[1]Lu Zhang
[1]Wuzheng Tan
[1]Xinru Wang

DCPFS: A Conditional Privacy-Preserving Authentication Scheme with Dual Cuckoo Pseudonym Filters for Vanets

Abstract: - With the increasing frequency of information dissemination and exchange, the attention paid to security and privacy in the Internet of Vehicles (IoV) is also on the rise. To protect user privacy, many anonymous authentication scheme have been proposed. These schemes assign pseudonyms to vehicles to hide their true identities when communicating with other vehicles or Roadside Units (RSUs). However, existing schemes also face pseudonym issues such as pseudonym abuse, high storage overhead, and low query efficiency. Motivated by this, we propose an RSU-based pseudonym assistance management scheme. In this scheme, RSUs employ dual cuckoo pseudonym filters to manage pseudonyms, effectively improving pseudonym query efficiency, preventing pseudonym abuse, and reducing storage overhead. Additionally, security and performance analyses demonstrate that the proposed protocol offers stronger security features and lower overhead. Besides, our scheme has reduced the generation time of pseudonym to only 0.0039 ms.

Keywords: VANETs; conditional privacy-preserving; pseudonym; cuckoo filter

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs), a crucial aspect of mobile ad hoc networks, facilitate communication between vehicles and roadside infrastructure (RSU) [27]. Their prime goal is to enhance road safety and efficiency by providing real-time traffic and vehicle status information. With the escalating interconnectedness of vehicles, VANETs' significance has grown, paving the way for innovative applications, including collision warnings and dynamic route planning. In VANETs, vehicles transmit traffic data to nearby vehicles every 100-300 milliseconds using the Dedicated Short-Range Communication (DSRC) protocol. These beacon messages contain crucial safety details like vehicle position, speed, and driving patterns [28].

In VANET, most solutions to ensure security and privacy utilize pseudonym-based methods to protect the privacy of vehicles. In this pseudonym-based approach, legitimate vehicles obtain a set of pseudonyms from a Certificate Authority (CA) or a Trusted Authority (TA) before participating in VANET. Instead of using their real identities, vehicles employ pseudonyms for V2V and V2I communications. To avoid traceability, vehicles frequently change their pseudonyms. When a vehicle's pseudonyms are running out, it requests a new set of pseudonyms. Pseudonyms ensure conditional privacy since the TA can still retrieve the vehicle's true identity. Therefore, the TA can revoke the credential and pseudonyms of malicious vehicles. Revocation Lists (RLs) are widely used to store the information of revoked vehicles. Vehicles store and check the RLs for mutual authentication. However, the size of the RL increases linearly with the number of revoked vehicles, resulting insignificant storage and computation overhead. Conversely, regularly updating and broadcasting RLs can lead to higher latency. In our paper, we propose an efficient pseudonym-based authentication scheme to address the aforementioned challenges. In our scheme, Roadside Units (RSUs) uniformly assign pseudonyms to all vehicles within their respective areas. Additionally, we adopt dual Cuckoo filters to manage pseudonyms by dividing pseudonyms into two sets and constructs two types of Cuckoo filters, DCFs (cf1, cf2). cf1, the valid pseudonym Cuckoo filter, is used to record the set of valid pseudonyms, while cf2, the revoked pseudonym Cuckoo filter, is used to record the set of revoked pseudonyms, effectively enhancing the efficiency of pseudonym queries, preventing pseudonym abuse, and reducing storage space overhead.

The contributions of this paper are summarized as follows:

- Unlike traditional pseudonym generation entities, RSU generates pseudonyms, effectively unifying the management of vehicles' pseudonyms. This approach avoids potential single-point failure hazards that may occur when pseudonyms are generated by the TA, as well as the Sybil attack behavior that may occur when vehicles generate pseudonyms on their own. Not only does it alleviate the load on the TA, but it can also generate pseudonyms for vehicles in real-time.

[1] *Corresponding author: Wuzheng Tan; Email: 619536283@qq.com
[2] College of Cyber Security, Jinan University, Guangzhou, China

- By constructing dual cuckoo filters and applying them to the processes of pseudonym insertion, query, and revocation, we can significantly improve query efficiency, prevent pseudonym abuse, reduce storage overhead, and provide a flexible pseudonym revocation mechanism. This enhances the security and privacy protection capabilities of VANETs.
- Performance analysis and security analysis show that, compared with other solutions, our solution has lower overhead and higher security features.

The remaining sections of the paper are organized as follows. Section 2 surveys related works in the field, while Section 3 presents the preliminaries, system model, and security requirement of the proposed scheme. Section 4 provides the details of the proposed CPPA scheme, followed by security analysis in Section 5 and performance evaluation in Section 6.

Finally, Section 7 concludes the paper.

II. Related Works

In the field of conditional privacy-preserving authentication(CPPA), numerous contributions have been made, and existing anonymous authentication schemes can be roughly categorized into four types: PKI-based[2,4,25], ID-based[12,17,26], group signature- based[10,11], and pseudonymous-based[5–7,9,15],and according to the management of anonymous identities, the main entities involved are the Trusted Authority (TA), Roadside Units (RSUs), and the vehicles themselves.Raya et al.[2] proposed a PKI-based scheme where the TA pre-generates numbers of anonymous certificates for vehicles, which are used for message authentication. This scheme successfully addresses privacy leakage concerns. However, it still has some drawbacks. For instance, vehicles need sufficient storage space to store all the anonymous certificates, which imposes storage overhead. There is also a key escrow issue and the TA manages certificates for all vehicles, leading to an increased workload. Moreover, certificate management becomes complex and challenging.Subsequently, to improve efficiency, Lin etal.[4] proposed a PKI-based blockchain authentication scheme in which blockchain technology is combined with key derivation algorithms to achieve effective certificate management.In [25]'scheme, they used smart contract-based trust chain to replace traditional CA trust chain, thereby reducing certificate transmission and management costs. However, with an increasing number of vehicles, certificate management still faces challenges. Furthermore, blockchain, as a relatively new technology, is not yet matured and has high throughput and latency, making it less suitable for high-speed moving vehicles and presenting limitations. Additionally, the size of the blockchain may restrict its practicality in resource-constrained vehicular systems.

