Conditional Privacy-Preserving Authentication Scheme for IoV Based on ECC

Peng-Shou Xie, Xiao-Jie Pan, Hong Wang, Jia-Lu Wang, Tao Feng, and Yan Yan
(Corresponding author: Xiao-Jie Pan)

School of Computer and Communications, Lanzhou University of Technology
No. 36 Peng-jia-ping road, Lanzhou, Gansu 730050, China
Email: 1075224210@qq.com

(Received July 23, 2021; Revised and Accepted Apr. 5, 2022; First Online Apr. 23, 2022)

Abstract

Internet of Vehicles (IoVs) is an important part of intelligent transportation systems that could improve the safety and efficiency of vehicle nodes. However, due to the mobility of IoVs, there are some security and privacy concerns in IoVs. The conditional privacy-preserving authentication (CPPA) scheme based on Elliptic Curve Cryptography (ECC) is proposed in this paper. This paper uses the small exponent test technology to achieve batch verification of multiple messages through Road Side Unit (RSU). To achieve anonymous authentication, our scheme uses the real identity of the vehicle node to generate an anonymous identity. According to security proof, our scheme can against adaptively chosen message attacks in the random oracle model. Furthermore, according to performance evaluation, our scheme reduces computation and communication costs without bilinear pairing. Therefore, our scheme is safer and more efficient than previous schemes, suitable for IoVs.

Keywords: Anonymous Identity; Authentication; Internet of Vehicles; Privacy-Preserving

1 Introduction

In recent years, with the progress of the development of wireless communication technology, IoVs have gradually become a promising research field [28]. As an application of intelligent transportation, IoVs have received a lot of attention as an important technology in the field of wireless network technology [3]. However, as an open wireless network, IoVs are in a state of high-speed movement, which has led to frequent privacy leakage accidents [26]. Thus, privacy of identity and secure communication cannot be ignored in IoVs [8].

In IoVs, each vehicle node transmits these messages to neighboring vehicle nodes via a dedicated short range communication (DSRC) protocol [2]. According to DSRC protocol, each vehicle in IoVs broadcasts a traffic message every 100-300 ms .Due to the fast-moving characteristics of vehicle nodes, vehicle nodes need to broadcast traffic message frequently, which require high real-time performance [17]. However, due to the limitations of wireless communication technology, vehicle nodes may suffer from message loss and forgery [24]. Therefore, it is necessary for receivers to authenticate messages and verify their integrity before receiving them. In addition, the security of traffic information and personal privacy is another issue in vehicle nodes communication [15]. In IoVs, attackers may obtain the user's personal information during the communication process, or obtain the vehicle's driving route by tracking the messages of On-Board Units OBU [11]. Besides, because the infrastructures in IoVs have the characteristics of openness and complexity, it will lead to a malicious attacker launches various attacks such as modification attack, denial of service attack(DoS) and so on [7, 23].

In recent years, security and privacy have become hot areas for IoVs. People want to enjoy the convenience of the vehicle network while keeping safety of the vehicle [20]. In order to solve these issues, a number of signature schemes for the authentication of traffic messages have been proposed by researchers.

1.1 Related Works

Security and privacy has always been an important area of research for IoVs. In order to achieve the secure communication between Vehicle-To-Vehicle (V2V) communication and Vehicle-To-Infrastructure (V2I)communication , a number of different authentication schemes have proposed in recent years [1]. Dissanayake *et al.* [6] proposed a novel digital signature algorithm with proving the efficiency against some kind of cyber attacks.The algorithm can be applied to the IoVs to ensure the security of messages. Hu *et al.* [9] used distributed and difficult-to-tamper characteristics of blockchain to propose an anonymous handover authentication scheme. Their scheme achieved robust security and high efficiency. Wang *et al.* [22] proposed a batch authentication scheme based identity. In their scheme, the secret key of the vehicle node depended on the RSU to prevent the leakage of vehicle node's secret key effectively. However, their scheme is vulnerable to attack as malicious vehicle nodes could impersonate legitimate vehicle nodes to generate false signatures. Wang *et al.* [21] proposed a secure blockchain based authentication scheme. In their scheme, a trusted cloud server is designed to store the anonymous certificates of vehicle nodes. Although the scalability of system is improved, many certificates increase computation cost and communication cost.

In 2020, Xu *et al.* [27] proposed a new certificateless aggregate signature scheme which is efficient in generating a signature and verification. Their scheme is secure under the extended computational Diffie-Hellman assumption.

In 2019, Alazzawi *et al.* [19] proposed an effective and robust authentication scheme for pseudo-identity communication. In their scheme, vehicle nodes sign a beacon so that the Trusted Authority(TA) obtains the real identity of the malicious vehicle nodes, and then deletes malicious vehicle nodes from the registration list. However, side-channel attacks can gain access to the private messages of the vehicle nodes, which undermines the security of the vehicle nodes.

Li *et al.* [13] proposed a lightweight authentication protocol. The protocol used hash functions and XOR operations to reduce communication cost. However, their protocol has relatively high storage overhead because of distribution and revocation of the certificate list, which is not suitable for IoVs. Elliptic curve cryptography is used in some authentication schemes [10, 25]. In their schemes, the system master key is generated by Private Key Generator (PKG), which eliminate the cost of certificate management and storage. However, the integrity of their schemes rely on the PKG, and there is a risk that the private key will be leaked once the PKG is attacked.

In 2020, Ali *et al.* [8] proposed an effective ID-based signature scheme. Their scheme used general one-way hash functions to speed up the process of signature verification. At the same time, their scheme supported batch verification of a large amount of information from vehicle nodes in high traffic density area, which reduces the computation cost of the RSU. However, bilinear pairing is used in verification scheme, which increases the computation cost in the verification phase.

