Article

An Efficient Conditional Privacy-Preserving Authentication for VANETs

Lu Zhang , Wuzheng Tan * , Xinru Wang

Posted Date: 20 February 2024

doi: 10.20944/preprints202402.1044.v1

Keywords: Conditional Privacy-preserving; VANETs; pseudonym; ECC

Article

An Efficient Conditional Privacy-Preserving Authentication for VANETs

Lu Zhang [1], Wuzheng Tan [2,*] and Xinru Wang [3]

[1] College of Cyber Security, Jinan University, Guangzhou, China
[2] College of Cyber Security, Jinan University, Guangzhou, China
[3] College of Cyber Security, Jinan University, Guangzhou, China
[*] Correspondence: 619536283@qq.com; Tel.: +86-150-1417-5851;
‡ These authors contributed equally to this work.

Abstract: With the rapid development of intelligent transportation, Vehicle Ad hoc Networks (VANETs) is becoming increasingly important.As a critical component of intelligent transportation systems, the Conditional Privacy-Preserving Authentication (CPPA) scheme plays a significant role in ensuring drivers' privacy and security.However, current CPPA schemes still face limitations in terms of security and efficiency, with these schemes either imposing higher computational overhead for enhanced security or compromising some level of security to reduce overhead. Motivated by this challenge, we propose a CPPA scheme that strikes a better balance between efficiency and security.By leveraging the token mechanism to achieve multiple authentication and minimizing information leakage. Furthermore, our performance analysis demonstrates that our ECC-based algorithm can significantly reduce overhead, with pseudonymous generation requiring only 0.0039ms.

Keywords: Conditional Privacy-preserving; VANETs; pseudonym; ECC

1. Introduction

As a significant research area within mobile ad hoc networks,Vehicular Ad Hoc Networks (VANETs) facilitates communication between vehicles and between vehicles and road-side infrastructure(RSU). Their primary objective is to ensure safer and more efficient road transportation by providing real-time information on traffic conditions, potential hazards, and vehicle statuses. As vehicles become increasingly interconnected, the importance of VANETs rises, opening avenues for innovative applications, ranging from collision warnings to dynamic route planning.As a result, the VANET has always been a research area focused on security and privacy, especially with the increasing information dissemination and exchange. In VANETs, each vehicle transmits traffic information to neighboring vehicles at intervals of 100-300 milliseconds using the Dedicated Short-Range Communication (DSRC) protocol. The beacon messages sent by vehicles contain safety-related information such as position, speed, and driving behavior [1].

While this communication protocol enables vehicles to receive real-time traffic information and enhance traffic management efficiency, it also presents vulnerabilities in an open environment. The transmitted plaintext data can be easily intercepted, monitored, or even tampered with by malicious third parties, resulting in the exposure of users' private information and irreversible harm [2].To address security and privacy concerns, numerous research papers have proposed CPPA schemes [3–17]. However,these schemes face limitations in terms of security and efficiency, with these schemes either imposing higher computational overhead for enhanced security or compromising some level of security to reduce overhead. In scheme [4],OBU requires large storage capacity to store pseudonyms and the authentication process involves complex bilinear mapping operations, which increases high-cost overhead. In scheme [8], the TA's involvement in the entire process results in a heavy workload and increases the risk of a single point of failure. In scheme [3], the inadequate management of pseudonyms exposes the system to vulnerabilities against Sybil attacks and the scheme [6] lacks mechanisms for revocation and mutual authentication.The insufficiencies of current solutions have served as our inspiration to design efficient solutions that achieve an enhanced equilibrium between safety and efficiency.The lightweight authentication scheme we developed is based on ECC and incorporates a token mechanism for achieving mutual authentication. This ensures minimal information leakage, with only the vehicle itself and TA being aware of the true identity of the vehicle. Furthermore, the lists maintained by the TA and RSUs facilitate efficient revocation of vehicles and prevent the reuse of pseudonyms by vehicles, effectively mitigating the risk of Sybil attacks.

Here are the main contributions of this paper:

- The token mechanism implemented ensures minimal privacy disclosure, wherein only the vehicle and TA possess the true identity of the vehicle.
- By enabling the RSU to centrally manage pseudonyms, it significantly alleviates the burden on TA and effectively safeguards against pseudonym abuse through a well-maintained revocation list, and make revocation easier.
- The performance analysis demonstrates that our scheme can achieve a reduced overhead, with the generation of a pseudonym for a vehicle requiring only 0.0039ms.