Considering the certificate management issues in PKI-based solutions, Shamir et al.[26] firstly introduced the ID-based scheme. According to their scheme, the public key of a vehicle is derived from its publicly available information. As a result, the vehicle's identity and public key can be associated without relying on any certificates. In this way, the issues related to certificate management are eliminated.Wang et al.[17] proposed a LIAP scheme, which simplifies the complexity of revocation. However, it introduces bilinear pairing algorithms that require significant computational overhead. Additionally, in both [17,26] schemes, the signing key pairs required by the vehicles are obtained from the third party, resulting in key escrow issues.To address this issue, Wang et al. [12] proposed an novel identity-based scheme. In the scheme, the key pair is generated collaboratively by TA, RSU, and the vehicle, effectively avoiding key leakage problems. However, the process of generating the key pair relies on the involvement of the TA and RSUs. This means that vehicles cannot independently generate their own keys and instead require support from external entities. This introduces increased complexity and dependency in the system, as well as requirements for trust and security in the TA and RSUs. Additionally, there is a risk of the single-point of failure.

Regarding group signature schemes, a group administrator generates the public key, enabling vehicles within the group to generate signatures which can be verified using the group public key. Privacy is ensured in this scheme as the signers maintain anonymity within the group.In [11], Nath et al. proposed a mutual authentication scheme.To enhance security,pseudonyms are used to protect users' privacy, and messages are encrypted before they are sent. However, in the pseudonym generation phase, vehicles need to frequently interact with both the TA and RSU, which introduces additional communication overhead. Furthermore, the frequent joining and leaving of vehicles result in large group management overhead. Additionally, tracking malicious vehicles becomes more challenging.To achieve greater flexibility and improved traceability, Guo et al. [10] proposed an efficient ring-based signature scheme. In this scheme, they devised a tracking algorithm that integrates tracking tags into messages, allowing trusted entities to easily find the malicious vehicle from ring list. However, these two schemes do not delve into the revocation of vehicles in detail.

There are numerous CPPA schemes based on pseudonyms, such as [3,5–9,13–16,18– 22]. In the fog-based scheme proposed by Zhong et al. [3], vehicles generate pseudonyms using two seed values, which partially alleviates the burden on the Trusted Authority (TA) and reduces the storage overhead for vehicles. However, there are also some drawbacks. If malicious vehicles continuously generate and use new pseudonyms, they can launch Sybil attacks.There are also certificateless schemes based on pseudonyms, such as [5,7,16]. Qi et al.

[16] proposed a certificateless conditional privacy-preservation scheme (CPPS) using bilinear mapping. In their scheme, a part of the vehicle's keys is generated by a Key Generation Center (KGC), while the remaining keys are randomly chosen by the KGC itself.However,the bilinear pairing operation is a computationally expensive operation, which leads to low efficiency in schemes like the one proposed in [5,16]. Although [7] avoids the use of bilinear mapping, its communication overhead is still not highly efficient. Ye et al. [15] proposed a CPPA scheme based on pseudonyms with (t,n) threshold secret sharing, optimizing the revocation overhead of pseudonyms. However, the scheme involves bilinear mapping, resulting in high computational costs. Additionally, the TA needs to be online for a long duration to generate pseudonyms, which poses a big challenge for its workload.

In addition,there are also some schemes that adopt the cuckoo filter (CF). Cui et al. [29] proposed a privacy-preserving authentication scheme based on CF, known as SPACF. In the batch verification phase of SPACF, the CF and binary search method are employed to achieve a high batch verification success rate. However, due to the use of identity-based signatures in SPACF [13], there exists a key escrow problem. Zhang et al.[30]introduced a VANET pseudonym certificate revocation scheme based on the cuckoo filter. This scheme stores the certificate fingerprints of unexpired pseudonyms of revoked vehicles in the cuckoo filter and broadcasts it to the network by the CA, simplifying the authentication process. Compared to traditional CRLs, this scheme significantly reduces computational overhead.

Finally, the proposed scheme offers improved security and functional attributes compared to the existing schemes mentioned in Table 1.

Table 1. The safety comparison between the proposed scheme and the existing scheme

Scheme	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10
[6]	√	√	√	√	X	√	√	√	X	√
[9]	√	√	√	√	X	√	√	√	X	√
[7]	√	√	X	√	X	√	X	√	X	√
[5]	√	√	X	√	X	√	√	X	X	√
Our scheme	√	√	√	√	√	√	√	√	√	√

Note S1:Message authentication; S2:Identity privacy preserving; S3:Requires less storage; S4:Traceability; S5:Revocation;

S6:Unlinkability; S7:Mutual authentication; S8:No pairing verification; S9:No TA on-line all time; S10:Replay attack resistance, Key escrow resistance, Man-in-the-middle attack resistance;

III. Preliminaries

In this section, we will introduce some prerequisite knowledge, including the system model, security model, security requirements, elliptic curve cryptography and the cuckoo filter.

A. System model

Figure 1 depicts the standard architectural model of VANETs, which primarily en- compasses three entities: the TA (Trust Authority), the RSU (Roadside Unit), and the V (Vehicle).

• TA: As an Authority which is trusted and cannot be compromised, TA possesses strong computing and storage resources and is responsible for the initialization operations of the entire system, as well as the registration of V and RSU within the system. Besides,TA also can track malicious vehicles.