Liu and Wang [9] proposed a conditional privacy-preserving scheme based on ring signature. In their scheme, the process of creating a ring is restricted, therefore ring members can be audited. However, the bilinear pairing operation causes the RSU increase the computation cost in message verification phase. Li *et al.* [20] proposed an effective message authentication scheme, which can resist the attack of key exposure. However, the scheme [20] uses Map-to-Point hash function operations, which increase computation cost in message verification phase.

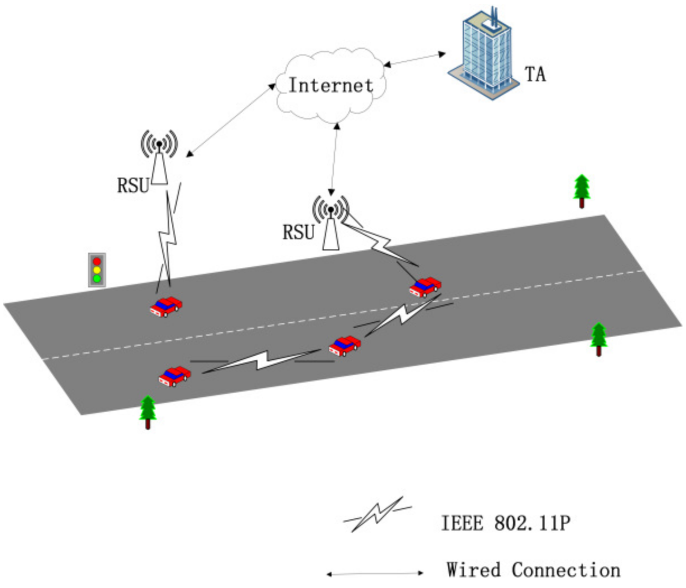

Figure 1: Network system of IoV

1.2 Our Contributions

In this paper, an efficient and secure authentication scheme is proposed in IoVs. The contributions of this paper are summarized as follows:

- Security analysis shows that our scheme can against forgery under adaptive chosen message attack under the random oracle model.
- Our scheme satisfies the security requirements for V2I communication in IoVs such as unlinkability requirements,traceability requirements and anonymous authentication.
- Our scheme without using pairing operations and Map-To-Point hash functions, which reduces computation cost and communication cost.

1.3 Organization

The rest of the this paper is organized as follows. Some preliminaries and security requirements are introduced for IoVs in Section2. The details of our scheme are shown in Section 3. Security analysis of our scheme is shown in Section 4. The performance of our scheme is shown in Section 5. Finally, Section6 concludes this paper.

2 Preliminaries

In this section, we introduce a network system of IoVs, security requirements and elliptic curve cryptography.

2.1 Network System

As shown in Figure 1, the network system of IoVs comprises three components:a trusted authority,a vehicle node, and an RSU. Three components are described as follow:

- **TA:** In IoVs, the TA is a registration center for RSUs and OBUs, which can obtain the real identity of vehicle nodes. System parameters are generated by the TA and sent to vehicle nodes.

- **RSU:** In IoVs, the RSU has higher computing power than OBUs. It is capable of receiving and verifying the authenticity of the traffic messages from vehicle nodes. In addition, the RSU can communicate with trusted authority to obtain some messages , such as notification messages.

- **OBU:** In IoVs, each vehicle node is equipped with an OBU. OBUs communicate with other RSUs and vehicle nodes based on the DSRC protocol. Compared to RSUs and TAs, OBUs have smaller computation power and storage capacity.

2.2 Security Requirements

In this paper, our scheme should satisfy security requirements as follows:

- **Message authentication and integrity**

  In IoVs, the RSU can ensure senders are legal vehicle nodes. In addition, the RSU can detect whether the messages have been tampered in the process of communication.

- **Identity privacy preserving**

  In IoVs, any RSU and vehicle node cannot obtain the real identity of vehicle nodes from traffic messages. The real identity of vehicle nodes can only be obtained by the trusted authority when privacy of vehicle nodes is threatened.

- **Traceability**

  In IoVs, the TA as a trusted authority has the ability to obtain the real identities of attackers when malicious attackers destroy messages, then marks attackers as illegal nodes.

- **Unlinkability**

  Malicious attackers receive some messages from a vehicle node, but attackers could not infer that these messages come from the same vehicle node.

2.3 Elliptic Curve Cryptography

We assume that F_p is the finite field, which p is a prime number. An elliptic curve E over a finite field F_p and be defined as $y^2 = y^3 + ax + b \bmod p$,where $a, b \in F_p$ and $(4a^3 + 27b^2) \bmod q \neq 0$.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.

3 The Proposed Scheme

In this section, a secure and efficient conditional privacy-preserving authentication scheme is proposed in detail for IoVs. Our scheme consists of the following five phases: system initialization phase, handshaking phase, anonymous identity generation phase, message signing phase and message verification phase. The notations used in the scheme are shown in Table 1.

Table 1: Notations

Notations	Description
V_i	The ith vehicle node
RSU	A roadside unit
OBU	A onboard unit
p, q	Two large prime numbers
s	The private key of the system
G	Cyclic additive group
P	A generator of the group G
P_{pub}	The public key of the system
AID_i	The anonymous identity of a vehicle node
OID_i	The real identity of a vehicle node
h_0, h_1, h_2	Three one-way hash functions
T_i	Current timestamp
M_i	Message
$\|$	The message concatenation operation
R	The exclusive-OR operation

Step 1. System initialization phase

1) The TA selects an elliptic curve as $y^2 = y^3 + ax + b \bmod p$. Then, TA selects an additive group G with the order q. The P is a generator of additive group G.