The remaining sections of this paper are organized as follows: Section 2 provides a comprehensive survey of related works in the field, while Section 3 presents the preliminaries, system model, and security requirements of the proposed scheme. In Section 4, we elaborate on the details of the proposed CPPA scheme, followed by an extensive security analysis in Section 5 and a thorough performance evaluation in Section 6. Finally, concluding remarks are presented in the last section.

2. 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 [18–20], ID-based [21–23], group signature-based [24,25], and pseudonymous-based [4–6, 8,11],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. [18] 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 et al. [19] proposed a PKI-based blockchain authentication scheme in which blockchain technology is combined with key derivation algorithms to achieve effective certificate management.In [20]'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. [21] 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. [22] proposed a LIAP scheme, which simplifies the complexity of revocation. However, it introduces bilinear pairing algorithms that require significant computational overhead. Additionally, in both [21,22] 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. [23] 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 [24], Nath et al. proposed a mutual authentication scheme. In this 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. [25] 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 [3–17]. 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 [4,6,12]. Qi et al. [12] 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 [4,12]. Although [6] avoids the use of bilinear mapping, its communication overhead is still not highly efficient. Ye et al. [11] 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 general, the proposed scheme provides better security and functionality compared to the existing schemes mentioned in Table 1.

Table 1. Comparison of our scheme with other schemes.

Scheme	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**	**S8**	**S9**	**S10**
[5]	✔	✔	✔	✔	✗	✔	✔	✔	✔	✔
[8]	✔	✔	✔	✔	✗	✔	✔	✔	✗	✔
[6]	✔	✔	✗	✔	✗	✔	✗	✔	✗	✔
[4]	✔	✔	✗	✔	✗	✔	✔	✗	✗	✔
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;

3. Preliminaries

In this section, we will introduce a network system that encompasses the Internet of Vehicles (IoV), security requirements, and elliptic curve cryptography.

3.1. System model

Figure 1 illustrates the standard architecture model of the vehicular ad hoc networks (VANETs) which primarily contains three entities: TA (Trust Authority), RSU (Roadside Unit), and V (Vehicle).

- TA: As a 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 TPD and OBU. The OBU is responsible for generating key pair, while the TPD can store the key pair and other sensitive datas.

3.2. Security Requirements

In this system, we have designed several security requirements that the vehicular network should achieve.

- **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.
- **Revocability**: If a vehicle engages in malicious behavior, both RSU and TA can collaborate to revoke the credentials or privileges of that vehicle.
- **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.

3.3. Elliptic Curve Cryptography

Let $\mathbb{F}_p$ represent a finite field where p is a large prime number.An elliptic curve E can be defined over $\mathbb{F}_p$ as $y^2 = x^3 + ax + b \pmod{p}$,where $a, b \in \mathbb{F}_p$ and $(4a^3 + 27b^2) \bmod p \neq 0$. Let's assume O is an infinity point on E,The set of points on the elliptic curve, including the point O, form an additive elliptic curve group $\mathbb{G}$ which has an order of q and generator P.

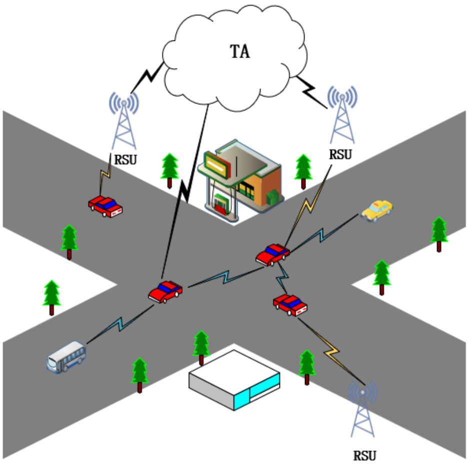

Figure 1. The system model of the VANETs

4. The Proposed Scheme

The proposed scheme will be comprehensively described in detail in this section.The scheme consists of five stages: system initialization stage, registration stage (which further includes vehicle registration and RSU registration), pseudonym generation stage, message signature stage, and message verification stage. The symbols employed in this scheme are illustrated in Table 2, providing a comprehensive overview of their meanings, usage, and other symbols that are described when used.

