issue, ref. [14] proposed a pseudonym swap scheme based on differential privacy. When a vehicle needs to change its pseudonym, the vehicle sends the request message to the RSUs and the surrounding vehicles. Other vehicles that need to change the pseudonym send the same message to the RSUs and apply to join the pseudonym swap. The RSUs collect the request messages and use the pseudonym swap algorithm to assign a new pseudonym for each vehicle according to differential privacy. The scheme realizes a pseudonym exchange scheme where the RSUs have the ability to guarantee pseudonym indistinguishability and achieve the unlinkability between the new pseudonym and the old one. However, the heavy computation and communication costs result in the low efficiency of the scheme. In LIAP [15], vehicles are able to use the certificate from the CA to enter the security domain in the RSU. The RSU is required to periodically change the public key in the domain, and vehicles can change their pseudonyms according to the change of the public key, thereby guaranteeing that the pseudonyms are changed periodically. Nevertheless, vehicles have to communicate with the RSU before changing their pseudonyms. As a result, under special conditions, the pseudonym of vehicles cannot be changed since they cannot communicate with the RSU in time.

2.2. Silent-Period-Based Strategies

The silent-period-based strategy refers to the transition period of the pseudonym change. In a silent period, no vehicle is allowed to disclose either the old or the new identity and location [16]. Different from mix-zone-based strategies, silent-period-based strategies support the vehicles in choosing the area of the pseudonym change independently, and the time of the pseudonym change can be determined through negotiation.
among the vehicles. Normally, silent-period-based strategies require that the vehicles in VANETs establish a group through communication. These vehicles in the group determine the time and mechanism of the pseudonym change, and other vehicles outside the group cannot obtain any useful information within the group [17]. In ref. [18], vehicles detected whether the surrounding vehicles have the possibility of expected the cooperation in the pseudonym exchange by receiving the BSM. If the driving state of the surrounding vehicles is similar to the vehicle, the pseudonym change scheme will be activated. When changing the pseudonym, each vehicle is requested to broadcast a BSM with the position where the pseudonym change starts and set the speed to 0 until the pseudonym change is complete. Nevertheless, since vehicles cannot provide accurate road information to the owners, a serious impact on traffic may be caused consequently. In ref. [19], each vehicle owned a time-slotted pseudonym pool. In each time slot, only one pseudonym is legal. At the end of each time slot, vehicles are required to exchange pseudonyms to guarantee anonymity. In particular, the time of exchanging pseudonyms is determined by the driving state of the surrounding vehicles. The proposed scheme eliminates the mapping between the pseudonym and vehicle and achieves the reuse of old pseudonyms. Furthermore, due to the fixed-size pseudonym pool, the workload of the certificate authority (CA) only depends on the number of vehicles joining the network. However, the scheme does not give the details of to verify the legality of the pseudonym. Ref. [20] provided a pseudonym changing strategy (SLOW), which does not require extensive RSUs or a complex communication procedure. When the speed of the vehicle is slower than the given threshold, the vehicle stops broadcasting the BSM and any other message containing location or trajectory data and changes its pseudonym. However, if the vehicle stops broadcasting the BSM, it is difficult for other vehicles to accurately obtain the surrounding road condition information [21]. Ref. [22] proposed a cooperative pseudonym change scheme based on a trigger. In the proposed scheme, a “Readyflag” bit is inserted into the BSM. According to the value of “Readyflag” (0 or 1) in the received BSM, the vehicle determines whether to cooperate with the vehicles in the vicinity to change the pseudonym together. Ref. [22] not only enabled vehicles to obtain the willingness of surrounding vehicles to change pseudonyms in time, but also expanded the size of the anonymous set. However, ref. [22] did not give the details about how to change the pseudonym. Besides, the influence of the vehicle running state on the security of pseudonym change was not considered. Ref. [23] proposed Mix Group to solve the issue that a small group is weak in preserving privacy while a large-scale group leads to low efficiency in managing the signatures. According to the “Pareto principle”, Mix Group supports the pseudonym exchange protocol for vehicles with a common driving status under any road condition, which guarantees that the location privacy is substantially enhanced. However, the pseudonym exchange is carried out independently between vehicles. Once a vehicles is compromised, it is difficult to track the illegal vehicle. Ref. [24] gave three options: cooperative pseudonym exchange (CPE), scheme permutation (SP), and CPE plus SP (CPESP), to improve the location privacy. Vehicles are able to choose the appropriate option according to different traffic statuses. As the scheme does not give the details about the pseudonym change, we cannot determine the security of the scheme. In SPA [25], vehicles store the password issued by the TA in tamper-proof devices (TPDs). The TDP is responsible for generating and changing the pseudonyms of vehicles. However, in order to protect the privacy, vehicles have to choose the appropriate time to change the pseudonym according to the nearby road conditions. Ref. [26] adopted blockchain technology to support the location privacy preserving of vehicles (BELP). Belp removes the central authority, which effectively prevents vehicle privacy from being tampered with or leaked by internal adversaries. However, the proposed scheme does not give the details of pseudonym generation and illegal vehicle revocation. Once a vehicle misbehaves, it is critical to track the vehicle and remove it from the VANET in a timely manner.

Due to the heavy dependence on the deployment density of mix zones and the driving state of surrounding vehicles, mix-zone-based strategies lack the flexibility to support the pseudonym change. Silent-period-based strategies makes the vehicle unable to transmit or
receive accurate road condition information in time, which may affect the driving safety of the vehicle. Consequently, it is very important to design an effective mechanism to adapt to the pseudonym change in various scenarios.

3. Preliminaries
3.1. Bilinear Pairing

Let $G_1$ be the additive cyclic group of prime order $q$ with $\lambda$ bits and $G_T$ be the multiplicative cyclic group of the same order. $e : G_1 \times G_1 \rightarrow G_T$ is a bilinear pairing with the following properties [27]:

1. Bilinearity: $\forall P, Q \in G_1$ and $\forall a, b \in \mathbb{Z}_q^*$, there is $e(P^a, Q^b) = e(P, Q)^{ab}$.
2. Non-degeneracy: $\exists P, Q \in G_1, e(P, Q) \neq 1_{G_T}$.
3. Computability: $\forall P, Q \in G_1$, there exists an efficient algorithm to calculate $e(P, Q)$.

3.2. Computational Diffie–Hellman Assumption

Given a random generator $P \leftarrow G_1$, random numbers $a, b \in \mathbb{Z}_q^*$, and security parameter $\lambda$, the advantage of an algorithm $A$ in solving the computational Diffie–Hellman problem in group $G_1$ is

$$ADV_A^{CDH}(\lambda) = Pr[A(P, aP, bP) = abP]$$

We say that an algorithm $A(t, \tau)$-breaks the computational Diffie–Hellman problem in $G_1$ if $A$ runs in time at most $t$ and $ADV_A^{CDH} \geq \tau$.

3.3. Identity-Based Signature Mechanism

The identity-based signature (IBS) is a special signature where the verifier is able to verify the signature given the identity information from the signer. PCP adopts the CC signature [28] and improves Lin’s signature scheme [29] to support the anonymous authentication protocol and pseudonym change protocol, which includes a tuple of four PPT algorithms: Setup, Extract, Sign, Verify.

$(msk, params) \leftarrow \text{Setup}(1^\lambda)$. Let $G_1$, $G_T$ be the additive group and multiplicative group such that $|G_1| = |G_T| = q$. A bilinear pairing is defined by $e : G_1 \times G_1 \rightarrow G_T$.

Given three hash functions $H : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $H_1 : \{0,1\}^* \rightarrow G_1$, $H_2 : \{0,1\}^* \rightarrow G_1$, generator $P \leftarrow G_1$, and random number $x' \leftarrow \mathbb{Z}_q^*$, compute $(x, P_{pub}) \leftarrow \text{CC\_Setup}(1^\lambda)$, $P'_{pub} = x'P$. Setup$(1^\lambda)$ outputs the master key $msk = \{x, x'\}$ and the public parameters $params = \{G_1, G_T, q, e, P, P_{pub}, P'_{pub}, H_1, H_2\}$.

$SK_{ID} \leftarrow \text{Extract}(msk, 1D)$. Given the master key $msk$ and user identity $ID$, return secret key $SK_{ID} = \{SK, SK'\}$ corresponding to $ID$, where $SK = \text{CC\_Extract}(x, ID)$, $SK' = x'H_1(1D)$.

$\sigma \leftarrow \text{Sign}(ID, SK_{ID}, M_1, M_2)$. This algorithm takes the user identity $ID$, secret key $SK_{ID}$, and messages $M_1, M_2$ as the input and outputs the signature $\sigma = \{r_1, r_2, w, s\}$, where $r_1 = \text{CC\_Sign}(w)$, $r_2 = H(M_1)SK' + r(sH_1(1D) + H(M_1)H_2(M_2))$, $w = rP$, $r, s \leftarrow \mathbb{Z}_q^*$, $\{0 \text{ or } 1\} \leftarrow \text{Verify}(ID, M_1, M_2, \sigma)$. Given the signer’s identity $ID$, messages $M_1, M_2$, and signature $\sigma$, the verifier checks $\text{CC\_Verify}(ID, w, r_1, r_2, P_{pub}) = 1$ and $e(\sigma_2, P) = e(H_1(1D), P'_{pub})$. If both of the above equations hold, output 1, and 0 otherwise.

The security of the above signature algorithms is based on the CDH assumption. The formal security proof is detailed in Appendix A.2.

4. The Proposed Scheme

In this section, a pseudonym change scheme for location privacy preserving in VANETs is elaborated. Figure 4 shows the scenario and participating entities of each protocol, which include system initialization, the registration protocol, the authentication protocol, the pseudonym issuance protocol, the pseudonym change protocol, and the pseudonym...
revocation protocol. In addition, the system architecture, adversary model, and security requirements are introduced first before describing the details of the scheme. The notations and descriptions are listed in Table 1.

| Notation       | Description                                                                 |
|----------------|-----------------------------------------------------------------------------|
| ID_A           | The real identity of entity A.                                              |
| PS_i           | The i-th pseudonym of the vehicle issued by the TA. Each vehicle owns n pseudonyms PS = \{PS_i\}_{i \in \mathbb{N}}. |
| PK_i/SK_i      | The public and private key pair of vehicle A’s pseudonym PS_i.              |
| PS_{BS}        | The i-th pseudonym of the vehicle issued by the base station. Each vehicle owns w pseudonyms PS_{BS} = \{PS_{BS_i}\}_{i \in \mathbb{N}}. |
| K_{A-B}        | The session key between entity A and entity B.                              |
| Cert_{PS}      | The i-th certification of PS_{BS_i} generated by the base station.         |
| TS_i           | The i-th current timestamp.                                                 |
| N_i            | The i-th challenge value.                                                   |
| EXP            | The expiration of the pseudonym.                                            |
| H_i            | The i-th hash function.                                                     |
| Sign_{SK_i}(M)| Sign message M with the private key SK_i.                                  |
| Sig_A          | The signature generated by entity A.                                       |
| Enc_K(M)       | Encrypt message M with the key K.                                          |
| C_{A-B}        | The ciphertext generated by entity A and the ciphertext sent to entity B.   |
| num            | The number of responses received by the vehicle when it sends a pseudonym change request. |
| t_{start}, t_{end}, t_{change} | The start time, the end time of pseudonym broadcast, and the pseudonym change time, respectively. |

Figure 4. The scenario and participating entities of each protocol.