• RSU: RSU serves as the roadside infrastructure and is also a trusted entity. It provides services to the communicating vehicles and acts as an intermediary between TA and V. RSU is responsible for managing the pseudonyms of vehicles.

• V: Vehicles are the communication entities in the system and are equipped with Tamper Proof Device(TPD) and Onboard Unit(OBU). The OBU is responsible for generating key pair, while the TPD can store the key pair and other sensitive datas.

B. Security Model

In our proposed scheme,we take into account the following assumptions:

• RSUs are considered trusted entities, they are physically protected and have a large computational capacity.

• An adversary Adv can launch different attacks including Replay attacks, Sybil attacks, and Man-in-the-middle attacks.

C. Security Requirements

Within this system, we have formulated numerous security requirements that ought to fulfill.

- **Anonymity**: The true identity of a vehicle must be transmitted in an anonymous manner, preventing a malicious adversary from analyzing the original sender's identity.
- **Traceability**: If deception occurs, the true identity of the malicious vehicle can be traced.
- **Message authentication and integrity**: The recipient can verify the legitimacy of the sender's identity and the validity of the message.

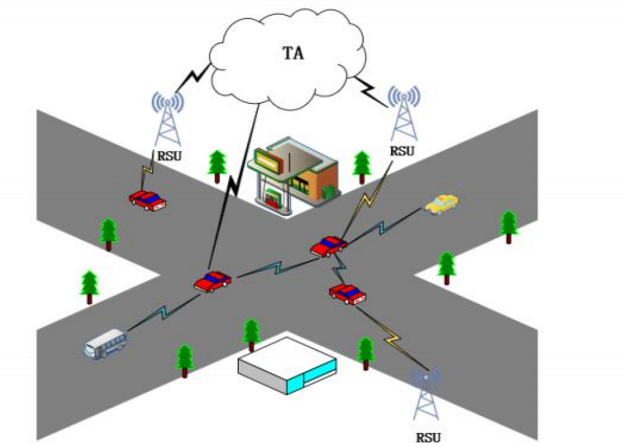

Figure 1. The system model of the VANETs

- **Revocation**: If a vehicle engages in malicious behavior, both RSU and TA can collaborate to revoke the credentials or privileges of that vehicle.
- **Key escrow resilience**:The vehicle generates and securely stores its own unique public and private key pair, which remains undisclosed to any other entity.
- **Confidentiality**: The two random seeds used to generate pseudonyms are known only to TA and RSU.
- **Mutual authentication**:The communication parties verify the validity of each other's identities to ensure the reliability of information.
- **Unlinkability**: Vehicles periodically change their pseudonyms to prevent malicious third parties or vehicles from determining whether the messages originate from the same vehicle.
- **Resist other attacks**: The Scheme could resist typical attacks such as replay attacks, Sybil attacks, man-in-the-middle attacks, key escrow, etc.

D. Elliptic Curve Cryptography

We assume that Fp is the finite field, which p is a large prime number.An elliptic curve E over a finite field Fp and be defined as $y^2=x^3+ax+b$(mod p),where a,b∈Fp and $(4a^3 + 27b^2)$ mod p $\neq$0..Suppose O is a point at infinity on E,Point O and points of ECC make up an additive elliptic curve group G with the order q and generator P. The security of ECC-based algorithms is based on the Elliptic Curve Discrete Logarithm Problem (ECDLP): Given two arbitrary and precise points Q and P,the computation Q = xP,with x represents a random number, gives the advantage for an adversary to compute xin polynomial time (t).AdvECDLP(t) = Prb[(Q, P) = x].AdvECDLP(t) $\leq$, is the concluded ECDLP assumption.[31]

E. 3.5. Cuckoo Filter

The Cuckoo Filter is a probabilistic data structure that saves memory space. It is an implementation of the cuckoo hashing algorithm, similar to the Bloom Filter, and is used to detect the existence of a specified element in a certain set. It functions as a hash table, storing fingerprints of data rather than the original data to reduce space usage. When inserting an element x, the fingerprint fp(x) of the element is first calculated, and then two candidate buckets are determined based on two hash functions h_1 and h_2. Depending on the occupancy of the buckets, the next step is as follows:

- If both buckets are empty, a position is randomly selected and the element is inserted there;
- If only one bucket is empty, the element is inserted into that empty bucket;
- If both bucket are occupied, a random element is evicted, and the evicted element is reinserted by recalculating its hash value and finding the corresponding bucket using the same method.

In addition, based on the element x and the two hash functions h_1 and h_2, we can quickly search for the fingerprint fp(x) of the element. Both the lookup and deletion operations for fp(x) have a time complexity of O(1).Following the parameter settings in [32], we set the number of slots in DCPFs to 4 and the size of the pseudonym fingerprint to 16 bits, which can reduce the false positive probability to 0.0033%.

IV. The Proposed Scheme

This section presents a detailed description of our scheme,which consists of six stages: system initialization stage, registration stage, pseudonym generation stage, message signature stage, message verification stage and revocation stage. The symbols used in this scheme are presented in Table 2,and other symbols are described when used.

A. System initialization stage

1. First,TA selects an elliptic curve E: $y^2 = x^3 + ax + b \pmod p$ defined over a finite field of prime order p,where p is a large prime number,and a, b $\in F_p$.Then, TA selects an additive group G with the order q. The P is a generator of additive group G.

2. Then, TA chooses a number s $\in Z_q^*$ as the master key of the system, and compute $sP_{pub} = sP$ as system public key.

3. Next, TA chooses four one-way general hash functions such as $H : \{0, 1\}^* \to Z_q^*$, $H0 : G \to Z_q^*$, $H1 : G \times \{0, 1\}^* \to Z_q^*$, $H2 : \{0, 1\}^* \times G \times \{0, 1\}^* \to Z_q^*$.