4.1. System initialization stage

1. Initially,the TA chooses an elliptic curve E,defined as $y^2 = x^3 + ax + b \pmod{p}$ over a finite field of prime order p,where p is a large prime number,and $a, b \in \mathbb{F}_p$.Subsequently, the TA chooses an additive group $\mathbb{G}$ that has an order of q. And P serves as the generator for $\mathbb{G}$.
2. Then the TA selects randomly a number $s \in \mathbb{Z}_q^*$,which serves as the master key of the system, and then computes$P_{pub} = sP$,which serves as the public key of the system.
3. Afterward,Four general one-way hash functions are selected by TA,which include $H : \{0,1\}^* \to \mathbb{Z}_q^*$, $H_0 : \mathbb{G} \to \mathbb{Z}_q^*$, $H_1 : \mathbb{G} \times \{0,1\}^* \to \mathbb{Z}_q^*$, $H_2 : \{0,1\}^* \times \mathbb{G} \times \{0,1\}^* \to \mathbb{Z}_q^*$.
4. Lastly,TA disseminates the public parameters $Params_{pub} = \{a, b, P, \mathbb{G}, H, H_0, H_1, H_2\}$ to all vehicles and RSUs,then, TA keeps s for itself.

Table 2. Involved notations in the paper

Notation	Description
V_i	The i-th vehicle
RSU	Road Side Unit
OBU	On Board Unit
TA	A reliable governmental entity
p, q	Two different large prime numbers
$\mathbb{G}, \mathbb{G}_1$	Cyclic additive group
$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$	Bilinear mapping
P	A generator of the group $\mathbb{G}$
E	An elliptic curve
s	The system's private key
P_{pub}	The system's public key
RID_i	The vehicle's true identity
PID_i	The vehicle's fake identity
$H(\cdot), H_0(\cdot), H_1(\cdot), H_2(\cdot)$	Four one-way hash functions
T_i	Current timestamp
m_i	A traffic-related message
(x)	Take the X-axis coordinate value
V_{token}	the vehicle's Valid token
R_{token}	the RSU's Valid token
V_{PK_i}	The i-th vehicle's public key
V_{SK_i}	The i-th vehicle's private key
R_{PK_i}	The i-th RSU's public key
R_{SK_i}	The i-th RSU's private key
$\oplus$	XOR operation
$\Vert$	Concatenation operation
σ_i	Message signing

4.2. Registration stage

1. The registration of Vehicle

   During the vehicle registration stage, all vehicles register offline. The registration process is as follows:

   (a) V generates its own private key $V_{SK} \in \mathbb{Z}_q^*$, then computes the public key $V_{PK} = V_{SK}P$.
   (b) V provides its real identity VID and public key V_{PK} to TA.

(c) TA first checks the registration list to determine if V has already registered. If V is already registered, TA rejects the registration. If V is not registered, then TA chooses a number $\alpha \in \mathbb{Z}_q^*$ randomly, and TA generates V_{token} for V and adds it to the list, setting the status of V as $legal$.

(d) Each row in the form is formatted as follows:$V_{ID}, V_{PK}, V_{token}, legal$.

(e) The process of TA generating V_{token} for V is as follows:

$$\begin{aligned} &P_1 = \alpha P, R_v = P_1(x) \\ &F_1 = H_0(V_{PK}) \\ &S_V = \alpha^{-1}(F_1 + sR_v) \pmod q \end{aligned} \tag{1}$$

(f) Finally, TA gets $V_{token} = (R_v, S_V)$ and sends it to the V.

2. The registration of RSU

   In this stage, the RSU obtains two seeds S_1, S_2 for generating pseudonyms, along with the corresponding token. The entire process is as follows:

(a) RSU generates its own private key $R_{SK} \in \mathbb{Z}_q^*$, then computes $R_{PK} = R_{SK}P$ which serves as its public key.

(b) RSU provides its real identity R_{ID} and public key R_{PK} to TA.

(c) TA randomly picks a number $\beta \in \mathbb{Z}_q^*$,then TA generates R_{token} for RSU, the process is as follows:

$$\begin{aligned} &P_2 = \beta P, A = P_2(x) \\ &F_2 = H_1(R_{PK} \| H_0(S_1 \| S_2)) \\ &S_R = \beta^{-1}(F_2 + sA) \pmod q \end{aligned} \tag{2}$$

(d) Lastly,TA generates $R_{token} = (A, S_R)$ for the RSU and selects two random seed values $S_1 \in \mathbb{Z}_q^*, S_2 \in \mathbb{Z}_q^*$, which are used for pseudonym derivation. TA then sends these values to the RSU.