Table 1. The notations and descriptions used in this paper.

4.1. System Architecture

Figure 5 shows the system architecture of PCP, which includes four components: trust authority (TA), base station (BS), roadside unit (RSU), and vehicle.

The TA is responsible for generating public parameters, pseudonyms, and public/private key pairs for vehicles, BSs, and RSUs. In addition, when a vehicle is compromised or conducts illegal behavior, the TA can assist other entities to disclose the real identity of the vehicle and exclude the vehicle from the system in time.

The BSs are deployed in multiple regions in the city, and the RSUs in each region are managed by the BSs. Besides, in PCP, the BSs generate temporary pseudonyms for vehicles in the region.
The RSUs adopt DSRC/WAVE to connect with the vehicles in the vicinity and provide a series of application services for legal vehicles [3,30]. Meanwhile, RSUs provide the pseudonyms’ related authentication and change services for the vehicles.

The vehicles communicate with the surrounding RSUs and other vehicles to obtain the services. In order to protect vehicles’ location privacy, available strategies are required to support pseudonym changes under the four scenarios shown in Figure 4.

Figure 5. Scenarios of pseudonym change.

- **Scenario 1**: In the area with a low vehicle density and no RSUs, if there are non-negligible differences in vehicle driving statuses, it is difficult to make an effective mechanism of pseudonym change in order to resist the tracking of external attackers. However, we hope to provide an efficient mechanism to make full use of such a scenario and obtain enough useful information as much as possible, so as to provide a higher level of location privacy preserving.

- **Scenario 2**: There is a high vehicle density in this area, and RSUs exist to provide services for surrounding vehicles. In this scenario, the vehicles and RSUs can cooperate to change their pseudonyms and resist the attacks from external adversaries for protecting the location privacy of vehicles.

- **Scenario 3**: The RSUs exist, but the vehicle density is low. The RSUs can provide the pseudonym update service for vehicles that are running out of pseudonyms. Multiple pseudonym change mechanisms are available.

- **Scenario 4**: This area has a high vehicle density without RSUs. The vehicles can use the pseudonym change mechanism to change their pseudonyms through their cooperation.

Since a variety of pseudonym change schemes are proposed in Scenario 2 and Scenario 3, PCP focuses on the details of pseudonym change in Scenario 1 and Scenario 4.

4.2. Adversary Model

It is assumed that the adversaries are the global passive adversaries (GPAs). The global adversary holds the capacity to eavesdrop on the communication message of the whole network. The passive adversary refers to the adversary that does no more than eavesdropping on the communication traffic in the VANET [9]. Therefore, a GPA has the ability to eavesdrop on the BSMs of all vehicles in the region of interest. In PCP, we assume that
the GPAs know the pseudonym change strategy and vehicles are required to broadcast BSMs to vehicles in the vicinity periodically while driving, which includes the identifier, position, velocity, direction, etc. If a vehicle does not change its identifiers for a long time, the GPAs are able to eavesdrop on the BSM sent by the vehicle, track the designated vehicle, and obtain the vehicle’s trajectory and privacy via the syntactic linking attack and the semantic linking attack.

4.3. Security Requirements

In this section, we assume that the TA is honest and trustworthy, but there is no trust relationship among the other entities in the VANET. According to [8,31], the proposed scheme should meet the following goals:

- **Anonymity**: No adversary is able to extract the vehicle’s real identity from its pseudonym. The identities broadcast by vehicles are required to be anonymous within a set of potential vehicles, which ensures that no entities can obtain useful information about the real identity of vehicles. Moreover, anonymity is supposed to be conditional according to the security requirements of VANETs.

- **Unlinkability**: If the adversaries can obtain the messages sent by vehicles through monitoring, it is difficult to determine whether the consecutive received messages are sent by the same vehicle. In the pseudonym change protocol, no pseudonym should reveal any connections among vehicles.

- **Mutual authentication**: As the basic security requirement, mutual authentication focuses on identities and messages. Identity authentication means that the identity claimed by the entity is legal. Message authentication requires that the integrity of the message be able to be verified.

- **Traceability**: In a secure network architecture, it is essential to provide an efficient mechanism to trace the origin of the message. However, such a mechanism can only be effective under an authorized authority.

- **Session key agreement**: For data transmission, the confidentiality of the data is also a security requirement of VANETs. Therefore, after finishing the initial authentication, designing a session key agreement mechanism between entities in VANETs to encrypt the communication messages usually needs to be considered.

- **Location privacy**: Vehicle owners usually do not want their location to be exposed in sensitive areas. Consequently, vehicles need to change their identity information at specific areas, so that the adversaries cannot track the specific vehicle for a long time or obtain the driving trajectory.

- **DoS attack resistance**: The external adversaries are able to forge and broadcast a large number of invalid messages to consume the computational resource of the vehicles, which leads to legitimate messages possibly being dropped. As a result, it is necessary to ensure a low computational overhead for vehicles during communication.

4.4. System Initialization

During system initialization, the TA generates and broadcasts public parameters to the whole network. The details are shown as follows:

- Let $G_1$ and $G_T$ be the additive group and multiplicative group, respectively, where $|G_1| = |G_T| = q$ for the same prime order $p$. $P$ is the generator of $G_1$. Let $e$ be a bilinear pairing: $G_1 \times G_1 \rightarrow G_T$.

- Six collision-resistant hash functions are defined: $H : \{0,1\}^* \rightarrow Z_q^*$, $H_1 : \{0,1\}^* \rightarrow G_1$, $H_2 : \{0,1\}^* \rightarrow G_1$, $H_3 : \{0,1\}^* \times G_1 \rightarrow G_1$, $H_4 : \{0,1\}^* \times \{0,1\}^* \rightarrow G_1$, $H_5 : \{0,1\}^* \times G_1 \rightarrow Z_q^*$.

- The TA chooses $x, x' \leftarrow Z_q^*$ as the master key and $s \leftarrow \{0,1\}^n$ as the key of the AES-256 encryption algorithm and computes the public key $P_{pub} = xP$, $P'_{pub} = x'P$.

The TA broadcasts public parameters $\text{param}=\{G_1, G_T, q, e, P, P_{pub}, P'_{pub}, H, H_1, H_2, H_3, H_4, H_5\}$ to all entities in the system.
4.5. Registration Protocol

4.5.1. Vehicle Registration Protocol

When vehicle $v$ with $ID_v$ enters the VANET, it requests to apply for registration with the TAs. The TAs are able to generate a series of pseudonyms $\{PS_i\}_{i \in [1,n]}$, public keys $\{PK_i\}_{i \in [1,n]}$, and private keys $\{SK_i\}_{i \in [1,n]}$ for the vehicle. The protocol is performed as Figure 6 and Protocol 1.

![Vehicle registration protocol](image)

- The vehicle chooses session key $K_{v-TA} \leftarrow \{0,1\}^n$ and encrypts $K_{v-TA}$ and $ID_v$ to obtain $C_{v-TA} = Enc_{PK_{v-TA}}\{ID_v, K_{v-TA}\}$. Then, the vehicle sends $C_{v-TA}$ to the TA for registration.
- The TA uses $x$ to decrypt $C_{v-TA}$ to obtain $ID_v, K_{v-TA}$. Then, the TA chooses $\{x_i\}_{i \in [1,n]} \leftarrow Z_q^*$ and computes the corresponding pseudonyms $PS = \{PS_i\}_{i \in [1,n]}$, public keys $PK = \{PK_i\}_{i \in [1,n]}$, private keys $SK = \{SK_i\}_{i \in [1,n]}$, and the expiration $EXP = \{EXP_i\}_{i \in [1,n]}$, where $PS_i = Enc_s\{ID_v||x_i\}, PK_i = H_1(PS_i||EXP_i), SK_i = xPK_i$.
- The TA utilizes $K_{v-TA}$ to encrypt $PS, EXP,$ and $SK$ and obtains $C_{TA-v} = Enc_{K_{v-TA}}\{PS||EXP||SK\}$.
- Upon receiving the message from the TA, vehicle $v$ uses $K_{v-TA}$ to decrypt $C_{TA-v}$ to obtain $PS, EXP,$ and $SK$.

4.5.2. BS and RSU Registration Protocol

In this protocol, the BS is able to obtain its public key $PK_{BS}$, private key $SK_{BS}, SK'_{BS}$, and expiration $EXP_{BS}$, and the RSU can obtain its public/private key $PK_{RSU}/SK_{RSU}$, and expiration $EXP_{RSU}$ from the TA via a secure channel, where

$$PK_{BS} = H_1(ID_{BS}||EXP_{BS})$$
$$SK_{BS} = xPK_{BS}$$
$$SK'_{BS} = x'PK_{BS}$$
$$PK_{RSU} = H_1(ID_{RSU}||EXP_{RSU})$$
$$SK_{RSU} = xPK_{RSU}$$

Finally, the BS chooses $r_{BS} \leftarrow Z_q^*$ and computes the public key $p_{pub}^{BS} = r_{BS}P$ used in the BS domain.
Protocol 1: Vehicle registration protocol.