2) The TA chooses a number $s \in Z_q^*$ as the master key of the system randomly, and then computes $P_{pub} = sP$ as master public key. Three one-way general hash functions such as $h_0 : \{0,1\}^* \rightarrow Z_q^*$,$h_1 : \{0,1\}^* \rightarrow Z_q^*$,$h_2 : \{0,1\}^* \rightarrow Z_q^*$ are chosen by the TA. Hash function h_0 is not published across IoVs because of it only involve in generating an anonymous identity AID_i.

3) Public parameters of the system are set $params = \{G, q, P, P_{pub}, h_1, h_2\}$.Then, the TA publish params to RSUs and vehicle nodes through secure channel.

Step 2. Handshaking phase

1) When the vehicle node V_i enters the communication range of the RSU, real identity OID_i of the vehicle node is encrypted by the RSU's public key into $Q = ENC_{PK_{RSU}}(OID_i, SIG_{SK_{OBU}}(OID_i))$. Then, the vehicle node V_i sends handshake

message $Z = (Q, T_i)$ to the RSU, where T_i is a timestamp.

2) Once handshake message Z is received, the RSU checks whether T_i is valid. If T_i is valid, the RSU decrypts Z to get real identity OID_i. Then, the RSU encrypts OID_i and identity of RSU RID_i into $W = ENC_{PK_{TA}}((OID_i, RID_i))$ by TA's public key PK_{TA}. Finally, W is sent to TA.

3) Once W is received, TA decrypts W to get OID_i and RID_i. Then, TA checks whether RID_i is in the registration list. If so, then TA continues to check whether OID_i is not in revocation list. If OID_i is not in revocation list, the RSU and vehicle node V_i are allowed to join IoVs, then TA sends a notification message $(verified, u_i, a_i)$ to the RSU. Otherwise TA sends a notification message (not verified)to the RSU.Two secret values u_i and a_i are generated by TA.

4) Once notification message is received, the RSU checks notification message whether is $(verified, u_i, a_i)$, If so, the RSU computes $A_i = a_i P$ and $U_i = u_i P$. Otherwise the vehicle node V_i will be identified as illegal. We assume that β_i is the unique symbol of the vehicle node, where $\beta_i = U_i + A_i$. Finally, the RSU sends β_i to TA and the vehicle node V_i.

Step 3. Anonymous identity generation phase

Before generating an anonymous identity, the vehicle node V_i inputs the unique real identity OID_i and password PWD_i to the tamper-proof device firstly. The tamper-proof device checks whether OID_i and PWD_i are equal to the stored values. If they are equal, the anonymous identity is generated as follows.

1) TPD generates a secret value $\gamma_i \in Z_q^*$ randomly and computes $AID_{i,1} = \gamma_i P$. Then, the tamper-proof device sends $(AID_{i,1}, OID_i)$ to TA through secure channel.

2) Once $(AID_{i,1}, OID_i)$ is received, the TA computes $AID_{i,2} = OID_i \oplus h_0(sAID_{i,1} \parallel t_i)$, where t_i is the timestamp that shows the validity of time for AID_i. Then, TA computes $SK_i = \eta_{AID_i} s \bmod q + u_i$. The secret key of the anonymous vehicle node V_i is (β_i, SK_i). In addition, we defined that $AID_i = (AID_{i,1}, AID_{i,2} \parallel t_i)$ and $\eta_{AID_i} = h_1(AID_i \parallel \beta_i)$.

Step 4. Message signing phase

In this phase, TA sends AID_i and (β_i, SK_i) to the vehicle node V_i through secure channel. Then vehicle node V_i signs message to ensure the authenticity of the message. The process of signing a message is as follows:

1) The vehicle node V_i randomly selects a number $r_i \in Z_q^*$. Then, the vehicle node V_i computes $R_i = r_i P$ and $\sigma_i = r_i + \mu_{AID_i}(a_i + SK_i \bmod q)$. The signature of a message M_i is (σ_i, R_i). Note that the R_i can be preloaded to the vehicle node V_i. We define that $\mu_{AID_i} = h_2(R_i \parallel AID_i \parallel M_i \parallel SK_i \parallel T_i)$ and $AID_i = (AID_{i,1}, AID_{i,2})$.

2) Finally, the vehicle node V_i sends a message as $\{\mathrm{AID}_i, \sigma_i, \mathrm{M}_i, \mathrm{T}_i, \mathrm{R}_i\}$ to nearby RSUs.

Step 5. Message verification phase

In this phase, the RSU receives a message as $\{\mathrm{AID}_i, \sigma_i, \mathrm{M}_i, \mathrm{T}_i, \mathrm{R}_i\}$ and verifies the validity of the message. Once the message is received, the RSU checks timestamp T_i whether is fresh firstly. If so, the RSU continues to verify the message. Otherwise, the RSU discards the message. The process of verification as follows:

Single Verification.

Once $\{\mathrm{AID}_i, \sigma_i, \mathrm{M}_i, \mathrm{T}_i, \mathrm{R}_i\}$ is received from the vehicle node V_i, the RSU checks whether the following Equation (1) holds.

$$\sigma_i P = R_i + \mu_{AID_i}(\beta_i + \eta_{AID_i} P_{pub}) \tag{1}$$

If the Equation (1) holds, we can conclude that message $\{\mathrm{AID}_i, \sigma_i, \mathrm{M}_i, \mathrm{T}_i, \mathrm{R}_i\}$ is valid. The correctness of the Equation (1) is as follows:

$$\begin{aligned}
&\sigma_i P = (r_i + \mu_{AID_i}(a_i + SK_i \bmod q))P \\
&= r_i P + \mu_{AID_i}(a_i P + (\eta_{AID_i} s \bmod q + u_i)P) \\
&= R_i + \mu_{AID_i}(A_i + \eta_{AID_i} P_{pub} + U_i) \\
&= R_i + \mu_{AID_i}(\beta_i + \eta_{AID_i} P_{pub})
\end{aligned}$$

Therefore, the correctness of the Equation (1) is proved. The message from vehicle node V_i has not been altered by malicious attackers.