(e) TA sends $\{R_{token}, S_1, S_2\}$ to the RSU via a protected channel.

4.3. Pseudonym generation stage

When V enters the RSU's domain and needs to request a service, the detailed procedure is outlined below.

1. V sends a service request =$\{V_{PK}, V_{token}, T\}$ to the RSU where $V_{token} = (R_v, S_v)$.
2. After receiving the request, The RSU will proceed with the verification.

- Firstly,The RSU checks the valid of T.If it is valid, the process continues; Otherwise, the RSU rejects the request.
- Secondly,The RSU checks if V_{PK} is in the revocation list (RL). If it is not in the RL, the process continues, otherwise the RSU rejects the request.
- Finally,the RSU verifies the V_{token}.It computes the value of $S_v{}^{-1}F_1P + S_v{}^{-1}R_vP_{pub}$, gets the x-coordinate value of the value and checks if it equals R_v.

3. If the verification not success, then the RSU refuses to provide services to the vehicle,otherwise, the RSU uses $\{S_1, S_2\}$ to generate pseudonyms,taking V_i as an example.

$$\begin{aligned} &S_{i,1} = S_1 \bigoplus V_{PK_i} \\ &S_{i,j} = H^j(S_{i,1}) \\ &S_{i,2} = S_2 \bigoplus V_{PKi} \\ &S_{i,w-j+1} = H^{w-j+1}(S_{i,2}) \\ &PID_{i,j} = H(S_{i,j} \bigoplus S_{i,w-j+1} \bigoplus T_j \bigoplus \zeta_{i,j}) \end{aligned} \tag{3}$$

where w represents the number of time periods in a day, $\zeta_{i,j} \in \mathbb{Z}_q^*$ is a number selected by RSU randomly in the j-th time interval,$j \in [1, w]$.
4. After generating the pseudonym, the RSU updates the information in the revocation list. For example, it adds a new row of information $\{V_{VPKi}, PID, available\}$, where $available$ means the pseudonym of the V_i is avaiable. The RSU then selects a random number $\theta \in \mathbb{Z}_q^*$,and generates a signature ε_R for (PID, R_{PK}, T_2). It responds to V_i with $response = \{PID, R_{token}, R_{PK}, H(S_1 S_2), T_2, \varepsilon_R\}$, where $\varepsilon_R = (C, X), R_{token} = (A, S_R)$.
5. The process of generating ε_R is as follows:

$$\begin{aligned} &P_3 = \theta P, C = P_3(x) \\ &F_3 = H_2(PID \| R_{PK} \| T_2) \\ &X = \theta^{-1}(H_2 + R_{SK} C) \bmod q \end{aligned} \tag{4}$$

6. Upon receiving the $response$, V_i performs necessary operations to verify the RSU's identity and the information's legitimacy. The specific steps are as follows:
   - Firstly, V_i checks whether T_2 is fresh. If that is the case, the process continues,or else the V_i rejects the request.
   - Then V_i verifies the legitimacy of the RSU. It computes the value of $S_R^{-1} F_2 P + S_R^{-1} A P_{pub}$ and gets the x-coordinate value of that value and checks if it is equal to A.
   - Lastly,V_i verifies the information by computing the value of $X^{-1} F_3 P + X^{-1} C R_{PK}$, gets the x-coordinate value of that value, and checks if it is equal to C.
   - If all the above equations hold true, then V_i accepts the information and uses the pseudonym for subsequent communication.

4.4. Message signature stage

After obtaining the pseudonym, the vehicle will use it for subsequent communication in this stage and the detailed steps are as follows:

1. For communication, V_i selects firstly a number $\omega_i \in \mathbb{Z}_q^*$ randomly.
2. Then, the V_i calculates the following formulas:

$$\begin{aligned} &P_4 = \omega_i P, Y = P_4(x) \\ &F_4 = H_2(m \| PID \| V_{PK} \| T_3) \\ &U = \omega_i^{-1}(F_4 + V_{SK} Y) \bmod q \end{aligned} \tag{5}$$

3. Lastly,the V_i sends $\{e = (Y, U), m, PID, V_{PK}, T_3\}$ to V_j.

4.5. Message verification stage

Upon receiving the tuple, V_j performs relevant verification and determine if it is false information,where $tuple = \{e = (Y, U), m, PID, V_{PK}, T_3\}$.