1: \[\begin{align*}
    & v: \\
    & \quad \text{choose } K_{v-\text{TA}} \leftarrow \{0, 1\}^n; \\
    & \quad \text{encrypt } K_{v-\text{TA}} \text{ and } ID_i \text{ to obtain } C_{v-\text{TA}} = \text{Enc}_{\text{pub}}\{ID_v, K_{v-\text{TA}}\}; \\
\end{align*}\]

2: \[\begin{align*}
    & v \rightarrow \text{TA}: C_{v-\text{TA}}; \\
\end{align*}\]

3: \[\begin{align*}
    & \text{TA:} \\
    & \quad \text{decrypt } C_{v-\text{TA}} \text{ to obtain } ID_v, K_{v-\text{TA}}; \\
    & \quad \text{choose } x_1, x_2, \ldots, x_n \leftarrow Z_q^* \\
    & \quad \text{compute } PS = \{PS_i|i \in [1, n]\}, \ PK = \{PK_i|i \in [1, n]\}, \ SK = \{SK_i|i \in [1, n]\}, \text{ where } \\
    & \quad \quad PS_i = \text{Enc}_{s}\{ID_v||x_i\} \\
    & \quad \quad PK_i = H_5(PS_i||\text{EXP}) \\
    & \quad \quad SK_i = xPK_i \\
    & \quad \text{compute } C_{\text{TA-}v} = \text{Enc}_{K_{v-\text{TA}}}\{PS||\text{EXP}||SK\}; \\
\end{align*}\]

4: \[\begin{align*}
    & \text{TA} \rightarrow v_i: C_{\text{TA-}v}; \\
\end{align*}\]

5: \[\begin{align*}
    & v: \\
    & \quad \text{decrypt } C_{\text{TA-}v} \text{ to obtain } PS, EXP, SK \\
    & \quad \text{store } PS, EXP, SK \text{ locally.} \\
\end{align*}\]

4.6. V2I Authentication and Pseudonym Issuance Protocols

When entering the signal coverage of the RSU, the vehicle is able to apply for new pseudonyms from the BS via the RSU. The RSU first verifies the legality of the vehicle through V2I authentication. If the vehicle is legal, the BS issues multiple pseudonyms for the vehicle, where these pseudonyms are valid within the scope of the BS.

4.6.1. V2I Authentication Protocol

V2I authentication supports the establishment of the trust relationship between the vehicle and RSU, as well as the construction of a secure channel. The details are depicted in Figure 7 and Protocol 2.

**Figure 7.** V2I authentication protocol.

- Vehicle \(v\) chooses \(PS_i\), \(SK_i\), and \(\text{EXP}_i\) and signs message \(PS_i, \text{EXP}_i, TS_1, N_1, \text{and } r_oP\) to obtain signature \(\text{sign}_v = \{V, W\}\), where \(r_o \in Z_q^*\), \(V = r_oH_1(PS_i||\text{EXP}_i)\), \(h = H_5(PS_i||\text{EXP}_i||TS_1||N_1||r_oP, V)\), \(W = (r_o + h)SK_i\).
- The vehicle sends \(PS_i, \text{EXP}_i, TS_1, N_1, r_oP, \text{and sign}_v\) to the RSU.
Upon receiving the message from the nearby vehicle, the RSU first checks whether $TS_1$ and $EXP$ are fresh. Then, the RSU computes $h = H_5(PS_i || EXP || TS_1 || N_1 || r_\text{v} P, V)$ and $PK_i = H_1(PS_i || EXP)$. After that, the RSU checks whether $e(P, W) = e(P_{\text{pub}}, V + h PK_i)$ holds. If the above equations are valid, the RSU believes $v$ is legal. Otherwise, the message from the vehicle is discarded. The RSU signs $ID_{RSU}, EXP_{RSU}, TS_2, N_2$, and $r_{RSU} P$ to obtain $\text{sign}_{RSU} = \{V', W'\}$, where $r_{RSU} \in Z_q^*$, $V' = r_{RSU} H_1(ID_{RSU} || \text{EXP}_{RSU})$, $h' = H_5(ID_{RSU} || \text{EXP}_{RSU} || TS_2 || N_2 || r_{RSU} P, V')$, $W' = (r_{RSU} + h') SK_{RSU}$. Finally, the RSU computes session key $K_{RSU-v} = r_{RSU} r_\text{v} P$ and encrypts $N_1$ to obtain $C_{RSU-v} = \text{Enc}_{K_{RSU-v}} \{N_1\}$.

The RSU sends $ID_{RSU}, EXP_{RSU}, TS_2, N_2$, $r_{RSU} P, \text{sign}_{RSU}$, and $C_{RSU-v}$ to $v$.

Upon receiving the message from the RSU, $v$ checks $TS_2, EXP_{RSU}$ and verifies the legality of $\text{sign}_{RSU}$ through computing $PK_{RSU}, h'$, and checking $e(P, W') \stackrel{?}{=} e(P_{\text{pub}}, V' + h' PK_{RSU})$. If the equation holds, $v_i$ computes $K_{v-\text{RSU}} = r_v r_{RSU} P$ and decrypts $C_{RSU-v}$ to obtain $N_1$. If $N_1$ is legal, $v_i$ believes RSU is legal, and the secure channel between $v_i$ and the RSU is established. Finally, $v$ encrypts $N_2$ to obtain $C_{v-\text{RSU}} = \text{Enc}_{K_{v-\text{RSU}}} \{N_2\}$.

Vehicle $v$ sends $C_{v-\text{RSU}}$ to the RSU.

The RSU decrypts $C_{v-\text{RSU}}$ and checks $N_2$. If $N_2$ is valid, the RSU believes that the secure channel between the RSU and $v$ is built.

**Protocol 2 V2I authentication protocol.**

1: $v$:
   - Choose $PS_i, SK_i, EXP$;
   - Compute
     \[
     V = r_\text{v} H_1(PS_i || EXP);
     h = H_5(PS_i || EXP || TS_1 || N_1 || r_\text{v} P, V);
     W = (r_\text{v} + h) SK_i;
     \]

2: $v \rightarrow RSU$: $PS_v, EXP_v, TS_1, N_1, r_\text{v} P$, and $\text{sign}_0 = \{V, W\}$;

3: RSU:
   - Check $EXP_v$ and $TS_1$;
   - Compute $h = H_5(PS_v || EXP || TS_1 || N_1 || r_\text{v} P, V)$ and $PK_i = H_1(PS_i || EXP)$;
   - Check $e(P, W) = e(P_{\text{pub}}, V + h PK_i)$;
   - Choose $r_{RSU} \in Z_q^*$;
   - Compute
     \[
     V' = r_{RSU} H_1(ID_{RSU} || \text{EXP}_{RSU});
     h' = H_5(ID_{RSU} || \text{EXP}_{RSU} || TS_2 || N_2 || r_{RSU} P, V');
     W' = (r_{RSU} + h') SK_{RSU};
     \]
   - Set $K_{RSU-v} = r_{RSU} r_\text{v} P$;
   - Encrypt $N_1$ to obtain $C_{RSU-v} = \text{Enc}_{K_{RSU-v}} \{N_1\}$;

4: RSU $\rightarrow v$: $ID_{RSU}, EXP_{RSU}, TS_2, N_2, r_{RSU} P, \text{sign}_{RSU}, C_{RSU-v}$;

5: $v$:
   - Check $EXP_{RSU}$ and $TS_2$;
   - Compute $h' = H_5(ID_{RSU} || \text{EXP}_{RSU} || TS_2 || N_2 || r_{RSU} P, V')$ and $PK_{RSU} = H_1(ID_{RSU} || \text{EXP}_{RSU})$;
   - Check $e(P, W') = e(P_{\text{pub}}, V' + h' PK_{RSU})$;
   - Set $K_{v-\text{RSU}} = r_v r_{RSU} P$;
   - Encrypt $N_2$ to obtain $C_{v-\text{RSU}} = \text{Enc}_{K_{v-\text{RSU}}} \{N_2\}$;

6: $v \rightarrow RSU$: $C_{v-\text{RSU}}$;

7. RSU:
   - Decrypt $C_{v-\text{RSU}}$;
   - Verify $N_2$.

4.6.2. Pseudonym Issuance Protocol

The pseudonym issuance protocol is presented as Figure 8 and Protocol 3. After finishing the V2I authentication, vehicle $v$ is able to send the message to the RSU and apply
for multiple temporary pseudonyms and certificates within the BS domain via a secure channel. When receiving the message from vehicle \( v \), the RSU forwards the message to the BS. The BS is able to generate multiple new pseudonyms, public keys, private keys, certificates, and group keys for the vehicle. Afterwards, the BS computes the session key between the BS and vehicle, encrypts the message by the session key to generate the ciphertext, and sends the ciphertext, its identity \( ID_{BS} \), and the public key \( p_{BS}^{pub} \) to the vehicle via the RSU. When receiving the message from the BS, \( v \) computes the session key between \( v \) and the BS to decrypt the ciphertext to obtain multiple new pseudonyms, public keys, private keys, certificates, and group keys from the BS. Here, \( v \) is able to use the pseudonyms issued by the BS to communicate with other entities in the BS domain and change the pseudonyms regularly to improve its anonymity. The details are depicted as follows.

**Protocol 3** Pseudonym issuance protocol.

1. \( v \):
   - compute \( C_{v-RSU} = Enc_{K_{v-RSU}}(Req_{PS}) \);
2. \( v \rightarrow RSU: \quad C_{v-RSU}, PS_i \);
3. \( RSU: \)
   - decrypt \( C_{v-RSU} \) to obtain \( Req_{PS_i} \);
   - compute \( C_{RSU-BS} = Enc_{K_{RSU-BS}}(Req_{PS} || PS_i || EXP_i || r_v P) \);
4. \( RSU \rightarrow BS: \quad ID_{RSU}, C_{RSU-BS} \);
5. \( BS: \)
   - decrypt \( C_{RSU-BS} \) to obtain \( Req_{PS_i}, EXP_i, PS_i, \) and \( r_v P \);
   - compute multiple \( PS_i^{BS}, SK_i^{BS}, PK_i^{BS}, Cert_i^{BS} \) and \( K_{BS}, K_{BS-v}, C_{BS-v} \):
     - \( PS_i^{BS} \leftarrow \{0, 1\}^n \);
     - \( SK_i^{BS} = x_i \leftarrow Z_q^* \);
     - \( PK_i^{BS} = x_i P \);
     - \( Cert_i^{BS} = \{c_1, c_i, w, s_i\} \);
     - where \( c_1 = CC_{Sign}(w) \);
     - \( c_i = H(PS_i^{BS}) SK_i^{BS} + r(s_i H_1(ID_{BS} || EXP_{BS}) + H(Ps_i^{BS}) H_2(PK_i^{BS})) \);
     - \( w = r_P \);
     - \( s_i \leftarrow Z_q^* \);
     - \( K_{BS} \leftarrow \{0, 1\}^n \);
     - \( K_{BS-v} = r_{BS-v} P \);
     - \( C_{BS-v} = Enc_{K_{BS-v}}(PS_i^{BS} || SK_i^{BS} || PK_i^{BS} || Cert_i^{BS}) || K_{BS} \);
   - store \( PS_i^{BS}, SK_i^{BS}, PK_i^{BS}, Cert_i^{BS}, K_{BS}, ID_{BS} \), and \( p_{BS}^{pub} \) in pseudonym list;
6. \( BS \rightarrow v: \quad ID_{BS}, C_{BS-v}, p_{BS}^{pub} \);
7. \( v: \)
   - compute \( K_{v-BS} = r_op_{BS}^{pub} \) and decrypts \( C_{BS-v} \);
   - store \( PS_i^{BS}, PK_i^{BS}, SK_i^{BS}, Cert_i^{BS}, K_{BS}, ID_{BS} \), and \( p_{BS}^{pub} \) in pseudonym list.