Batch Verification.

In order to improve the efficiency of verification, our scheme supports batch verification. The small exponent test technology [18] is used to batch verification. Once multiple messages are received from the vehicle node as $\{AID_1, \sigma_1, M_1, T_1, R_1\}$,$\{AID_2, \sigma_2, M_2, T_2, R_2\}$, $\{AID_n, \sigma_n, M_n, T_n, R_n\}$. The RSU checks whether Equation (2) holds for the following:

$$\begin{aligned}
(\sum_{i=1}^{n} \nu_i \sigma_i)P &= \sum_{i=1}^{n} \nu_i R_i \\
&+ \sum_{i=1}^{n} \nu_i \mu_{AID_i}(\beta_i + \eta_{AID_i} P_{pub})
\end{aligned} \tag{2}$$

If Equation (2) holds, we can conclude that multiple messages are valid. The correctness of the

Equation (2) is as follows:

$$\begin{aligned}
&(\sum_{i=1}^{n} v_i\sigma_i)P \\
=\ &(\sum_{i=1}^{n} v_i(r_i+\mu_{AID_i}(a_i+SK_i \bmod q)))P \\
=\ &(\sum_{i=1}^{n} v_ir_i)P+(\sum_{i=1}^{n} v_i\mu_{AID_i}(a_iP \\
&\quad +(\eta_{AID_i}s \bmod q+u_i)P)) \\
=\ &\sum_{i=1}^{n} v_iR_i+\sum_{i=1}^{n} v_i\mu_{AID_i}(A_i \\
&\quad +\eta_{AID_i}P_{pub}+U_i) \\
=\ &\sum_{i=1}^{n} v_iR_i+\sum_{i=1}^{n} v_i\mu_{AID_i}(\beta_i+\eta_{AID_i}P_{pub})
\end{aligned}$$

Therefore, the correctness of Equation (2) is proved.The messages from vehicle node V_i have not been altered by malicious attackers.

4 Security Proof and Security Analysis

The security of our scheme is proved in this section. Through security analysis, we have proved that our scheme can achieve the security requirements proposed in Section 3.

4.1 Security Proof

Mathematical Model: The security proofs of our proposed CPPA protocol is given in this subsection. The security model of proposed scheme is defined through a game played between a challenger C and an adversary A.Random oracle model is a mathematical model which abstracted from the hash function. It is widely used in provable security. In this paper, we use random oracle model to prove the our scheme is secure against adaptive chosen message attack. The adversary A could make the following queries in the game.

- Setup-Oracle: This query simulates the initialization of the VANET system.The system parameters are sent to the adversary A.
- $h_1$oracle: In response to this query, challenger C chooses a random number $r \in Z_q^*$ inserts the tuple (m, r) into the list Lh_1 and returns r to adversary A.
- $h_2$oracle: In response to this query, challenger C chooses a random number $r \in Z_q^*$ inserts the tuple (m, r) into the list Lh_2 and returns r to adversary A.
- Sign-Oracle: In this query, the adversary A sends a traffic information message M_i to challenger C.In response, C sends {AID$_i$,σ_i,M$_i$,T$_i$,R$_i$} to the adversary A.

Theorem 1. *We assume that times of algorithm A requests random oracle query and request signature oracle query is Q and Y respectively. If our conditional privacy-preserving authentication scheme can be broken by algorithm A , then there is an algorithm C to solve the ECDL problem.*

Proof. We assume that A is an adversary that could forge the message {AID$_i$,σ_i,M$_i$,T$_i$,R$_i$} . Then, ECDL problem is be solved by challenger C with a non-negligible probability. The Lh_1 and Lh_2 are lists which maintained by the C. Now, query phase is shown as follows:

Setup-Oracle. Challenger C picks a number s randomly as its master key. Then, C calculates the public key as $P_{pub} = sP$ and sends system parameters $params = \{G, q, P, h_1, h_2\}$ to A.

h_1 **oracle.** The Lh_1 is a list which maintained by C. When adversary A issues a query with message (AID_i, β_i) to C, the C checks whether $\langle AID_i, \beta_i, \tau_1\rangle$ exists in Lh_1. If so, C issues $\tau_1 = h_1(AID_i, \beta_i)$ to A; otherwise, C picks a number $\tau_1 \in Z_q^*$ and then adds (AID_i, β_i) into Lh_1. Finally, C returns $\tau_1 = h_1(AID_i, \beta_i)$ to A.

h_2 **oracle.** The Lh_2 is a list which maintained by C. When adversary A issues a query with message $(R_i, AID_i, M_i, SK_i, T_i)$ to C, the C checks whether $\langle R_i, AID_i, M_i, SK_i, T_i, \tau_i\rangle$ exists in Lh_2. If so, C issues $\tau_2 = h_2(R_i, AID_i, M_i, SK_i, T_i)$ to A; otherwise, C picks a number $\tau_2 \in Z_q^*$ and then adds $(R_i, AID_i, M_i, SK_i, T_i)$ into Lh_2. Finally, C returns $\tau_2 = h_2(R_i, AID_i, M_i, SK_i, T_i)$ to A.

Sign-Oracle. When adversary A issues a query with a message M_i, challenger C checks the $\langle AID_i, \beta_i, \tau_1\rangle$ from Lh_1 firstly. The C then retrieves τ_1 from $\langle AID_i, \beta_i, \tau_1\rangle$ and selects two numbers r_i and H_i. Next, C selects two random numbers s_i and l_i to try again. The C computes $R_i = H_i^{-1}s_iP - Q$ and $\sigma_i = s_i$, then returns (R_i, σ_i) to A. We set H_i as $h_2(R_i, AID_i, M_i, SK_i, T_i)$.