4. Lastly,TA disseminates the public parameters Params = {a, b, P, G, H, H0, H1, H2}to all vehicles and RSUs,and TA keeps s for itself.

B. Registration stage

During the registration phase, both the vehicle and the RSU register with the TA and will each obtain an identity credential.

1. The registration of Vehicle

a. First, the vehicle generates its own private key,denoted as VSK $\in Z_q^*$, and subsequently computes the corresponding public key as VPK = VSKP.

b. Subsequently, the vehicle will store VSK in its own TPD and transmit its real identity VID and public key VPK to TA through a secure channel.

c. Upon receipt, the TA will select a random number $\alpha \in Z_q^*$, and generate Vtoken for the vehicle.

d. Then, the TA will store { Vid, Vpk, Vtoken} in the local database and set the status to activated, indicating that the identity credential of the vehicle is activated. After that, the TA will securely transmit the Vtoken = (Rv, SV) to the vehicle through a secure channel.

The process of generating Vtoken is as follows:

Table 2. Involved notations in the paper

Notation	Description
Vi	The i-th vehicle
RSU	A roadside unit
OBU	A onboard unit
TA	A trust authority
p, q	Two large prime numbers
G, G1	Cyclic additive group
$e : G1 \times G1 \to G2$	Bilinear pairing
P	A generator of the group G
E	An elliptic curve
s	The private key of the system
Ppub	The public key of the system
RIDi	The real identity of a vehicle
PIDi	The anonymous identity of a vehicle
$H(\cdot)$, $H0(\cdot)$, $H1(\cdot)$, $H2(\cdot)$	Four one-way hash functions
Ti	Current timestamp
m_i	A traffic-related message
(x)	Take the X-axis coordinate value
Vtoken	the vehicle’s identity is legitimate
Rtoken	the RSU’s identity is legitimate
VPKi	A public key of the i-th vehicle
VSKi	A private key of the i-th vehicle
RPKi	A public key of the i-th RSU
R_{SKi}	A private key of the i-th RSU
⊕	Exclusive-OR operator
∥	Concatenation operator

σi	Signature on m_i
Enc(·)	Symmetric encryption
Dec(·)	Symmetric decryption
DCPFs	Dual cuckoo pseudonym filters
df 1	A cuckoo filter for storing valid pseudonyms
df 2	A cuckoo filter for storing revoked pseudonyms

$P1 = \alpha P, R_V = P1(x), F1 = H0(VPK)\ SV = \alpha^{-1}(F1 + sRv)(\text{mod } q)$ (1)

2. The registration of RSU

The entire process is as follows:

a. First, the RSU generates its own private key,denoted as RSK $\in Z_q^*$, and subsequently computes the corresponding public key as RPK = RSKP.

b. Subsequently, the RSU will transmit its real identity RID and public key RPK to TA through a secure channel.

c. Upon receipt, the TA will select a random number $\beta \in Z_q^*$, and generate Rtoken for the RSU.

The process of generating Rtoken is as follows:

$P2 = \beta P, A = P2(x)$

$F2 = H1(RPK \,\|\, H0(S1 \,\|\, S2))$

$SR = \beta^{-1}(F2 + sA)(\text{mod } q)$ (2)

d. Finally,the TA will store { Rid, Rpk, Rtoken } in the local database and send Rtoken = (A, SR) to the RSU through a secure channel.

C. Pseudonym generation stage

When a vehicle enters the communication range of the RSU, in order to ensure safe and effective vehicle-to-network services, the vehicle will perform a series of authentication and communication processes. This process involves identity-related authentication, followed by the storage of pseudonyms using the Cuckoo Filter. The detailed process is outlined below:

1. Firstly, the vehiclesends a request message req = {c= Enc(Vtoken, Rpk), Vpk, T }to the RSU, where T represents the current timestamp.

2. After receiving the req, the RSU performs the following steps:

• The RSU will first check the validity of the timestamp T. If it is invalid, the request will be rejected; otherwise, the process will continue to the next step.

• Then, the RSU obtains the vehicle's identity credential Vtoken through Dec(Rsk, c) and verifies whether Vtoken is valid.

• The legitimacy of Vtoken is determined by computing the value of $S_v^{-1}F1P + S_v^{-1}R_V P_{pub}$ and subsequently comparing its x-coordinate value with R_V to verify if they are equivalent.

3. If the verification is successful, the RSU will randomly select two numbers ($s1 \in Z_q^*, s2 \in Z_q^*$), to generate a pseudonym for the vehicle for subsequent communication.

The specific process is as follows:

$S_{i,1} = s1 \oplus VPKi\ \ S_{i,j} = H^j(S_{i,1})\ S_{i,2} = s2 \oplus VPKi$

$S_{i,w-j+1} = H^{w-j+1}(S_{i,2})$

$PID_{i,j} = H(S_{i,j} \oplus S_{i,w-j+1} \oplus T_j)$ (3)

where w represents the number of time periods in a day, $j \in [1, w]$, Hj(·) and $H^{w-j+1}(\cdot)$ represents the hash value at time j and w −j + 1, respectively.

4. After generating the pseudonym, the RSU selects a hash function hash(·) and fp(·), h_1 and h_2, and then inserts the cf 1. The specific steps are as follows:

• f = fp(PIDi,j)

• i = hash(PIDi,j)

• j = i⊕ hash(f)

The RSU then selects a random number $\theta \in Z_q^*$,and generates a signature ε_R for (PID, RPK, T2). It responds to Vi with response = { PID, Enc(Rtoken, Vpk), RPK, T2, ε_R }, where εR = (C, X), Rtoken = (A, SR).