- Firtly,V_j validates the validity of T_2. If it is valid, the process continues,otherwise, V_j rejects.

- Then V_j accesses the revocation list and checks the legitimacy of PID. If it is marked as $available$, the process continue,but if it is marked as $revoked$, V_j rejects.
- Next V_j computes $H_2(m\|PID\|V_{PK}\|T_3)$ and the value of $U^{-1}F_4P + U^{-1}YV_{PK}$,and checks if the x-coordinate value of the value is equal to Y.
- If the equation holds true, it indicates the reliability of the message.Otherwise V_j finds that m is fake message, it will report to the RSU, which will report it to the TA by sending V_{PK}. Then the TA will update the status of V_{token} corresponding to VID_i as $illegal$. At the same time, the RSU will update the status of PID corresponding to V_{PKi} in the revocation list as $revoked$.The RSU will no longer distribute pseudonyms to V_i and remove it from the system.

5. Security Analysis

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

- **Anonymity**: The anonymous identity $PID_{i,j} = H(S_{i,j} \bigoplus S_{i,w-j+1} \bigoplus T_j \bigoplus \zeta_{i,j})$ serves to conceal the true identity,where $\zeta_{i,j}$ is a number selected randomly by RSU in the j-th time interval.Therefore, an Adv can never extract the real identity of the vehicle.In addition to that, when an RSU wants to check the validity of the generated pseudonym, it bases on (S_1, S_2). It does not require knowing the real identity of the vehicle, which satisfies conditional privacy preservation.
- **Traceability**: The message $tuple = \{e = (Y, U), m, PID, V_{PK}, T\}$that sent by the vehicle includes the V_{PKi}. When the RSU sends V_{PKi} 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 $tuple = \{e = (Y, U), m, PID, V_{PK}, T_3\}$, the receiver will compute $H_2(m \parallel PID \parallel V_{PK} \parallel T_3)$ and then verify the authenticity by checking if the result of the equation $U^{-1}F_4P + U^{-1}YV_{PK}$ is equal to Y. If the equation holds true, it indicates a successful authentication.
- **Revocation**: If a vehicle engages in malicious behavior, both the RSU and TA will revoke the vehicle by following these steps: When the V_j detects that m is false information, they report it to the RSU, which in turn reports it to the TA by sending the VPK. The TA updates the status of V_token corresponding to VID_i as $illegal$. Simultaneously, the RSU updates the status of PID corresponding to V_{PKi} in the revocation list as $revoked$. The RSU will cease distributing pseudonyms to V_i and remove it from the system.
- **Confidentiality**: In the RSU registration phase, the TA sends to the RSU a pair (S_1, S_2) to generate pseudonyms. S_1 and S_2 are sent via a secure channel and are known only by the TA, RSU. In the pseudonym generation stage, S_1 and S_2 are used for the generation of pseudonyms and they will never be sent. An Adv who tries to analyze a pseudonym to extract S_1 and S_2 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 (S_1, S_2) remains unmodifiable and is only known by the TA and RSU. An malicious adversary 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}. 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 R_{token} and signature. During inter-vehicle communication, the receiver will check the revocation list according to the pk and pseudonym of the sender to determine whether the other party is legitimate and the message is authentic by calculating $Sig(V_{pk}, e)$.
- **Replay attacks**: There is a system timestamp T in each message. The recipient can prevent replay attacks by verifying the validity of T.

- **Sybil attack**: The RSU not only imposes time and quantity limits on pseudonyms but also enforces strict restrictions. Specifically, the RSU only allocates a single new pseudonym to each vehicle within a given time period. It updates and stores the current list of valid pseudonyms. Any requests with invalid pseudonyms are directly rejected.
- **Man-in-the-middle attack**: Even if a malicious third party intercepts the message, they do not possess the sender's private key. Therefore, they can't forge the signature. The receiver can verify the authenticity of the message using sender's public key.