- In order to apply for multiple temporary pseudonyms and certificates within the BS, vehicle \( v \) uses session key \( K_{v-RSU} \) to encrypt request \( Req_{PS_i} \) to obtain ciphertext \( C_{v-RSU} = Enc_{K_{v-RSU}}(Req_{PS_i}) \).
- Vehicle \( v \) sends \( C_{v-RSU} \) to the RSU.
- When obtaining the ciphertext from vehicle \( v \), the RSU uses session key \( K_{RSU-BS} \) to decrypt \( C_{v-RSU} \) to obtain the request \( Req_{PS_i} \). Then, the RSU uses the session key between the RSU and BS \( K_{RSU-BS} \) to encrypt \( Req_{PS_i}, PS_i, EXP_i, \) and \( r_v P \) and obtain \( C_{RSU-BS} \).
- The RSU sends ciphertext \( C_{RSU-BS} \) to the BS.
- The BS decrypts \( C_{RSU-BS} \) and obtains \( Req_{PS_i}, PS_i, EXP_i, \) and \( r_v P \). Then, multiple temporary pseudonyms \( PS_i^{BS} \leftarrow \{0, 1\}^n \), multiple random numbers \( x_i \leftarrow Z_q^* \), group
key $K_{BS} \leftarrow \{0,1\}^n$, and $r, s_i \leftarrow \mathbb{Z}_q^*$ are selected and the private key $SK_i^{BS}$, public key $PK_i^{BS}$, and certificate $Cert_i^{BS}$ are computed, where

\begin{align*}
SK_i^{BS} &= x_i, \\
PK_i^{BS} &= x_i P, \\
\sigma &= CC_{\text{sign}}(w), \\
\sigma_i &= H(PS_i^{BS})SK_i^{BS} + r(s_i H_1(ID_{BS}||EXP_{BS}) + H(PS_i^{BS})H_2(PK_i^{BS})), \\
Cert_i^{BS} &= \{\sigma_1, \sigma_2, w, s_i\}
\end{align*}

The BS sets the session key $K_{BS-v} = r_{BS}^v P$ and encrypts $PS_i^{BS}$, $SK_i^{BS}$, $PK_i^{BS}$, and $K_{BS}$ to obtain ciphertext $C_{BS-v}=\text{Enc}_{K_{BS-v}}(PS_i^{BS}||SK_i^{BS}||PK_i^{BS}||K_{BS})$. Finally, the BS stores $PS_i^{BS}$, $SK_i^{BS}$, $PS_i$, $EXP_{BS}$.

- The BS sends $C_{BS-v}$, $ID_{BS}$, and $P_{pub}$ to vehicle $v$ via the RSU.
- After receiving the ciphertext from the BS, vehicle $v$ computes the session key $K_{v-BS} = r_{v_{pub}}^{PS}$ and decrypts $C_{BS-v}$ to obtain the message from the BS. Finally, vehicle $v$ stores $PS_i^{BS}$, $PK_i^{BS}$, $SK_i^{BS}$, $Cert_i^{BS}$, $K_{BS}$, $ID_{BS}$, and $P_{pub}$ locally.

**Figure 8.** Pseudonym issuance protocol.

### 4.7. Pseudonym Change Protocol

When vehicle $v_i$ runs on the road, it is requested to broadcast the BSM with $PS_i^{BS}$. If meeting other vehicles in the BS domain, vehicle $v_i$ believes that there is a chance to change its pseudonym. Now, $v_i$ is able to broadcast a pseudonym change request and try to communicate with other vehicles in the vicinity to change its pseudonym. Different from the traditional mix zone mechanism, the proposed pseudonym change protocol does not need the assistance of the RSUs, which means all vehicles in the BS domain can change their pseudonyms independently.

The pseudonym change protocol includes two periods: pseudonym sharing period and pseudonym change period. In the pseudonym sharing period, vehicles share their own stored pseudonyms, certificates, and driving status. If the number of pseudonyms received is not enough or there are considerable differences in the driving among vehicles, vehicles only store the information received. Otherwise, vehicles store the information received and start the pseudonym change period. In this period, all vehicles change their pseudonyms and communicate with other entities as group members. The details of the pseudonym change protocol are depicted as Figure 9 and Protocol 4:
• Vehicle $v_i$ selects pseudonym $PS_i^{BS}$, public key $PK_i^{BS}$, and certificate $Cert_i^{BS}$ and computes signature $Sign_{v_i} = \text{sign}_{SK_i^{BS}}\{PS_i^{BS}|PK_i^{BS}|TS_i|t_{start}|t_{end}|t_{change}|\text{change~request}\}$, where $TS_i$ is the current timestamp and $change~request$ is the pseudonym change request.

• Vehicle $v_i$ broadcasts $PS_i^{BS}$, $PK_i^{BS}$, $TS_i$, $t_{start}$, $t_{end}$, $t_{change}$, $Cert_i^{BS}$, $Sign_{v_i}$, and $change~request$ to other surrounding vehicles.

• When receiving the request from vehicle $v_i$, the vehicle in the vicinity (e.g., $v_j$) checks the freshness of timestamp $TS_j$ and the legality of signature $Sign_{v_j}$. If the above verification is successful, $v_j$ updates the pseudonym certificate list $PS - Cert - List_j$ and computes the ciphertext $Msg = \text{Enc}_{K_{BS}}\{PS - Cert - List_j\}$.

• When the current time $t \geq t_{start}$ and $t < t_{end}$, $v_i$ broadcast the ciphertext to surrounding vehicles.

• Surrounding vehicles $v_k$ (including $v_j$) decrypt $Msg$ and add $PS_j^{BS}$, $PK_j^{BS}$, and $Cert_j^{BS}$ into $PS - Cert - List_k$.

• Finally, if $num \geq \text{threshold}$, all vehicles compute $Cert^{BS} = \sum_{i=1}^{num} Cert_i^{BS} = \{\sigma_1, \sigma_2\}$, where $\sigma_2 = \sum_{i=1}^{num} \sigma_i$, $PK^{BS} = PK^{BS} \cup PK_j^{BS}$, $PS^{BS} = PS^{BS} \cup PS_i^{BS}$, and change pseudonym $PS^{BS}$ and certificate $Cert^{BS}$ after $t_{change}$.

**Protocol 4** Pseudonym change protocol.

1: $v_i$:
   
   compute $Sign_{SK_i^{BS}}\{PS_i^{BS}|PK_i^{BS}|TS_i|t_{start}|t_{end}|t_{change}|\text{change~request}\}$

2: $v_i$ → other vehicle (e.g., $v_j$):
   
   broadcast $PS_j^{BS}$, $PK_j^{BS}$, $TS_j$, $t_{start}$, $t_{end}$, $t_{change}$, $Cert_j^{BS}$, $Sign_{v_j}$, $change~request$;

3: $v_j$:
   
   verify pseudonym changing request $request_j$;
   
   update and add new $PS_j^{BS}$, $PK_j^{BS}$, $Cert_j^{BS}$ into $PS - Cert - List_j$;
   
   compute $Msg = \text{Enc}_{K_{BS}}\{PS - Cert - List_j\}$;

4: $v_j$ → surrounding vehicle (e.g., $v_k$): $Msg$

5: $v_k$:
   
   decrypt $Msg$;
   
   add $PS_j^{BS}$, $Cert_j^{BS}$ from $PS - Cert - List_j$ into $PS - Cert - List_k$;
   
   compute $Cert^{BS} = \sum_{i=1}^{num} Cert_i^{BS} = \{\sigma_1, \sigma_2\}$, where $\sigma_2 = \sum_{i=1}^{num} \sigma_i$;

   $PS^{BS} = PS^{BS} \cup PS_i^{BS}$,

   $PK^{BS} = PK^{BS} \cup PK_j^{BS}$;

6: all vehicles:
   
   if $num \geq \text{threshold}$ then
   
   all vehicles change pseudonym $PS^{BS}$ and certificate $Cert^{BS}$ after $t_{change}$;

   end if

The number of vehicles changing pseudonyms depends on the current user-centric location privacy level (as depicted in Section 5.3.2). When the location privacy level of the vehicle is low, the vehicle has to share more pseudonyms. When the user-centric location privacy is at a high level, the vehicle does not need to sacrifice too many pseudonyms to protect its privacy. In addition, due to the limited communication range of the BS, when the vehicle is driven from one BS (e.g., $BS_1$) to another BS (e.g., $BS_2$), the vehicle is required to reapply to $BS_2$ for the new pseudonym list. Therefore, the number of pseudonyms only needs to guarantee the privacy and security of vehicles within the BS domain.
4.8. Pseudonym Revocation Protocol

Generally, the pseudonym revocation protocol is used in the following conditions:

1) The vehicle’s pseudonym and certificate have expired. In the pseudonym issuance protocol, $K_{BS}$ is required to be regularly updated by the BS and the period of the availability of $K_{BS}$ cannot be longer than that of $EXP_i$. Since the BS issues enough pseudonyms to the vehicles, the validity period of $K_{BS}$ can be set long enough, which can reduce the communication overhead caused by the frequent requests for new pseudonyms. However, once $K_{BS}$ or $EXP_i$ expires, vehicles have to reapply for new pseudonyms from the BS or TA.