5. The process of generating εR is as follows:

$P3 = \theta P, C = P3(x)$

$F3 = H2(PID \| RPK \|T2)$

$X = \theta^{-1} (H2 + RSKC) \bmod q$ (4)

6. Upon receiving the response, Vi performs necessary operations to verify the identity of the RSU and the legitimacy of the information. The specific steps are as follows:

- Vi initially verifies the validity of T2 . If it is deemed valid, the process proceeds; otherwise, Vi rejects the request.
- Vi verifies the legitimacy of the RSU by computing the value of $S_R^{-1} F2P + S_R^{-1} AP_{pub}$ and then extracting the x-coordinate of the computed result. It subsequently checks whether this x-coordinate is equivalent to A.
- Vi validates the information furnished by the RSU through the computation of $X^{-1} F3P + X^{-1} CRPK$. It then extracts the x-coordinate of the computed result and verifies if it matches the value of C.
- If all the aforementioned equations are validated as true, Vi will acknowledge the information and adopt the pseudonym for subsequent communications.

D. Message signature stage

Once the pseudonyms are obtained, the vehicle will utilize them for all subsequent communications. This entire communication process is conducted anonymously, thereby safeguarding the privacy of individuals and ensuring the security of the exchange.

1. The Vi selects firstly a random number $\omega i \in Z_q^*$.
2. Then, the Vi calculates the following formulas:

$P4 = \omega iP, Y = P4(x)$

$F4 = H2(m \| PID \| VPK \| T3)$

$U = \omega_i^{-1} (F4 + VSKY) \bmod q$ (5)

3. Lastly,the Vi sends $\{e = (Y, U), m, C, VPK, T3\}$to Vj.

E. Message verification stage

When the receiver receives a message from the sender, in order to ensure the security and privacy of the message, the receiver will take a series of relevant verification measures.

- The receiver first checks the validity of the timestamp T3, and if it is invalid, the message will be rejected directly.
- The receiver queries cf 1 based on the PID to see if it exists. If it does not exist, it means the PID is invalid, and the message will be rejected. If it does exist, the receiver will proceed to the next step.
- The receiver computes $H2(m \| PID \| VPK \| T3)$.
- The receiver computes the value of $U-1 F4P + U-1 YVPK$ and subsequently verifies whether the x-coordinate of the computed value is equivalent to Y.If the equation is unsuccessful, the revocation stage will be entered..

F. Revocation stage

When the receiver detects a malicious vehicle sending false messages, it will immediately take action and send a report to the RSU. The revocation process typically involves removing the pseudonym from the RSU's cfl, adding it to cf2, and sending a notification to the TA to revoke the vehicle's identity credential. This ensures that the malicious vehicle cannot continue to use its original pseudonym for communication within the network. The specific steps are as follows:

- The receiving vehicle Vj sends the sender's public key Vpki, pseudonym PIDi, its own public key Vpkj, the false message m', and the signature s to the RSU.
- Firstly, the RSU locates the corresponding pseudonym fingerprint f in cf 1 based on PIDi and then deletes this value. Subsequently, the revoked pseudonym is added to cf 2.
- In addition, the RSU sends the public key Vpki of Vi to the TA and inform the TA of Vi's malicious behavior. In response, the TA will set the status of the identity credential Vtokeni corresponding to V_{pki} to revoked.

V. SECURITY ANALYSIS

We introduce how proposed scheme could achieve the following security requirements in this section:

- **Anonymity**: During vehicle-to-vehicle communication, all information is transmitted solely based on PIDs, without disclosing the actual identity of the vehicle. Consequently, the proposed scheme effectively ensures anonymity of identities.
- **Traceability**: The message tuple = $\{e = (Y, U), m, PID, VPK, T\}$that sent by the vehicle includes the VPKi. When the RSU sends VPKi of a malicious vehicle to the TA, the TA can get the true identity of the vehicle by check the registration list.
- **Message authentication and integrity**: Upon receiving the message tuple = $\{e = (Y, U), m, PID, VPK, T3\}$, the receiver will compute $H2(m \| PID \| VPK \| T3)$ and then verify the authenticity by checking if the result of the equation $U^{-1} F4P + U^{-1} YVPK$ is equal to Y. If the equation holds true, it indicates a successful authentication.

• **Revocation**: When the receiver detects a malicious vehicle sending false messages, it will immediately take action and send a report to the RSU. The revocation process typically involves removing the pseudonym from the RSU's cf1, adding it to cf2, and sending a notification to the TA who will update the vehicle's identity credential as revoked

• **Confidentiality**: In the pseudonym generation stage, S1 and S2 are used for the generation of pseudonyms and they will never be sent. An Adv who tries to analyze a pseudonym to extract S1 and S2 will never succeed due to the one-way hash function used and the random number.

• **Key escrow resilience**:the vehicle is the only entity who knows its private key. No one else is capable of imitating the vehicle.

• **Unlinkability**: The pseudonyms are updated frequently by the RSU. But the pair (S1, S2) remains unmodifiable and is only known by the TA and RSU. An Adv cannot distinguish whether two messages sent at time j and j + 1 are sent by the same vehicle or not.

• **Mutual authentication**:In the pseudonym generation stage, when the vehicle initially requests service from the RSU, the RSU will authenticate the vehicle's legal identity based on its V_{token} and signature. Upon successful authentication, the RSU transmits a pseudonym, R_{token} and signature to the vehicle, which then verifies the validity of the information and the legitimacy of the RSU's identity based on the Rtoken and signature.

• **Replay attacks**: There is a system timestamp T in each message. If An Adv wants to use an already sent message and changes the T with a recent one will be detected by the signature of the authentic message attached to the request.

• **Sybil attack**: RSU manages the pseudonyms of vehicles, employing an effective pseudonym cuckoo filter (cf1) to record the set of valid pseudonyms and a revoked pseudonym cuckoo filter (cf2) to record the set of revoked pseudonyms. This approach effectively prevents vehicles from abusing pseudonyms and launching Sybil attacks.