The A could achieve two valid signatures $(R_i, \sigma_i = r_i + H_i(a_i + SK_i \bmod q))$ and $(R_i, \sigma'_i = r_i + H'_i(a_i + SK_i \bmod q))$ by forking lemma , where $H_i \neq H'_i$. The C can get value of r_i as follows:

$$\begin{aligned}
&\frac{H'{}_i\sigma_i - H_i\sigma'{}_i}{H'{}_i - H_i} \bmod q \\
=\ &\frac{H'{}_ir_i + H'{}_iH_i(a_i+SK_i) - H_ir_i - H_iH'{}_i(a_i+SK_i)}{H'{}_i - H_i} \\
=\ &r_i
\end{aligned}$$

We have proved the our scheme can against forgery under adaptive chosen message attack in the random oracle model.

□

4.2 Security Analysis

In this subsection, we introduce our scheme satisfies some security requirements as follows:

- **Message authentication and integrity**

  According to the above security proof, the ECDL problem is difficult to solve. Thus, malicious attackers cannot forge any signature. RSUs can verify the correctness of Equation (1) to determine whether the messages from a vehicle node has been tampered or forged by malicious attackers. Thus, we make a conclusion that our scheme satisfies message authentication and integrity.

- **Identity privacy preserving**

  In anonymous identity generation phase, our scheme generates anonymous identities $AID_{i,1}$ and $AID_{i,2}$. According to $AID_{i,2} = OID_i \oplus h_0(sAID_{i,1} \parallel t_i)$ and $AID_{i,1} = \gamma_i P$, the anonymous identity $AID_i = (AID_{i,1}, AID_{i,2})$ contains two random secret numbers γ_i and s. In order to get OID_i, malicious attackers must compute $sAID_{i,1} = s\gamma_i P$ from $P_{pub} = sP$ and $AID_{i,1} = \gamma_i P$. It means that attackers must solve CDH problem. Thus, we make a conclusion that our scheme satisfies identity privacy-preserving .

- **Traceability**

  The real identity of a vehicle node is not available to any RSU or vehicle node. However, as a trusted authority, TA can obtain the real identity of malicious attackers when malicious attackers destroy messages. As a trusted center, TA computes $OID_i = AID_{i,2} \oplus h_0(sAID_{i,1} \parallel t_i)$ through $\{AID_n, \sigma_n, M_n, T_n, R_n\}$.Thus, we make a conclusion that our scheme satisfies traceability.

- **Unlinkability**

  Our scheme chooses two random secret numbers γ_i and s to generate an anonymous identity AID_i, where $AID_{i,2} = OID_i \oplus h_0(sAID_{i,1} \parallel t_i)$ and $AID_{i,1} = \gamma_i P$. In addition, the vehicle node V_i chooses a random secret number r_i to generate a signature. That is to say, each message from vehicle node V_i has an unique anonymous identity and signature. Attackers can not link any message. Thus, we make a conclusion that our scheme satisfies unlinkability.

5 Performance Evaluation

In this section, we evaluate the performance of schemes in terms of computation cost and communication cost. The schemes [4,21,27] are based on ECC. The schemes [8,9,17, 20] are based on bilinear pairing. Our scheme is compared with these schemes.

5.1 Computation Cost

In this paper, we use a famous cryptographic library MIRACL to calculate the execution time of cryptographic operations. The experiment of our scheme is performed on a PC equipped with an Intel i5 2.30 GHZ CPU and 8 GB memory. The execution time of the encryption operations are shown in Table 2. We denote T_{BP} as the execution time of bilinear pairing operation, T_H as the execution time of Map-To-Point hash function,T_{PM-BP} as the execution time of point multiplication operation in bilinear pairing, T_{PA-BP} as the execution time of point addition operation in bilinear pairing,T_{PM-ECC} as the execution time of point multiplication operation in ECC, T_{PA-ECC} as the execution time of point addition operation in ECC.

Table 2: Execution time of the encryption operations

Cryptographic operation	Execution time(ms)
T_{BP}	4.2110
T_H	4.406
T_{PM-BP}	1.709
T_{PA-BP}	0.0071
T_{PM-ECC}	0.442
T_{PA-ECC}	0.0018

In single message verification phase, the Ali *et al.*'s scheme [8] requires one bilinear pairing operation, one point multiplication operation in bilinear pairing and one point addition operation in bilinear pairing. Thus, the verification time in this phase is $1T_{BP} + 1T_{PM-BP} + 1T_{PA-BP} \approx 5.9271ms$. In batch message verification, the verification time is $1T_{BP} + nT_{PM-BP} + nT_{PA-BP} \approx 1.7161n + 4.2110ms$. Similarly, the execution times of the other three schemes based on bilinear pairing are shown in Table 3.

In single message verification phase, our scheme requires three point multiplication operations in ECC and two point addition operations in ECC. Thus, the verification time in this phase time in this phase is $3T_{PM-ECC} + 2T_{PA-ECC} \approx 1.3296ms$.In batch message verification, the verification time is $(n+2)T_{PM-ECC} + (3n-1)T_{PA-ECC} \approx 0.4474n + 0.8822ms$. Similarly, the execution times of the other three schemes based on ECC are shown in Table 3.

The percentage improvement of our scheme with respect to single and batch signature verifications as compared to the scheme [17] is $\frac{7.6290-1.3296}{7.6290} \approx 82.57\%$ and $(\frac{3.4180n+4.2110-(0.4474n+0.8822)}{3.1480n+4.2110}) \approx 86.81\%$, respectively,where $n = 100$ is the number of signatures.Other percentage improvement could be achieved by using a similar method.The improvement on computation cost of the our scheme is shown in the Table 4.