2) Legal vehicles are compromised. In PCP, two cuckoo filters [32] are used and maintained by the BS: the positive filter $pos_{filter}$ and the negative filter $neg_{filter}$, where $pos_{filter}$ stores the valid pseudonyms and $neg_{filter}$ stores the illegal pseudonyms. After receiving the illegal vehicles’ information including signature $\sigma$, message $M$, multiple group pseudonyms $PS_{BS}$, and $proof$, the BS queries the local pseudonym list and obtains the multiple private keys $SK_{BS}$ according to $PS_{BS}$ firstly. Then, the BS computes the signatures of $M$ to obtain $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$, respectively. If $\sigma_i = \sigma$, the BS believes that the pseudonym $PS_{BS_i}$ and private key $SK_{BS_i}$ corresponding to $\sigma_i$ are the identity information of the illegal vehicle. After that, the BS selects all pseudonyms $PS_i$ issued by the BS and the pseudonym issued by the TA about the illegal vehicle, removes these pseudonyms from $pos_{filter}$, and adds them to $neg_{filter}$ to exclude the illegal vehicles from the VANET. The BS further broadcasts two filters in the BS domain via the RSU. Finally, the BS sends $PS_i$ to the TA and reveals the real identity of the illegal vehicle. When receiving the message from the BS, the TA decrypts $PS_i$ to obtain the real identity $ID_i$. The TA sends all pseudonyms related to the illegal vehicles to the BS and prevents the illegal vehicles from reapplying for new pseudonyms.

5. Performance Analysis

In this section, we discuss the performance of the proposed scheme in V2I authentication in terms of the computational cost and communication cost compared with LIAP [15] and SPA [25]. In addition, the Veins simulation framework is adopted to conduct the simulation experiment in terms of the average anonymous set size and user-centric location privacy level to manifest the security of the proposed pseudonym change protocol.
5.1. Computation Cost

The computational cost is defined to evaluate the total computation time required for pseudonym change, which is mainly dominated by hash-to-point ($T_{\text{htp}}$), point exponentiation ($T_{\text{exp}}$), point multiplication ($T_{\text{mul}}$), and bilinear pairing ($T_{\text{bp}}$) all over the group.

In LIAP, given system parameters $\{p, q, G_1, G_2, e, PK_{\text{CA}}, H, h\}$, where $H : \{0, 1\}^* \rightarrow Z_q^*$ and $h$ is the one-way hash function, such as SHA-2, the RSU broadcasts message $M = \{PK_{\text{R}}, \text{Cert}_{\text{R}}, T, RPK_1, RPK_2, RPK_{1^{-1}}, RPK_{2^{-1}}, RPK_{1^{+1}}, RPK_{2^{+1}}\}$, and $\sigma_r$, where $\text{Cert}_{\text{R}} = \text{Sign}_{\text{CA}}\{PK_{\text{R}}\}$ is the certificate of the public key $PK_{\text{R}}$ of the RSU, $T$ is the timestamp of the message, $\sigma_r = \text{Sign}_{\text{RSU}}(PK_{\text{R}}, \text{Cert}_{\text{R}}, T)$, and signature $\sigma_r = \text{Sign}_{\text{RSU}}(PK_{\text{R}}, \text{Cert}_{\text{R}}, T)$ and obtains $\text{Cert}_{\text{RSU}}$. Then, the RSU verifies the legality of $\sigma_r$. If the above verification is successful, the RSU believes that the vehicle is legal; otherwise, the message will be dropped. Since LIAP does not give the detail of the certification and signature generation mechanisms, we adopted the same CC signature mechanism as PCP and the BF-IBE encryption algorithm to derive the computational cost of LIAP.

In SPA, the RSU is used as the fog–edge node (FEN) to provide the communication service for the vehicles. Given public parameter $\{p, q, a, b, G_1, G_2, e, P, Q, Q', h_1, h_2, h_3\}$, when entering in the communication range of the RSU, vehicle $v = (W_{\text{RSU}}, h_1, h_2, h_3)$, $v$ believe the RSU is legal, $v$ uses $PK_{\text{R}}$ to encrypt the vehicle’s public key $PK_v$, $\text{Cert}_v$, $\text{timestamp}$ $T'$, and signature $\sigma_v = \text{Sign}_{\text{RSU}}(PK_{\text{R}}, \text{Cert}_{\text{R}}, T')$ and obtains $\text{Cert}_{v-\text{RSU}}$. When receiving the message from the vehicle, the RSU first decrypts $\text{Cert}_{v-\text{RSU}}$ and checks $T'$. Then, the RSU verifies the legality of $\sigma_v$. If the above verification is successful, the RSU believes that $v$ is legal; otherwise, the message will be dropped. Since LIAP does not give the detail of the certification and signature generation mechanisms, we adopted the same CC signature mechanism as PCP and the BF-IBE encryption algorithm to derive the computational cost of LIAP.

In PCP, vehicle $v$ generates signature $\text{sign}_v = \{V, W\}$ and sends $PS_v, EXP_v, TS_1, N_1, r_v, P, \text{sign}_v$ to the RSU, where $V = r_v H_1(PS_1 || \text{EXP}_1), h = H_5(PS_1 || TS_1 || N_1 || r_v, P, V), W = (r_v + h)SK_i$. When obtaining the message from $v$, the RSU computes $h$ and $PK_v$. Then, the RSU checks the equation $e(P, W) = e(P_{\text{pub}}, V + hPK_v)$. If the equation holds, the RSU believes $v$ is legal. Afterwards, the RSU signs $ID_{\text{RSU}}, EXP_{\text{RSU}}, TS_2, N_2$, and $r_{\text{RSU}}P$ to obtain $\text{sign}_{\text{RSU}} = \{V', W'\}$, where $V' = r_{\text{RSU}} H_1(ID_{\text{RSU}} || \text{EXP}_{\text{RSU}}), h' = H_5(ID_{\text{RSU}} || TS_2 || N_2 || r_{\text{RSU}}P, V'), W' = (r_{\text{RSU}} + h')SK_{\text{RSU}}$. After that, the RSU sends $ID_{\text{RSU}}, TS_2, N_2, r_{\text{RSU}}P, \text{sign}_{\text{RSU}}$, and $C_{\text{RSU}}$ to $v$. $v$ computes $h'$, $PK_{\text{RSU}}$ and verifies the legality of the RSU by checking $e(P, W') = e(P_{\text{pub}}, V + h'PK_{\text{RSU}})$.

Table 2 depicts the comparisons of the computational costs for the vehicle and RSU. In LIAP, in order to protect the public key and certificate of the vehicle from being exposed, the vehicle is requested to use the public key of the RSU to encrypt its certificate and public key, which leads to extra computational cost. Since the complicated signature mechanism is adopted, the V2I authentication protocol in SPA requires the vehicle and RSU to execute more point multiplications and bilinear pairing operations, causing a high computational cost. In PCP, the identity-based signature mechanism is adopted, so the computational cost of the hash-to-point operation becomes the vital factor for the efficiency of V2I authentication.
We used the Veins simulation framework to conduct extensive simulations, through the RandomTrips Python script was adopted to generate random vehicle trips. A SUMO configuration file was edited to simulate the scenario of pseudonym change depicted in Figure 5 (Simulation 1). In addition, a road map of Xi’an from OpenStreetMap (OSM) [36] was chosen as the real simulation scenario (Simulation 2). The road map from OSM can be converted into the network file by NETCONVERT. POLYCONVERT was used to generate the topographic file. The RandomTrips Python script was adopted to generate random vehicle trips. A SUMO configuration file was edited to integrate the network file, topographic file, and vehicle trips file. The SUMO simulation from the real map and Veins simulation are shown in Figure 10. The parameters used in the simulations are shown in Table 3.

Table 2. Comparison of the computational cost.

| Algorithm | LIAP | SPA | PCP |
|-----------|------|-----|-----|
| RSU-Gen   | $2T_{PM}$ | $3T_{PM}$ | $3T_{PM}$ |
| RSU-Ver   | $5T_{BP} + 3T_{PM}$ | $3T_{BP} + 3T_{PM}$ | $2T_{BP} + T_{PM} + T_{MTP}$ |
| V-Gen     | $T_{BP} + 3T_{PM} + T_{PE}$ | $3T_{PM}$ | $3T_{PM}$ |
| V-Ver     | $4T_{BP} + 2T_{PM}$ | $3T_{BP} + 3T_{PM}$ | $2T_{BP} + T_{MP} + T_{MTP}$ |
| Total     | $10T_{BP} + 10T_{PM} + T_{PE}$ | $6T_{BP} + 12T_{PM}$ | $4T_{BP} + 8T_{PM} + 2T_{MTP}$ |

5.2. Communication Cost

The communication cost refers to the total size of the message transmitted during authentication. According to [33], the size of each single element in $G_1$ and $Z_q^*$ is 128 bytes and 40 bytes, respectively. The sizes of the expiration and timestamp are 4 bytes. In the authentication protocol, since LIAP and SPA only transmit authentication-related messages and ignore the necessary messages to establish a secure channel, we only considered the communication cost related to V2I authentication.

In LIPA, the RSU broadcasts message $M = \{PK_R, Cert_R, T, M_{RPK}\}$, $\sigma_r$, where $|PK_R| = |G_1|$, $|Cert_R| = 2|G_1|$. The vehicle sends $C_{v-RSU}$ to the RSU, where $|C_{v-RSU}| = 3|G_1| + |TS|$. Thus, the total communication cost of LIAP is:

$$6 \times |G_1| + 2|TS|$$

In SPA, the vehicle needs to send $PID_v, M_v$, and signature $\mu_v = \{T_v, U_v\}$ to the RSU for authentication, where $|PID_v| = |Z_q^*|$, $|T_v| = |U_v| = |G_1|$. After verifying the message, the RSU sends $RID_{FEN}, M_{FEN}$ and signature $\mu_{FEN} = \{T_{FEN}, U_{FEN}\}$ to the vehicle, where $|RID_{FEN}| = |Z_q^*|$, $|T_{FEN}| = |U_{FEN}| = |G_1|$. Consequently, the communication cost of SPA is:

$$4 \times |G_1| + 2|TS| + 2 \times |Z_q^*|$$

In PCP, the vehicle sends $PS_i, TS_1$, and $\text{sign}_{v}$ to the RSU. When finishing the verification of the received message, the RSU sends $ID_{RSU}, TS_2$, and $\text{sign}_{RSU}$ to the vehicle, where $|PS_i| = |ID_{RSU}| = |Z_q^*|$, $|\text{sign}_{v}| = |\text{sign}_{RSU}| = 2|G_1|$. Thus, the communication cost of PCP is:

$$4 \times |G_1| + 2|TS| + 2 \times |Z_q^*|$$

We can see that PCP and SPA have a low communication cost. In LIPA, the vehicle and RSU are requested to send extra certificates and public keys, which causes a high communication cost.