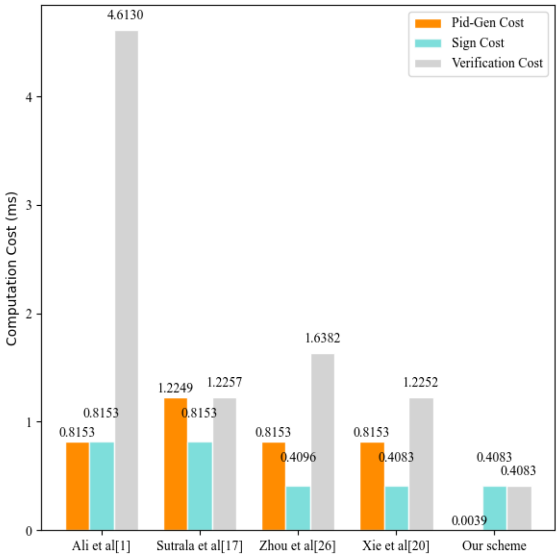

Figure 2. Comparison Of computational overhead.

6. Performance Evaluation

In this section, We assess the efficiency of our approach considering both the computational expense and the communication overhead. We contrast the proposed scheme with others [5,6,8], and Ali et al. [4] used the bilinear pairing operation, which can be represented as $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ where $\mathbb{G}_1$ is an additive group.Similarly, we use another additive group $\mathbb{G}$ based on ECC and an elliptic curve E.We utilized the well-known Miracl library to measure the execution time of all encryption operations. The corresponding operation execution times are displayed in Table 3.

doi:10.20944/preprints202402.1044.v1

Table 3. Execution time of the encryption operations

Notation	Description	Time(ms)
T_{pb}	The time required for executing bilinear pairing operation.	4.2039
T_h	The time required for executing one-way hash function.	0.0013
T_{bp-pm}	The time required for executing point multiplication operation in bilinear pairing.	1.537
T_{bp-pa}	The time required for executing point addition operation in bilinear pairing.	0.0069
T_{ecc-pm}	The time required for executing point multiplication operation in ECC.	0.407
T_{ecc-pa}	The time required for executing point addition operation in ECC.	0.0021

6.1. Computational Cost

Considering the overhead of computation, we primarily consider the cryptographic operations involved in pseudonym generation, message signing, and verification.

In the pseudonym generation phase, scheme [5] requires three hash operations and three point multiplication operations.Therefore, the time is $3T_h + 3T_{ecc-pm} \approx 1.2249ms$.In schemes [4,6,8], both of them require two point multiplication operations and one hash operation,so the time is $T_h + 2T_{ecc-pm} \approx 0.8153ms$.However,in our proposed scheme, we only require three hash operations, resulting in a time of $3T_h \approx 0.0039ms$.

In the individual message signing phase, scheme [5] requires one hash operation and two point multiplication operations.Thus, the execution time of the signature is $T_h + 2T_{ecc-pm} \approx 0.8153ms$.Scheme [8] needs one hash operation and one point multiplication operation,so the time is $T_h + T_{ecc-pm} \approx 0.4083ms$.In scheme [6], it requires two hash operations and one point multiplication operation.The verification needs time $2T_h + T_{ecc-pm} \approx 0.4096ms$. [4]'scheme,signing a message executes one hash operation and two point multiplication operations.Thus signing a message needs $T_h + 2T_{ecc-pm} \approx 0.8153ms$.In our proposed scheme, however, we only require one hash operation and one point multiplication operation.And the total time is$T_h + T_{ecc-pm} \approx 0.4083ms$.

In single message verification phase,scheme [5] requires two hash operations, one point addition operation, and three point multiplication operations.So the execution time is $2T_h + T_{ecc-pa} + 2T_{ecc-pm} \approx 1.2257ms$.In scheme [8], it requires three point multiplication operations and two point addition operations.So the execution time is $2T_{ecc-pa} + 3T_{ecc-pm} \approx 1.2252ms$.In scheme [6], it requires four point multiplication operations, three point addition operations, and three hash operations.Thus the execution time is $3T_h + 3T_{ecc-pa} + 4T_{ecc-pm} \approx 1.6382ms$.In scheme [4], it requires one bilinear pairing operation, one point multiplication operation, and one point addition operation,which needs whole time is $T_{pb} + T_{ecc-pm} + T_{ecc-pa} \approx 4.613ms$.In our proposed scheme, we require one hash operation and one point multiplication operation.So the time is $T_h + T_{ecc-pm} \approx 0.4083ms$.

As shown in Figure 2, compared to several relevant schemes [4–6,8], Our scheme exhibits relatively lower computational cost.