The computation cost of single message verification is shown in Figure 2. From Figure 2, it can be seen that the computation cost of our scheme is lower than schemes [8,9,17,20] because of bilinear pairing is not used in our scheme. In schemes [4, 21, 27] based on ECC, the

Table 3: Comparison of computation cost

Scheme	Single Verification(ms)	BatchVerification(ms)
Scheme [17]	$2T_{PM-BP} + 1T_{BP} \approx 7.6290$	$1T_{BP} + 2nT_{PM-BP} \approx 3.4180n + 4.2110$
Scheme [8]	$1T_{BP} + 1T_{PM-BP} + 1T_{PA-BP} \approx 5.9271$	$1T_{BP} + nT_{PM-BP} + nT_{PA-BP} \approx 1.7161n + 4.2110$
Scheme [9]	$2T_{BP} + 1T_{PM-BP} \approx 10.1310$	$2T_{BP} + nT_{PM-BP} \approx 1.7090n + 8.4220$
Scheme [20]	$T_{BP} + 1T_{PM-BP} + 1T_{PA-BP} + 1T_H \approx 14.5441$	$2nT_{BP} + nT_{PM-BP} + nT_{PA-BP} + nT_H \approx 14.5441n$
Scheme [4]	$4T_{PM-ECC} + 3T_{PA-ECC} \approx 1.7734$	$(2n + 3)T_{PM-ECC} + (4n - 1)T_{PA-ECC} \approx 0.8912n + 1.3242$
Scheme [21]	$4T_{PM-ECC} + 3T_{PA-ECC} \approx 1.7734$	$(2n + 2)T_{PM-ECC} + (4n - 1)T_{PA-ECC} \approx 0.8912n + 0.8822$
Scheme [27]	$4T_{PM-ECC} + 2T_{PA-ECC} \approx 1.7716$	$(2n + 2)T_{PM-ECC} + (3n - 1)T_{PA-ECC} \approx 0.8894n + 0.8822$
Our Scheme	$3T_{PM-ECC} + 2T_{PA-ECC} \approx 1.3296$	$(n + 2)T_{PM-ECC} + (3n - 1)T_{PA-ECC} \approx 0.4474n + 0.8822$

Table 4: Percentage improvement of the our scheme over other scheme

Scheme	Single Verification	Batch Verification
Scheme [17]	82.57%	86.81%
Scheme [8]	77.57%	74.05%
Scheme [9]	86.88%	74.56%
Scheme [20]	90.86%	96.86%
Scheme [4]	23.05%	49.56%
Scheme [21]	25.03%	49.31%
Scheme [27]	24.97%	49.21%

computation cost of our scheme is lower than Wang *et al.*'s scheme [4] and Ming *et al.*'s scheme [21] because of our scheme uses less point operation in message signing phase. The computation cost of batch signature verification is shown Figure 3, which increases with the number of messages.

5.2 Communication Cost

The size of the elements in G_1 is 128 bytes and the size of the elements in G is 40 bytes. In addition, we suppose that the size of a general one-way hash function is 20 bytes, and the size of a time-stamp is 4 bytes. In Lawrence *et al.*'s scheme [4], the signature $\{\sigma_i, t_i\}$ is sent from a vehicle node to the receiver, where $\sigma_i = (k_i, U_i, S_i)$, $U_i, S_i \in G_1$ and $k_i \in Z_q^*$. Thus, the communication cost is $128 \times 2 + 20 + 4 = 280 bytes$. In Ali *et al.*'s scheme [5], the signature $\{AID_i, \sigma_i, t_i\}$ is sent from a vehicle node to the receiver,where $\sigma_i = (A_i, B_i)$,$AID_i = (AID_{i,1}, AID_{i,2})$, $A_i, B_i, AID_{i,1} \in G_1$ and $AID_{i,2} \in Z_q^*$. Thus, the communication cost is $128 \times 3 + 20 + 4 = 408 bytes$. In Wang and Liu.'s scheme [14], the signature $\{AID_i, \sigma_i, t_i\}$ is sent from vehicle node to the receiver, where $\sigma_i = (A_i, B_i)$ and $A_i, B_i, AID_i \in G_1$.Thus, the communication cost is $128 \times 3 + 20 + 4 = 408 bytes$. In Liu *et al.*'s scheme [12], the signature $\{OID_i, \sigma_i, t_i\}$ is sent from a vehicle node to the receiver, where $\sigma_i = (A_i, B_i, C_i)$, $A_i, B_i, C_i \in G_1$ and $OID_i \in Z_q^*$. Thus, the communication cost is $128 \times 3 + 20 = 404 bytes$.

In Wang *et al.*'s scheme [22], the signature $\{AID1_{i,j}, AID2_{i,j}, U_{i,j}, \nu_{i,j}, T_i\}$ is sent from vehicle node to the receiver, where $AID1_{i,j}, AID2_{i,j}, U_{i,j} \in G$. Thus, the communication cost is $40 \times 3 + 20 \times 1 + 4 \times 1 = 144 bytes$.In Ming *et al.*'s scheme [16], the signature $\{AID_i, tt_i, P_i, D_i, R_i, \sigma_i\}$ is sent from a vehicle node to the receiver, where $AID_i = (AID_{i,1}, AID_{i,2})$ and $P_i, D_i, R_i, \sigma_i \in Z_q^*$. Thus, the communication cost is $40 \times 1 + 20 \times 4 + 4 \times 1 = 124 bytes$. In Thumbur *et al.*'s scheme [19],the signature $\{vpk_i, PID_i, T_i, \sigma_i\}$ is sent from a vehicle node to the receiver, where $PID_i = (PID_{i,1}, PID_{i,2}) \in G$, $\sigma_i = (U_i, S_i)$, $U_i, vpk_i \in G$ and $S_i \in Z_q^*$. Thus, the communication cost is $40 \times 4 + 20 \times 1 + 4 \times 1 = 184 bytes$. In our scheme, the signature $\{AID_i, \sigma_i, M_i, T_i, R_i\}$ is sent from a vehicle node to the receiver, where $PID_i = (PID_{i,1}, PID_{i,2})$, $PID_{i,1}, R_i \in G$ and $PID_{i,2}, \sigma_i \in Z_q^*$. Thus, the communication cost is $40 \times 2 + 20 \times 2 + 4 \times 1 = 124 bytes$.