5.3. Simulation

In this section, Veins [34] is introduced to evaluate PCP in terms of the average anonymous set size and the average strength of location privacy. The proposed protocols were implemented using C++, where the experimental environment included a 2.6 GHz Intel(R) Core(TM) i7-6700HQ CPU, 2GB RAM, and the Debian 9.4 operating system. The Pairing Based Cryptography Library [35] was adopted to implement the cryptographic operations. We used the Veins simulation framework to conduct extensive simulations, through the tools of SUMO and OMNET++. A SUMO network file was edited to simulate the scenario of pseudonym change depicted in Figure 5 (Simulation 1). In addition, a road map of Xi’an from OpenStreetMap (OSM) [36] was chosen as the real simulation scenario (Simulation 2). The road map from OSM can be converted into the network file by NETCONVERT. POLYCONVERT was used to generate the topographic file. The RandomTrips Python script was adopted to generate random vehicle trips. A SUMO configuration file was edited to integrate the network file, topographic file, and vehicle trips file. The SUMO simulation from the real map and Veins simulation are shown in Figure 10. The parameters used in the simulations are shown in Table 3.
5.3.1. Average Anonymous Set Size

The average anonymous set size is defined as the set of available candidate pseudonyms that are used in the pseudonym change protocol [14]. The larger the set of pseudonyms, the better it is able to confuse the tracking of GPAs. Figures 11 and 12 show the average anonymous set size in Simulation 1 and Simulation 2, respectively.

In Figure 11, the vehicle switches to the different scenarios shown in Figure 5 every 15 s. In Scenario 1 of Figure 5, since there are not enough vehicles to guarantee that the vehicles’ anonymity set meets the pseudonym change security requirements and there is no RSU to provide pseudonym change support, the PCP, mix zone and silent period schemes cannot support pseudonym change in Scenario 1. However, in order to evaluate Scenario 1 for the effect of pseudonym change in subsequent scenarios, Scenario 1 is supplemented during the switching process of Scenarios 2–4. In Scenario 2, the above three schemes are able to support pseudonym change. Mix zones support more vehicles participating in pseudonym change than silent periods due to the wider communication range of RSUs. Since the vehicle collects more pseudonyms form other vehicles in Scenario 1, PCP guarantees providing larger pseudonym sets in Scenario 2. In Scenario 3, due to the low numbers of vehicles, the silent period scheme cannot protect the location privacy of vehicles that want to change pseudonyms. Because the RSU is not deployed, mix zones cannot provide the pseudonym change service for vehicles in Scenario 4.
In Figure 12, we can see that the average anonymous set size increases rapidly due to the pseudonym change protocol. However, more notably, we observe that the vehicle density and traffic conditions have a significant impact on the anonymous set size since the vehicles have a greater chance to communicate with surrounding vehicles and share local pseudonym sets. The denser traffic conditions make it easier for the vehicle to meet other vehicles with a similar driving status. Moreover, the average anonymous set size in mix zones depends entirely on the deployment density of the RSUs. However, the high-density deployment of the RSUs requires a very high cost in a short time, which makes the silent period and PCP more suitable for the actual traffic scene. Meanwhile, as it depends on the number of pseudonyms shared by the vehicles in the communication group rather than the number of vehicles, PCP has a higher average anonymous set size compared with the silent period.

![Figure 11. Average anonymous set size (Simulation 1).](image1)

![Figure 12. Average anonymous set size (Simulation 2). (a) Vehicle number $N = 50$. (b) Vehicle number $N = 100$. (c) Vehicle number $N = 300$.](image2)
5.3.2. User-Centric Location Privacy Level

The user-centric location privacy level [37] of the vehicles in VANETs is modeled by the location privacy loss function $\beta_i(t, T_i) : (IR^+, IR^+) \rightarrow IR^+$, where $t$ and $T_i$ refer to the current time and the time when $v_i$ changes pseudonym successful. According to a sensitivity parameter $0 < \lambda_i < 1$, the privacy loss is set 0 initially and increases with the time. The higher the value of $\lambda_i$, the faster the rate of privacy loss is. The privacy loss function is defined as

$$\beta_i(t, T_i) = \begin{cases} \lambda_i \cdot (t - T_i) & \text{for } T_i \leq t < T_{i}^{\text{max}} \\ A_i(T_i) & \text{for } T_{i}^{\text{max}} \leq t \end{cases}$$

where $T_{i}^{\text{max}}=\frac{A_i(T_i)}{\lambda_i} + T_i$ refers to the time when the privacy loss function arrives at the maximal value. Given the location privacy loss function, the user-centric location privacy level of vehicle $v_i$ at time $t$ is

$$A_i(t) = A_i(T_i) - \beta_i(t, T_i), t \geq T_i$$

Since vehicles cannot compute $A_i(T_i)$, an approximation $\log_2(n)$ was used in the simulation [37].

Figure 13 gives the result of the user-centric location privacy level in different scenarios from Figure 5, where $\lambda$ is defined as 0.1 and 0.8. Before changing the pseudonym, the user-centric location privacy level of each vehicle decreases linearly. Consequently, in Scenario 1 and other scenarios that do not meet the pseudonym change, the user-centric location privacy level of each vehicle gradually decreases and rises after changing pseudonym. Moreover, since the user-centric location privacy level is positively correlated with anonymous integration, the growth trend of the location privacy protection level is consistent with Figure 11.

![Figure 13. User-centric location privacy level (Simulation 1).](image)

Figure 14 shows the changes in the user-centric location privacy level of PCP, mix zones, and silent periods under different traffic conditions, respectively. We can see that the location privacy level increases dramatically at the beginning and remains stable after about 40 s. The greater the number of vehicles, the shorter the time for the user-centric location privacy level to reach the high level. Since silent periods and mix zones have more stringent requirements on pseudonym change conditions (e.g., slow speed, RSU deployment), PCP is able to improve the location privacy level faster than the other two schemes and maintains a high location privacy level.
6. Discussion

Aiming at the uneven distribution of vehicle density and low-density RSU deployment, this paper proposed a pseudonym change scheme for location privacy preserving in VANETs (PCP). PCP follows the 1609 standard proposed by the IEEE and is able to effectively guarantee the protection of the privacy of vehicles. However, there are several open problems that need to be addressed to support the large-scale deployment of VANETs:

- **Mac address change**: PCP supports the pseudonym change in the application layer. However, according to the 1609.4 standard [38], in order to protect the full location privacy and security of the vehicle, it is necessary to propose an effective mechanism to support the change of MAC address. Otherwise, only the pseudonym is changed, and the adversaries can still be associated with the tracked vehicle through the MAC address.

- **Beacon interval**: According to DSRC, each vehicle periodically broadcasts a BSM every 100–300 milliseconds [39,40]. Thus, the period of pseudonym change has to be limited to the beacon interval. However, a long time interval may cause the vehicle to be unable to obtain the driving status of the surrounding vehicles in time, and a short time interval cannot guarantee that the vehicle has enough time to change its pseudonym through cooperation. It is vital for VANETs to support an efficient beacon strategy.

- **Non-cooperative behavior**: The cooperation among vehicles is a key factor for a successful pseudonym changing strategy. However, due to the costs that are involved in changing the pseudonym, some vehicles may not be willing to cooperate with other vehicles. Therefore, how to improve the willingness of vehicles to change pseudonyms and ensure that the pseudonyms can be changed at a high location privacy level need to be further researched.
7. Conclusions

In this paper, we proposed a pseudonym change scheme for location privacy preserving in VANETs (PCP) to address the issue of location privacy. PCP first proposes a registration protocol, authentication protocol, and pseudonym revocation protocol to guarantee that all legal vehicles are able to communicate with surrounding entities and compromised vehicles can be revealed in time. Furthermore, we improved the ID-based linearly homomorphic signature scheme to support vehicle pseudonym change in various conditions, which can protect vehicle location privacy more effectively. Security and performance analysis showed that PCP is able to resist attacks from GPAs and keep a high location privacy level.

Our work leaves several open problems to be solved, for example designing an efficient signature mechanism to support vehicle anonymous communication and how many pseudonyms should a vehicle store to keep the balance between vehicle communication security and performance. In the future, we will focus on the above issues.

Author Contributions: Conceptualization, X.D.; methodology, X.D.; software, J.Q.; validation, J.Q. and C.Z.; formal analysis, T.G. and N.G.; investigation, T.G.; resources, X.D.; data curation, C.Z.; writing—original draft preparation, X.D.; writing—review and editing, T.G. and. N.G.; visualization, X.D.; supervision, T.G.; project administration, T.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China grant number 52130403 and the Fundamental Research Funds for the Central Universities grant number N2017003.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Security Analysis

In this section, we first prove the correction of certificate Cert_{BS} in the pseudonym change protocol, which is able to guarantee the legality of the vehicle after changing the pseudonym. Then, the formal security proof is conducted to show that the certificate generation mechanism executed by the BS in the pseudonym generation protocol is secure. Finally, the necessary security requirements are also discussed.

Appendix A.1. Correctness

Theorem A1. In the pseudonym change protocol, the certificate generation is correct if the algorithm Verify outputs 1.

Proof. For pseudonyms and certificates of multiple vehicles: $<P_{BS1}, Cert_{BS1}>, <P_{BS2}, Cert_{BS2}>, \ldots, <P_{BSnum}, Cert_{BSnum}>, \sigma_2$ in the certificate $Cert_{BS}$ generation and verification is computed as follows.

$$\sigma_2 = \sum_{i=1}^{num} \sigma_i$$

$$= \sum_{i=1}^{num} (H(P_{BS_i}) \cdot SK'_{BS} + r(s_i \cdot H_1(ID_{BS_i}||EXP_{BS}) + H(P_{BS_i}) \cdot H_2( PK^i_{BS})))$$

$$= (SK'_{BS}) \sum_{i=1}^{num} H(P_{BS_i}) + r((\sum_{i=1}^{num} s_i) \cdot H_1(ID_{BS_i}||EXP_{BS}) + (\sum_{i=1}^{num} H(P_{BS_i}) \cdot H_2( PK^i_{BS})))$$

Given pseudonyms $<P_{BS1}, P_{BS2}, \ldots, P_{BSnum}>, <s_1, s_2, \ldots, s_{num}>, w, ID_{BS}, EXP_{BS}$, and $P'_{pub}, \sigma_2$ are verified through checking
Theorem A2. Given the additive group and multiplicative group $G_1$ and $G_T$, where $|G_1| = |G_T| = q$, if there exists a PPT adversary $A$ for adaptively chosen message attacks with a runtime at most $t$, making at most $q_t$ extracted queries with the advantage $\epsilon$, then the adversary $A$ is able to construct algorithm $A_1$ to break the CDH assumption, where the advantage is at least $\epsilon(1 - 1/q)/(eq.)$.