6.2. Communication Cost

We have conducted a detailed assessment of the communication expenditure of the aforementioned schemes in this phase.Let an element in $\mathbb{G}1$ has a size of 128 bytes, the element in $\mathbb{G}$ has a size of 40 bytes, and the $\mathbb{Z}q^*$ has a size of 20 bytes. Additionally, we assume that the hash function has a size of 20 bytes, the timestamp has a size of 4 bytes, the a pseudonym has a size of 20 bytes, and the message m has a size of 20 bytes.

Table 4. Comparative analysis of communication cost (bytes)

Scheme	Send a message
Sutrala et al. [5]	244
Xie et al. [8]	144
Zhou et al. [6]	228
Ali et al. [4]	556
Our scheme	124

In scheme [5], A message $\{AID_i = (AID_{i,1}, AID_{i,2}, \sigma_i = (f_i, g_i), B_i,$ $K_i, R_i, T_1, M_i)\}$ is transmitted by V_i, where $AID_{i,2}, f_i, g_i \in \mathbb{Z}_q^*$, $AID_{i,1}, B_i, K_i, R_i \in \mathbb{G}$,thus, the communication cost is (40 × 4 + 20 × 3 + 4 + 20) = 244 bytes.In scheme [8],the tuple sent from a vehicle is $\{PID_i, \sigma_i, M_i, T_i, R_i\}$,where $PID_i = (PID_{i,1}, PID_{i,2})$. $PID_{i,1}, R_i \in \mathbb{G}, PID_{i,2}, \sigma_i \in \mathbb{Z}_q^*$, Hence, the cost of communication is (40 × 2 + 20 × 2 + 4 × 1 + 20) = 144 bytes.In the paper [6], the message is $\{AID_{i,1}, AID_{i,2}, T_i, X_i, U_i, \eta_i, A_i, t_i, m_i\}$,where $AID_{i,1}, X_i, U_i, A_i \in \mathbb{G}$,$AID_{i,2}, \eta_i \in \mathbb{Z}_q^*$,and (T_i, t_i) is timestamp.So the communication overhead needs 40 × 4 + 20 × 2 + 4 × 2 + 20 = 228 bytes.In the paper [4],the tuple of messages sent by the vehicle is $\{PID_i = (PID_{i,1}, PID_{i,2}), PK_i = (R_i, U_i), T_i, \sigma_i, m_i\}$,where $PID_{i,1}, R_i, U_i, \sigma_i \in \mathbb{G}_1, PID_{i,2} \in \mathbb{Z}_q^*$.Therefore, the communication overhead needs 128 × 4 + 20 × 1 + 4 × 1 + 20 × 1 = 556 bytes.In our scheme,the vehicle broadcasts $\{e = (Y, U), m, PID,$ $T_3, V_{PK}\}$ to Neighboring vehicles, where $Y, U \in \mathbb{Z}_q^*, V_{PK} \in \mathbb{G}$.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 our scheme has lower communication overhead compared to other schemes [4–6,8]. [5,6,8].

7. Conclusions

This paper compares the limitations of existing schemes and proposes an efficient CPPA scheme that achieve a better balance between safety and efficiency.Furthermore, a comprehensive security analysis has demonstrated that our scheme successfully fulfills the essential security and privacy criteria for VANETs. Moreover, the evaluation of computational and communication overhead validates the enhanced efficiency offered by our proposed approach, rendering it more suitable for VANETs.

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. 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.
2. 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.
3. H. Zhong, L. Chen, J. Cui, J. Zhang, I. Bolodurina, and L. Liu, "Secure and lightweight conditional privacy-preserving authentication for fog-based vehicular ad hoc networks," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8485–8497, 2021.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of computer security*, vol. 15, no. 1, pp. 39–68, 2007.
19. 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.

20. 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.
21. A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology: Proceedings of CRYPTO 84 4*. Springer, 1985, pp. 47–53.
22. S. Wang and N. Yao, "Liap: A local identity-based anonymous message authentication protocol in vanets," *Computer Communications*, vol. 112, pp. 154–164, 2017.
23. 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.
24. H. J. Nath and H. Choudhury, "A privacy-preserving mutual authentication scheme for group communication in vanet," *Computer Communications*, vol. 192, pp. 357–372, 2022.
25. 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.
26. 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.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.