As can be seen from Table 5, the bilinear pairing-based scheme [8,9,17,20] has higher communication costs than our scheme. In the schemes [4, 21, 27] based on ECC, the communication cost of our scheme is lower than schemes [4, 27]. Although our scheme is the same as scheme [21], it is superior to scheme [21] in individual signature verification and batch signature verification.

6 Conclusions

In this paper, a CPPA scheme is proposed, which uses a batch signature verification method to allow RSUs to

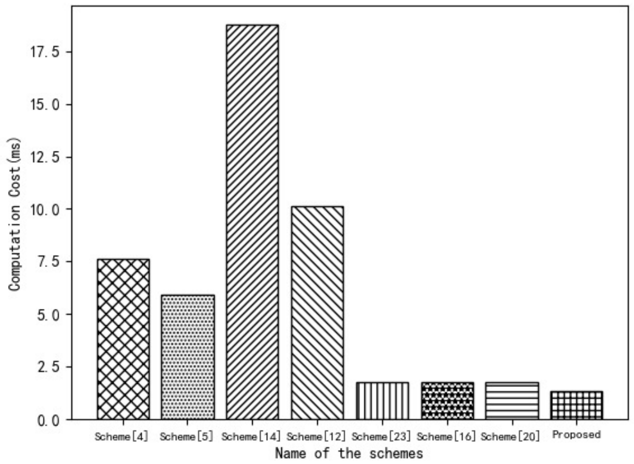

Figure 2: Computation cost for single message verification

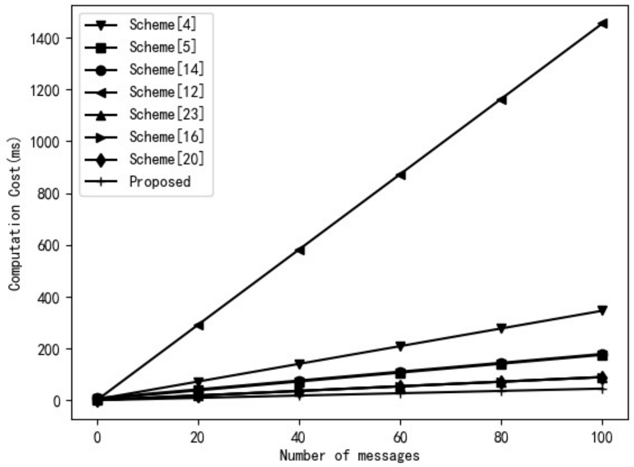

Figure 3: Computation cost for batch messages verification

Table 5: Comparison of communication cost

Scheme	Send a message	Send n messages
Scheme [17]	208 bytes	208 bytes
Scheme [8]	408 bytes	408 bytes
Scheme [9]	408 bytes	408 bytes
Scheme [20]	404 bytes	404 bytes
Scheme [4]	144 bytes	144 bytes
Scheme [21]	124 bytes	124 bytes
Scheme [27]	184bytes	184bytes
Our scheme	124 bytes	124 bytes

verify multiple messages. In order to prevent vehicle nodes from exposing their identities, our scheme generates anonymous identity during transmission. For malicious vehicle nodes, the trust authority TA can obtain its real identity, which realizes conditional privacy-preserving authentication. We provide a security analysis to show our CPPA scheme can satisfy security and privacy requirements. Hence, our scheme is suitable for IoVs.

Our scheme only considers the identity privacy of vehicle nodes, and does not consider the location privacy and route of vehicle nodes. In addition, the safety of vehicle nodes depends on TPD. Once the TPD is attacked, the safety of vehicle nodes will be destroyed. In the future, we should reduce the dependence of vehicle nodes on TPD and strengthen the protection of location privacy.

Acknowledgments

This research is supported by the National Natural Science Foundations of China under Grants No.61862040, No.61762059 and No.6176 2060.The authors gratefully acknowledge the anonymous reviewers for their helpful comments and suggestions.

References

[1] M. A. Al-shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "An efficient identity-based conditional privacy-preserving authentication scheme for secure communication in a vehicular ad hoc network," *Symmetry*, vol. 12, no. 10, p. 1687, 2020.

[2] I. Ali, Y. Chen, N. Ullah, M. Afzal, and W. He, "Bilinear pairing-based hybrid signcryption for secure heterogeneous vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, 2021.

[3] I. Ali, A. Hassan, and F. Li, "Authentication and privacy schemes for vehicular ad hoc networks (vanets): A survey," *Vehicular Communications*, vol. 16, no. APR., pp. 45–61, 2019.

[4] I. Ali, T. Lawrence, A. A. Omala, and F. Li, "An efficient hybrid signcryption scheme with conditional privacy-preservation for heterogeneous vehicular communication in vanets," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 11 266–11 280, 2020.

[5] I. Ali and F. Li, "An efficient conditional privacy-preserving authentication scheme for vehicle-to-infrastructure communication in vanets," *Vehicular Communications*, vol. 22, p. 100228, 2020.

[6] M. W. Dissanayake, "A novel scheme for digital signatures," *International Journal of Electronics and Information Engineering*, vol. 11, no. 2, pp. 61–72, 2019.

[7] Z. Guo, "Cryptanalysis of a certificateless conditional privacy-preserving authentication scheme for wireless

body area networks," *International Journal of Electronics and Information Engineering*, vol. 11, no. 1, pp. 1–8, 2019.