• **Man-in-the-middle attack**: Even if an Adv intercepts the message, it do not possess the sender's private key. Therefore, it can't forge the signature. The receiver can verify the authenticity of the message using sender's public key.

VI. Performance Evaluation

In this section, we evaluate the performance of our scheme from the perspectives of computational cost and communication cost. We compare our solution with other existing schemes[6,7,9] based the ECC encryption algorithm, and Ali etal.[5] used the bilinear pairing encryption algorithm.To more clearly analyze the computational and communication overhead of basic cryptography operations, the cryptographic operations related to the scheme are designed as follows.G1 is an additive group, and a symmetric bilinear pairing: $e : G1 \times G1 \rightarrow G2$. Similarly, we construct the ECC algorithm:G is an additive group and a non-singular elliptic curve E.We utilized the well-known Miracl library to measure the execution time of all encryption operations. The computer used for the experiments was an AMD Ryzen 7 5700U with Radeon Graphics 1.80 GHz processor and 16GB of memory. The execution times of the relevant operations are shown in Table 3.

Table 3. Execution time of the encryption operations

Notation	Description	Time(ms)
Tpb	the execution time of bilinear pairing operation.	4.2039
Th	the execution time of one- way hash function.	0.0013
Tbp−pm	the execution time of point multiplication operation in bilinear pairing.	1.537
Tbp−pa	the execution time of point addition operation in bilinear pairing.	0.0069
T_{ecc-pm}	the execution time of point multiplication operation in ecc.	0.407
T_{ecc-pa}	the execution time of point addition operation in ecc.	0.0021

A. Computational Cost

Regarding computational cost, we primarily consider the cryptographic operations involved in pseudonym generation, message signing, and verification.

In the pseudonym generation phase, scheme [6] requires three hash operations and three point multiplication operations.Therefore, the time is $3T_h + 3T_{ecc-pm} \approx 1.2249$ms.In schemes [5,7,9], both of them require two point multiplication operations and one hash operation,so the time is $T_h + 2T_{ecc-pm} \approx 0.8153$ms.However,in our proposed scheme, we only require three hash operations, resulting in a time of $3T_h \approx 0.0039$ms.

In the individual message signing phase, scheme [6] requires one hash operation and two point multiplication operations.Thus, the execution time of the signature is $T_h + 2T_{ecc-pm} \approx 0.8153$ms.Scheme[9] needs one hash operation and one point multiplica- tion operation,so the time is T_h +

$T_{ecc-pm} \approx 0.4083$ms.In scheme [7], it requires two hash operations and one point multiplication operation.The verification needs time $2T_h + T_{ecc-pm} \approx 0.4096$ms.[5]'scheme,signing a message executes one hash operation and two point multiplication operations.Thus signing a message needs $T_h + 2T_{ecc-pm} \approx 0.8153$ms.In our proposed scheme, however, we only require one hash operation and one point multiplication operation.And the total time is$T_h + T_{ecc-pm} \approx 0.4083$ms.

In single message verification phase,scheme [6] requires two hash operations, one point addition operation, and three point multiplication operations.So the execution time is $2T_h + T_{ecc-pa} + 2T_{ecc-pm} \approx 1.2257$ms.In scheme [9], it requires three point multiplication operations and two point addition operations.So the execution time is $2T_{ecc-pa} + 3T_{ecc-pm} \approx 1.2252$ms.In scheme [7], it requires four point multiplication operations, three point addition operations, and three hash operations.Thus the execution time is $3T_h + 3T_{ecc-pa} + 4T_{ecc-pm} \approx 1.6382$ms.In scheme [5], it requires one bilinear pairing operation, one point multiplication operation, and one point addition operation,which needs whole time is $T_{pb} + T_{ecc-pm} + T_{ecc-pa} \approx 4.613$ms.In our proposed scheme, we require one hash operation and one point multiplication operation.Therefore the time is $T_h + T_{ecc-pm} \approx 0.4083$ms.

As shown in Figure 2, compared to several relevant schemes [5–7,9], Our scheme exhibits relatively lower computational cost.

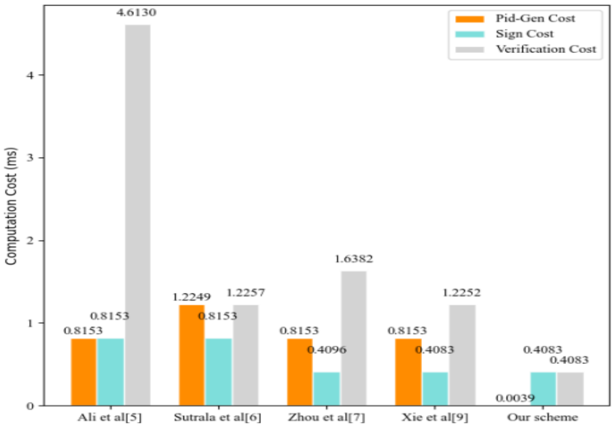

Figure 2. Comparison Of computational overhead.

B. *Storage Cost*

With the increase of pseudonyms, the storage overhead of pseudonyms has also become a problem that cannot be ignored. Reducing storage overhead is a key objective in the design and implementation of pseudonym systems, which can not only save storage space but also improve the efficiency and response speed of the system. In our proposed protocol, unlike schemes[5–7,9], we store the fingerprint of the pseudonym, which can effectively reduce the waste of storage space compared to directly storing the pseudonym. We setup two sets of comparative experiments. Group A is the overhead of directly storing pseudonyms, while Group B is the overhead of storing pseudonym fingerprints. We also calculated the storage space occupied by different numbers of pseudonyms, as shown in Figure 3.