Proof. A game is designed to confirm that the proposed certificate generation algorithm is provably secure. Define $\delta$ to be the probability distribution over $\{0, 1\}$, where 1 is drawn with probability $\delta$ and 0 with probability $(1 - \delta)$. The specific proofs are: $A_1$ is given a challenge $(P, aP, bP)$. $A_1$ runs $(x, P_{pub}) \leftarrow CC_{Setup}(1^\lambda)$ as the master key and public key of the whole system and sets $P_{pub}' = aP$. Then, $A_1$ sends system parameters $\text{param} = \{p, G_1, G_T, P, P_{pub}, P_{pub}' , H, H_1, H_2\}$ to $A$ and responses as follows.

$H$-queries: Assume $A$ makes $H$-queries at most $q_H$ times. A queries message $M_i$ to the $H$-oracle; $A_1$ chooses $h_i \leftarrow Z_q^*$ and adds $(M_i, h_i)$ to the $H$-List and responds $h_i$ to $A$.

$H_1$-queries: Assume $A$ makes $H_1$-queries at most $q_{H_1}$ times. A queries $ID_i$ to the $H_1$-oracle; $A_1$ responds as follows.

1) If $ID_i$ already exists in $H_1$-List, $A_1$ answers $H_1(ID_i)$.

2) Otherwise, $A_1$ flips a coin $c_i \in \{0, 1\}$. If $c_i = 0$, then $A_1$ selects $k_i \leftarrow Z_q^*$ and computes $H_1(ID_i) = k_iP$; otherwise, $A_1$ sets $k_i = b$, $H_1(ID_i) = bP$. $A_1$ adds $(ID_i, H_1(ID_i), c_i, k_i)$ to the $H_1$-List and returns $H_1(ID_i)$ as the answer from $A$ (when $k_i = b$, the value of $k_i$ is unknown).

$H_2$-queries: Assume $A$ makes $H_2$-queries at most $q_{H_2}$ times. A queries message $M'_i$ to the $H_2$-oracle; $A_1$ chooses $\alpha_i, \beta_i \leftarrow Z_q^*$ and sets $H_2(M'_i) = \alpha_i bP + \beta_i P$. Then, $A_1$ adds $(M'_i, H_2(M'_i), \alpha_i, \beta_i)$ to the $H_2$-List and responds $H_2(M'_i)$ to $A$.

Extract queries: Assume $A$ makes extract queries at most $q_t$ times. When $A$ requests the private key for $ID_i$, $A_1$ queries $H_1$-List to obtain $k_i$ according to $ID_i$. If $c_i = 0$, $A_1$ computes $SK_i \leftarrow CC_{Extract}(k_i, ID_i)$ and $SK'_i = a(H_1(ID)) = a(k_i P) = k_i (P_{pub}' )$ and returns it to $A$; otherwise, $A_1$ aborts.
Theorem A3. Security Analysis

Given $r_i, s_i \leftarrow \mathbb{Z}_q^n$ and computes $\sigma_i = \{\sigma_{i-1}, \sigma_{i-2}, w_i, s_i\}$, where $w_i = r_i P, \sigma_{i-1} \leftarrow \text{CC\_Sign}(ID_i, w_i), \sigma_{i-2} = h SK_i + r_i (s_i H_i(ID_i) + h_i H_2(M'_i))$. A returns $\sigma_i$ to $A$ as the response and stores $(r_i, w_i)$ in table $L$.

Output. A outputs a signature $\sigma = \{\sigma_{\tau-1}, \sigma_{\tau-2}, w_\tau, s_\tau\}$ for message $M_\tau$ and $M'_\tau$ on $ID_\tau$. If $c_\tau$, corresponding to $ID_\tau$ in the $H_1$-List is equal to 0, $A$ aborts. Otherwise, $A$ finds $r_\tau, h_\tau$, $H_1(ID_\tau) = b P, H_2(M'_\tau) = \alpha_\tau(b P) + \beta_\tau P$ from table $L$, $H_1$-List, $H_2$-List. If $w_\tau$ is not in table $L$, $A$ cannot generate a legal signature $\sigma_{\tau-1}$. If $\sigma_{\tau-2}$ is legal, we can see that

$$e(\sigma_{\tau-2}, P) = e(H_1(ID_\tau), P_{pub})^h e(s_\tau H_1(ID_\tau) + h_\tau H_2(M'_\tau), w_\tau)$$

$$= e(b P, a P)^h e(s_\tau b P + h_\tau (\alpha_\tau b P + \beta_\tau P), r_\tau a P)$$

$$= e(h SK_\tau, P) e((s_\tau + \alpha_\tau h_\tau) r_\tau SK_\tau + \beta_\tau h_\tau w_\tau, P)$$

According to the non-degenerate property, we can see that $\sigma_{\tau-2} = (s_\tau r_\tau + \alpha_\tau r_\tau + 1) h_\tau SK_\tau + \beta_\tau h_\tau w_\tau$. If $s_\tau \neq -(1/r_\tau + \alpha_\tau) h_\tau, A_1$ is able to obtain

$$ab P = SK_\tau$$

$$= \frac{\sigma_{\tau-2} - \beta_\tau h_\tau w_\tau}{s_\tau r_\tau + (\alpha_\tau r_\tau + 1) h_\tau}$$

Given $r_\tau, h_\tau$, since $s_\tau$ is a random number and is independent, and the equation $s_\tau = -(1/r_\tau + \alpha_\tau) h_\tau, A_1$ holds randomly and the probability is $1/q$. Consequently, if the game does not abort, $A_1$ has probability $\delta(1 - \delta)^{q e} (1 - 1/q) e$ in solving the CDH problem. The function $\delta(1 - \delta)^{q e}$ is maximized at $\delta = 1/(q e + 1)$, where it has the value

$$\frac{1}{q e + 1} \left(1 - \frac{1}{q e + 1}\right)^{q e} (1 - 1/q) e$$

$$= \frac{1}{q e} \left(1 - \frac{1}{q e + 1}\right)^{q e + 1} (1 - 1/q) e$$

For large $q e$, $(1 - 1/(q e + 1))^{q e + 1} \approx 1/e$. To summarize: If $A$ has advantage $e$ to forge a signature, then $A_1$ has probability $e(1 - 1/q) / (e q e)$ to solve the CDH problem.  

Appendix A.3. Security Analysis

Theorem A3. (Anonymity). The real identity of the vehicles in VANETs should not be disclosed, and the messages sent by the vehicles are required to be hidden within a set of potential vehicles.
Proof. In the V2I authentication protocol, the real identity of each vehicle is concealed in $PS_i$; any RSU or BS that does not know the secret value $s$ cannot obtain $ID_i$ through $PS_i$ unless AES becomes insecure. In the pseudonym change protocol, $PS_{iBS}$ is randomly picked by the BS. No vehicle can link $PS_{iBS}$ to $ID_i$. $\square$

Theorem A4. (Unlinkability). Two messages related to the same vehicle cannot be linked for a long time.

Proof. Firstly, the vehicles that cooperate to change the pseudonym must have a similar driving trajectory, so as to guarantee that no adversaries can use the beacon received before changing the pseudonym to track the target vehicle by predicting the driving trajectory. Secondly, the pseudonym change is required within the time interval when the vehicle sends the beacon. After changing the pseudonyms, each vehicle broadcasts the beacon with the new pseudonym. Since the vehicles execute the pseudonym change protocol in ciphertext within the time interval of two beacons, the adversaries cannot obtain any details of the pseudonym change, so it is impossible to link to the target vehicle through received beacon after changing the pseudonym. $\square$

Theorem A5. (Mutual authentication). The identity declared by the sender must be verified, and the integrity of the sent message should be confirmed by all receivers.

Proof. V2I authentication is based on the IBS signature mechanism. Any vehicle is able to compute the public key $H_1(PS_i || EXP_i)$. Vehicles cannot generate the legal public/private key independently unless they have the ability to solve the CDH problem. Consequently, as long as the signatures are verified correctly, the vehicles can be regarded as the legal ones by the TA or BS. The integrity of the message from the sender can be verified through the hash function. $\square$

Theorem A6. (Traceability). An efficient mechanism should be designed so that the TA and BS are able to trace the real identity of a misbehaving vehicle.

Proof. If there is a malicious vehicle in the VANET and its misbehavior is proven, the BS is able to query $PS_i, EXP_i$ according to $PS_{iBS}$ and send $PS_{iBS}, EXP_{iBS}$ to the TA. Then, the TA can track the real identity of the malicious vehicle by computing $ID_i = Dec_s(PS_i || EXP_i)$. Consequently, only the cooperation between the BS and TA can reveal the true identity of the illegal vehicles, which also meets the requirement of restricted credential usage and conditional privacy protection in VANETs. $\square$

Theorem A7. (Session key agreement). After finishing the mutual authentication, entities in VANETs should establish a session key to guarantee that the messages can be transmitted through a secure channel.

Proof. The proposed scheme adopts the Diffie–Hellman key exchange algorithm to support session key agreement. In V2I authentication, the vehicle and RSU compute $r_vR_{RSU}P\text{ and } R_{RSU}r_vP$, respectively, and obtain session key $K_{v-RSU}$. $\square$

Theorem A8. (Location privacy). No adversary can track the target vehicle by eavesdropping on the communications of vehicles within a region of interest.

Proof. The Shannon entropy is considered as the pseudonym entropy to assess the level of location privacy protection for vehicles, which can be interpreted as the effective size of the anonymity set. In the traditional scheme, a group of vehicles that change pseudonyms is defined as $V = \{v_1, v_2, \ldots, v_m\}$. Let $p_i$ represent the probability that vehicle $v_i$ is tracked successfully. Then, the pseudonym entropy of $V$ can be expressed as:
\[ \text{Priv}_V = - \sum_{i=1}^{m} p_i \log_2 p_i. \]

Different from traditional schemes, the achieved entropy in PCP depends on the number of pseudonyms that the vehicle broadcasts, rather than the number of pseudonyms changed simultaneously. We define \( PS = \{ P_{S1}^{BS}, P_{S2}^{BS}, \ldots, P_{Sn}^{BS} \} \) to represent the pseudonyms used in the pseudonym change protocol for group \( V \). Let \( p_i \) refer to the probability that vehicle \( PS^{BS} \) is linked to a vehicle \( v_i \), respectively. Obviously, under the same conditions, \( m \leq n \). Consequently,

\[ \text{Priv}_{PS} = - \sum_{i=1}^{n} p_i' \log_2 p_i' \geq \text{Priv}_V. \]

**Theorem A9.** DoS attack resistance: The adversaries can launch DoS attacks by injecting a large number of legitimate or false messages into the VANET, which makes the useful resources unavailable and leads to a serious decline in performance. The proposed pseudonym change scheme is able to resist the DoS attack by the broadcast communication and low computational cost.