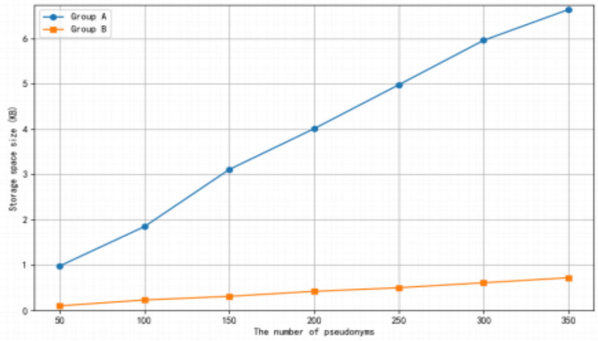

Figure 3. Comparison Of Storage overhead.

C. *Communication Cost*

In this section, we have conducted a detailed evaluation of the communication cost of the aforementioned schemes.Let the size of an element in G1 be 128 bytes, the size of an element in G be 40 bytes,and the size of Z_q^* be 20 bytes. Additionally, we assume that the size of a general one-way hash function is 20 bytes,the size of a timestamp is 4 bytes, the size of a pseudonym is 20 bytes, and the size of the transmitted message m is 20 bytes.

In scheme [6],the vehicle Vi broadcasts a tuple {AIDi = (AIDi,1, AIDi,2, σi = (fi, gi), Bi, Ki, Ri, T1, Mi)}, where AIDi,2, f_i, $g_i \in Z_q^*$, AIDi,1, Bi, Ki, Ri $\in$ G,thus, the communication cost is (40 × 4 + 20 × 3 + 4 + 20) = 244 bytes.In scheme [9],the tuple sent from a vehi-cle is {PIDi, σi, Mi, Ti, Ri},where PIDi = (PIDi,1, PIDi,2). PIDi,1, Ri $\in$ G, PIDi,2, σi $\in Z_q^*$, Therefore, the communication overhead is (40 × 2 + 20 × 2 + 4 × 1 + 20) = 144 bytes.In the paper [7], the transmitted message is {AIDi,1, AIDi,2, Ti, Xi, Ui, ηi, Ai, ti, mi},where AIDi,1, Xi, Ui, Ai $\in$ G,AIDi,2, ηi $\in Z_q^*$,and (Ti, ti) is timestamp.Thus, the communication overhead needs 40 × 4 + 20 × 2 + 4 × 2 + 20 = 228 bytes.In the paper [5],the tuple of messages sent by the vehicle is {PIDi = (PIDi,1, PIDi,2), PKi = (Ri, Ui), Ti, σi, mi},where PIDi,1, Ri, Ui, σi $\in$G1, PIDi,2 $\in Z_q^*$.Therefore, the communication overhead needs 128 × 4 +20 × 1 + 4 × 1 + 20 × 1 = 556 bytes.In our scheme,the vehicle broadcasts {σi = (Y, U), m, PID, T3,4V45PK }to nearby vehicles or infrastructures, where Y, U $\in Z_q^*$, VPK $\in$ G.Thus,the communication overhead is 20 × 2 + 40 × 1 + 4 × 1 + 20 × 1 + 20 = 124 bytes. From Table 4, it can be observed that the scheme [5] based on bilinear pairing has higher communication cost. Among the ECC-based schemes, the communication cost of our scheme is lower compared to schemes [6,7,9].

Table 4. Communication overhead comparison (bytes)

Scheme	Send a message
Sutrala etal. [6]	244
Xie et al. [9]	144
Zhou et al. [7]	228
Ali etal. [5]	556
Our scheme	124

VII. Conclusion

In this paper, we innovatively propose a pseudonym-assisted management scheme based on RSU. In this scheme, RSU skillfully utilizes dual pseudonym cuckoo filters for pseudonym management. This design not only significantly alleviates the burden on TA but also effectively suppresses the abuse of pseudonyms. More importantly, our scheme achieves remarkable improvements in pseudonym storage and query efficiency, bringing great convenience to practical applications. Furthermore, through thorough security analysis, our scheme demonstrates higher security performance compared to other solutions,further safeguarding the security and stability of information communication.

Author Contributions: L.Z. was responsible for writing the original draft. W.Z.T. was responsible for thesis revision and review. X.R.W was responsible for doing the experiments and producing the results. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Guangdong Key Laboratory of Data Security and Privacy Preserving (Grant No. 2023B1212060036).

Acknowledgments: In this section you can acknowledge any support given which is not covered by the author contribution or funding sections. This may include administrative and technical support, or donations in kind (e.g., materials used for experiments).

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

References

[1] J. Petit, F. Schaub, M. Feiri, and F. Kargl, “Pseudonym schemes in vehicular networks: A survey,” IEEE communications surveys &tutorials, vol. 17, no. 1,pp. 228–255, 2014.

[2] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” Journal of computer security, vol. 15, no. 1,pp. 39–68, 2007.

[3] H. Zhong, L. Chen,J. Cui,J. Zhang,I. Bolodurina, and L. Liu, “Secure and lightweight conditional privacy-preserving authentica- tion for fog-based vehicular ad hoc networks,” IEEE Internet of Things Journal, vol. 9, no. 11,pp. 8485–8497, 2021.

[4] C. Lin, D. He,X. Huang,N. Kumar, and K.-K. R. Choo, “Bcppa: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks,” IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 12,pp. 7408–7420, 2020.

[5] I. Ali, Y. Chen, M. Faisal, M. Li, I. Ali, Y. Chen, M. Faisal, and M. Li, “Certificateless signature-based authentication scheme for vehicle-to-infrastructure communications using bilinear pairing,” Efficient and Provably Secure Schemes for Vehicular Ad-Hoc Networks, pp. 91–119, 2022.

[6] A. K. Sutrala, P. Bagga, A. K. Das, N. Kumar, J. J. Rodrigues, and P. Lorenz, "On the design of conditional privacy preserving batch verification-based authentication scheme for internet of vehicles deployment," IEEE Transactions on Vehicular Technology, vol. 69, no. 5,pp. 5535–5548, 2020.

[7] X. Zhou, M. Luo, P. Vijayakumar, C. Peng, and D. He, "Efficient certificateless conditional privacy-preserving authentication for vanets," IEEE Transactions on Vehicular Technology, vol. 71, no. 7,pp. 7863–7875, 2022.

[8] I. Ali, Y. Chen, M. Faisal, M. Li,I. Ali, Y. Chen, M. Faisal, and M. Li, "An ecc-based conditional privacy-preserving authentication scheme for vehicle-to-vehicle communications," Efficient and Provably Secure Schemes for Vehicular Ad-Hoc Networks, pp. 121–146, 2022.

[9] P.-S. Xie, X.-J. Pan, H. Wang,J.-L. Wang, T. Feng, and Y. Yan, "Conditional privacy-preserving authentication scheme for iov based on ecc," Int. J. Netw. Secur, vol. 24,pp. 501–510, 2022.

[10] R. Guo, L. Xu, X. Li,Y. Zhang, and X. Li, "An efficient certificateless ring signcryption scheme with conditional privacy-preserving in vanets," Journal of Systems Architecture, vol. 129,p. 102633, 2022.

[11] H. J. NathandH. Choudhury, "A privacy-preserving mutual authentication scheme for group communication in vanet," Computer Communications, vol. 192,pp. 357–372, 2022.

[12] X. Wang, Q. Chen, Z. Peng, and Y. Wang, "An efficient and secure identity-based conditional privacy-preserving authentication scheme in vanets," International Journal of Network Security, vol. 24, no. 4,pp. 661–670, 2022.

[13] H. Artail and N. Abbani, "A pseudonym management system to achieve anonymity in vehicular ad hoc networks," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 1,pp. 106–119, 2015.

[14] S. Mathews and B. Jinila, "An effective strategy for pseudonym generation & changing scheme with privacy preservation for vanet," in 2014 International Conference on Electronics and Communication Systems (ICECS).IEEE, 2014,pp. 1–6.

[15] Y. Xu,F. Li, and B. Cao, "Privacy-preserving authentication based on pseudonyms and secret sharing for vanet," in 2019 Computing, Communications and IoT Applications (ComComAp).IEEE, 2019,pp. 157–162.

[16] J. Qi, T. Gao, X. Deng, and C. Zhao, "A pseudonym-based certificateless privacy-preserving authentication scheme for vanets," Vehicular Communications, vol. 38,p. 100535, 2022.

[17] S. Wang and N. Yao, "Liap: A local identity-based anonymous message authentication protocol in vanets," Computer Communica- tions, vol. 112,pp. 154–164, 2017.

[18] A. Sudarsono and M. Yuliana, "An anonymous authentication with received signal strength based pseudonymous identities generation for vanets," IEEE Access, vol. 11,pp. 15 637–15 654, 2023.

[19] J. Qi and T. Gao, "A privacy-preserving authentication and pseudonym revocation scheme for vanets," IEEE Access, vol. 8,pp. 177 693–177 707, 2020.

[20] H. Artail and N. Abbani, "A pseudonym management system to achieve anonymity in vehicular ad hoc networks," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 1,pp. 106–119, 2015.

[21] S. Mathews and B. Jinila, "An effective strategy for pseudonym generation & changing scheme with privacy preservation for vanet," in 2014 International Conference on Electronics and Communication Systems (ICECS).IEEE, 2014,pp. 1–6.

[22] J. Qi and T. Gao, "An anonymous authentication scheme based on self-generated pseudonym for vanets," in International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing.Springer, 2022, pp. 75–84.

[23] A. Yang,J. Weng, K. Yang,C. Huang, and X. Shen, "Delegating authentication to edge: A decentralized authentication architecture for vehicular networks," IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 2,pp. 1284–1298, 2020.

[24] A. Yang,J. Weng, N. Cheng,J. Ni, X. Lin, and X. Shen, "Deqos attack: Degrading quality of service in vanets and its mitigation," IEEE Transactions on Vehicular Technology, vol. 68, no. 5,pp. 4834–4845, 2019.

[25] H. Zhang and F. Zhao, "Cross-domain identity authentication scheme based on blockchain and pki system," High-Confidence Computing, vol. 3, no. 1, p. 100096, 2023.

[26] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology: Proceedings of CRYPTO 84 4. Springer, 1985, pp. 47–53.

[27] J. Cheng,J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, "Routing in internet of vehicles: A review," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 5,pp. 2339–2352, 2015.

[28] C. Cseh, "Architecture of the dedicated short-range communications (dsrc) protocol," in VTC'98. 48th IEEE Vehicular Technology Conference. Pathway to Global Wireless Revolution (Cat. No. 98CH36151), vol. 3. IEEE, 1998,pp. 2095–2099.

[29] J. Cui,J. Zhang, H. Zhong, and Y. Xu, "Spacf: A secure privacy-preserving authentication scheme for vanet with cuckoo filter," IEEE transactions on vehicular technology, vol. 66, no. 11,pp. 10 283–10 295, 2017.

[30] H. Zhang, D. Zhang, H. Chen, and J. Xu, "Improving efficiency of pseudonym revocation in vanet using cuckoo filter," in 2020 IEEE 20th International Conference on Communication Technology (ICCT). IEEE, 2020,pp. 763–769.

[31] S. D. Galbraith and P. Gaudry, "Recent progress on the elliptic curve discrete logarithm problem," Designs, Codes and Cryptography, vol. 78,pp. 51–72, 2016.

[32] Y. Liu, "RResearch on Cross-domain Identity Authentication Scheme Based on Blockchain,".in 2023 IEEE 21th International Conference on Communication Technology (ICCT). IEEE, 2023,pp. 456–463.