**Proof.** As depicted in Section 4.7, vehicle \( v_i \) broadcasts a pseudonym change request to the surrounding vehicles. The surrounding vehicles do not need to respond to the request from \( v_i \) before \( t_{\text{start}} \). When the time reaches \( t_{\text{start}} \), the vehicles participating in the pseudonym change conduct AES to encrypt \( PS - \text{Cert} - \text{List} \) and broadcast the ciphertext to other vehicles. According to reference [41], the ciphertext verification operation can be performed within 0.8\( \mu \)s; therefore, the proposed pseudonym change scheme is robust against the DoS attack.

**References**

1. Zhang, J.; Wang, F.-Y.; Wang, K.; Lin, W.-H.; Xu, X.; Chen, C. Data-Driven Intelligent Transportation Systems: A Survey. *IEEE Trans. Intell. Transp. Syst.* **2011**, *12*, 1624–1639. [CrossRef]

2. Karagiannis, G.; Altintas, O.; Ekici, E.; Heijenk, G.; Jarupan, B.; Lin, K.; Weil, T. Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions. *IEEE Commun. Surv. Tutor.* **2011**, *13*, 584–616. [CrossRef]

3. *IEEE Std 1609.0-2019 (Revision of IEEE Std 1609.0-2013)*; IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture. IEEE: Piscataway, NJ, USA, 10 April 2019; pp. 1–106.

4. Rehman, O.; Qureshi, R.; Ould-Khaoua, M.; Niazi, M.F. Analysis of mobility speed impact on end-to-end communication performance in VANETs. *Veh. Commun.* **2020**, *26*, 100278. [CrossRef]

5. Obaidat, M.; Shahwan, I.; Hassebo, A.; Obeidat, S.; Ali, M.; Khodjaeva, M. SNR-Based Early Warning Message Scheme for VANETs. *J. Mob. Multimed.* **2020**, *16*, 162–190. [CrossRef]

6. Zhang, M.; Ali, G.M.; Chong, P.H.; Seet, B.C.; Kumar, A. A Novel Hybrid MAC Protocol for Basic Safety Message Broadcasting in Vehicular Networks. *IEEE Trans. Intell. Transp. Syst.* **2020**, *21*, 4269–4282. [CrossRef]

7. *IEEE Std 1609.2.1-2020*; IEEE Standard for Wireless Access in Vehicular Environments (WAVE)–Certificate Management Interfaces for End Entities. IEEE: Piscataway, NJ, USA, 30 December 2020; pp. 1–287.

8. Boualouache, A.; Senouci, S.-M.; Moussaoui, S. A Survey on Pseudonym Changing Strategies for Vehicular Ad-Hoc Networks. *IEEE Commun. Sur. Tutor.* **2018**, *20*, 770–790. [CrossRef]

9. Babaghayou, M.; Labraoui, N.; Ari, A.A.A.; Lagraa, N.; Ferrag, M.A. Pseudonym change-based privacy preserving schemes in vehicular ad-hoc networks: A survey. *J. Inf. Secur. Appl.* **2020**, *55*, 102618. [CrossRef]

10. Freudiger, J.; Raya, M.; Felegyhazi, M.; Papadimitratos, P.; Hubaux, J.-P. Mix-zones for location privacy in vehicular networks. In *Proceedings of the 1st International Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*; Vancouver, BC, Canada, 14 August 2007; pp. 1–7.

11. Lu, R.; Lin, X.; Luan, T.H.; Liang, X.; Chen, C. (Sherman) Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs. *IEEE Trans. Veh. Technol.* **2012**, *61*, 86–96. [CrossRef]

12. Boualouache, A.; Senouci, S.-M.; Moussaoui, S. VLPZ: The vehicular location privacy zone. *Procedia Comput. Sci.* **2016**, *83*, 369–376. [CrossRef]

13. Kang, J.; Yu, R.; Huang, X.; Zhang, Y. Privacy-Preserved Pseudonym Scheme for Fog Computing Supported Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 2627–2637. [CrossRef]

14. Li, X.; Zhang, H.; Ren, Y.; Ma, S.; Luo, B.; Weng, J.; Ma, J.; Huang, X. PAPU: Pseudonym Swap With Provable Unlinkability Based on Differential Privacy in VANETs. *IEEE Internet Things J.* **2020**, *7*, 11789–11802. [CrossRef]
15. Wang, S.; Yao, N. LIAP: A local identity-based anonymous message authentication protocol in VANETs. *Comput. Commun.* 2017, 112, 154–164. [CrossRef]

16. Huang, L.; Matsuura, K.; Yamane, H.; Sezaki, K. Enhancing wireless location privacy using silent period. In Proceedings of the IEEE Wireless Communications and Networking Conference, New Orleans, LA, USA, 13–17 March 2008; Volume 2, pp. 1187–1192.

17. Sampigethaya, K.; Huang, L.; Li, M.; Poovendran, R.; Matsuura, K.; Sezaki, K. CARAVAN: Providing Location Privacy for VANETs. Tech. Rep.; Washington Univ Seattle Dept of Electrical Engineering: Seattle, WA, USA, 2005.

18. Benarous, L.; Kadri, B.; Boudjait, S. Alloed Pseudonym Change Strategy for Location Privacy in VANETs. In Proceedings of the 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 10–13 January 2020; pp. 1–6. [CrossRef]

19. Eckhoff, D.; Sommer, C.; Gansen, T.; German, R.; Dressler, F. Strong and affordable location privacy in VANETs: Identity diffusion using time-slots and swapping. In Proceedings of the 2010 IEEE Vehicular Networking Conference, Jersey City, NJ, USA, 13–15 December 2010; pp. 174–181. [CrossRef]

20. Buttyan, L.; Holczer, T.; Weimerskirch, A.; Whyte, W. SLOW: A Practical pseudonym changing scheme for location privacy in VANETs. In Proceedings of the 2009 IEEE Vehicular Networking Conference (VNC), Tokyo, Japan, 28–30 October 2009; pp. 1–8. [CrossRef]

21. Rayma, H.; Hubaux, J.-P. Securing vehicular ad hoc networks. *J. Comput. Secur.* 2007, 15, 39–68. [CrossRef]

22. Pan, Y.; Li, J. Cooperative pseudonym change scheme based on the number of neighbors in VANETs. *J. Netw. Comput. Appl.* 2013, 36, 1599–1609. [CrossRef]

23. Yu, R.; Kang, J.; Huang, X.; Xie, S.; Zhang, Y. Gjessing, S. MixGroup: Accumulative Pseudonym Exchanging for Location Privacy Enhancement in Vehicular Social Networks. *IEEE Trans. Dependable Secur. Comput.* 2016, 13, 93–105. [CrossRef]

24. Singh, P.K.; Gowtham, S.N.; S, T.; Nandi, S. CPESP: Cooperative Pseudonym Exchange and Scheme Permutation to preserve location privacy in VANETs. *Veh. Commun.* 2019, 20, 100183. [CrossRef]

25. Soleymani, S.A.; Goudarzi, S.; Anisi, M.H.; Zareei, M.; Abdullah, A.H.; Kama, N. A security and privacy scheme based on node and message authentication and trust in fog-enabled VANET. *Veh. Commun.* 2021, 29, 100335. [CrossRef]

26. Chaudhary, B.; Singh, K. A Blockchain enabled location-privacy preserving scheme for vehicular ad-hoc networks. *Peer-Netw. Appl.* 2021, 14, 3198–3212. [CrossRef]

27. Boneh, D.; Franklin, M. "Identity-Based Encryption from the Weil Pairing" in CRYPTO 2001; Springer: Berlin/Heidelberg, Germany, 2001; pp. 213–229.

28. Cha, J.C.; Cheon, J.H. An Identity-Based Signature from Gap Diffie–Hellman Groups. In *Vehicles in the Internet of Things: Concepts, Technologies, and Frameworks for the IoV*; Springer: Cham, Switzerland, 2020.

29. Pan, B.; Andersen, D.G.; Kaminsky, M.; Mitzenmacher, M.D. Cuckoo filter: Practically better than bloom. In *Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies*, Sydney, Australia, 2–5 December 2014; pp. 75–88.

30. Boyen, X.; Martin, L. Identity-Based Cryptography Standard (IBCS) 1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems. Document RFC 5091. 2007. Available online: http://www.rfc.fr/rfc/en/rfc5091.pdf (accessed on 7 December 2021)

31. Sommer, C.; German, R.; Dressler, F. Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis. *IEEE Trans. Mob. Comput.* 2011, 10, 3–15. [CrossRef]

32. Lynn, B.; Shacham, H.; Steiner, M.; Cooley, J.; Figueiredo, R.; Khazan, R.; Kosolapov, D.; Bethencourt, J.; Miller, P. The Pairing-Based Cryptography Library. Available online: https://crypto.stanford.edu/pbc/times.html (accessed on 5 January 2022).

33. Haklay, M.; Weber, P. OpenStreetMap: User-generated street maps. *IEEE Perva-Sive Comput.* 2008, 7, 12–18. [CrossRef]

34. Freudiger, J.; Manshaei, M.H.; Hubaux, J.; Parkes, D.C. Non-Cooperative Location Privacy. *IEEE Trans. Dependable Secur. Comput.* 2013, 10, 84–98. [CrossRef]

35. IEEE Std 1609.4-2016/Cor 1-2019 (Corrigendum to IEEE Std 1609.4-2016); IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Multi-Channel Operation—Corrigendum 1: Miscellaneous Corrections. IEEE: Piscataway, NJ, USA, 17 October 2019; pp. 1–13.

36. He, D.; Zeadally, S.; Xu, B.; Huang, X. An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks. *IEEE Trans. Inf. Forensics Secur.* 2015, 10, 2681–2691. [CrossRef]

37. Tangade, S.; Manvi, S.; Lorenz, P. Decentralized and Scalable Privacy-Preserving Authentication Scheme in VANETs. *IEEE Trans. Veh. Technol.* 2018, 67, 8647–8655. [CrossRef]

38. Chuang, M.-C.; Lee, J.-F. SF-PMIPv6: A secure fast handover mechanism for Proxy Mobile IPv6 networks. *J. Syst. Softw.* 2013, 86, 437–448. [CrossRef]