[8] J. Han, Y. Li, and W. Chen, "A lightweight and privacy-preserving public cloud auditing scheme without bilinear pairings in smart cities," *Computer Standards & Interfaces*, vol. 62, pp. 84–97, 2019.

[9] C. Hu, D. Zheng, R. Guo, A. Wu, L. Wang, and S. Gao, "A novel blockchain-based anonymous handover authentication scheme in mobile networks," *International Journal of Network Security*, vol. 22, no. 5, pp. 874–884, 2020.

[10] J. Jenefa and E. M. Anita, "An enhanced secure authentication scheme for vehicular ad hoc networks without pairings," *Wireless Personal Communications*, vol. 106, no. 2, pp. 535–554, 2019.

[11] L. Kang and L. Zhang, "A privacy-preserving data sharing system with decentralized attribute-based encryption scheme," *International Journal of Network Security*, vol. 22, no. 5, pp. 815–827, 2020.

[12] J. Li, Y. Liu, Z. Zhang, B. Li, H. Liu, and J. Cheng, "Efficient id-based message authentication with enhanced privacy in wireless ad-hoc networks," in *2018 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2018, pp. 322–326.

[13] X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar, and N. Kumar, "A lightweight privacy-preserving authentication protocol for vanets," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3547–3557, 2020.

[14] F. Liu and Q. Wang, "Ibrs: An efficient identity-based batch verification scheme for vanets based on ring signature," in *2019 IEEE Vehicular Networking Conference (VNC)*. IEEE, 2019, pp. 1–8.

[15] Z. C. Liu, L. Xiong, T. Peng, D.-Y. Peng, and H.-B. Liang, "A realistic distributed conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Access*, vol. 6, pp. 26 307–26 317, 2018.

[16] Y. Ming and H. Cheng, "Efficient certificateless conditional privacy-preserving authentication scheme in vanets," *Mobile Information Systems*, vol. 2019, 2019.

[17] S. O. Ogundoyin, "An autonomous lightweight conditional privacy-preserving authentication scheme with provable security for vehicular ad-hoc networks," *International Journal of Computers Applications*, vol. 42, no. 2, pp. 196–211, 2020.

[18] J. Shen, D. Liu, X. Chen, J. Li, N. Kumar, and P. Vijayakumar, "Secure real-time traffic data aggregation with batch verification for vehicular cloud in vanets," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 1, pp. 807–817, 2019.

[19] G. Thumbur, G. S. Rao, P. V. Reddy, N. Gayathri, D. K. Reddy, and M. Padmavathamma, "Efficient and secure certificateless aggregate signature-based authentication scheme for vehicular ad hoc networks," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1908–1920, 2020.

[20] G. K. Verma, B. Singh, N. Kumar, M. S. Obaidat, D. He, and H. Singh, "An efficient and provable certificate-based proxy signature scheme for iiot environment," *Information Sciences*, vol. 518, pp. 142–156, 2020.

[21] L. Wang, D. Zheng, R. Guo, C. Hu, and C. Jing, "A blockchain-based privacy-preserving authentication scheme with anonymous identity in vehicular networks," *International Journal of Network Security*, vol. 22, no. 6, pp. 981–990, 2020.

[22] Y. Wang, H. Zhong, Y. Xu, J. Cui, and G. Wu, "Enhanced security identity-based privacy-preserving authentication scheme supporting revocation for vanets," *IEEE Systems Journal*, vol. 14, no. 4, pp. 5373–5383, 2020.

[23] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. Rodrigues, "Authentication in cloud-driven iot-based big data environment: Survey and outlook," *Journal of systems architecture*, vol. 97, pp. 185–196, 2019.

[24] Z. Wei, J. Li, X. Wang, and C.-Z. Gao, "A lightweight privacy-preserving protocol for vanets based on secure outsourcing computing," *IEEE Access*, vol. 7, pp. 62 785–62 793, 2019.

[25] F. Wu, X. Zhang, C. Zhang, X. Chen, W. Fan, and Y. Liu, "Batch-assisted verification scheme for reducing message verification delay of the vehicular ad hoc networks," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8144–8156, 2020.

[26] H. Xiong, Y. Bao, X. Nie, and Y. I. Asoor, "Server-aided attribute-based signature supporting expressive access structures for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 1013–1023, 2020.

[27] Z. Xu, D. He, N. Kumar, and K.-K. R. Choo, "Efficient certificateless aggregate signature scheme for performing secure routing in vanets," *Security and Communication Networks*, vol. 2020, 2020.

[28] M. B. Younes, "Secure traffic efficiency control protocol for downtown vehicular networks," *International Journal of Network Security*, vol. 21, no. 3, pp. 511–521, 2019.

Biography

Peng-shou Xie was born in Jan. 1972. He is a professor and a supervisor of master student at Lanzhou University of Technology. His major research field is Security on Internet of Things.E-mail: xiepsh_lut@163.com .

Xiao-jie Pan was born in Feb. 1996. He is a master student at Lanzhou University of Technology.His major research field is network and information security. E-mail:1075224210 @qq.com.

Hong Wang was born in Oct. 1997. He is a master student at Lanzhou University of Technology. His major research field is network and information security. E-mail: 2967589625 @ qq.com.

Jia-lu Wang was born in Feb. 1997. He is a master student at Lanzhou University of Technology. His major research field is network and information security. E-mail: 1126334429 @ qq.com.

Tao Feng was born in Dec. 1970. He is a professor and a supervisor of Doctoral student at Lanzhou University of Technology. His major research field is modern cryptography theory, network and information security technology. E-mail: fengt@lut.cn .

Yan Yan was born in Oct.1980. She is a associate professor and a supervisor of master student at Lanzhou University of Technology.Her major research field is privacy protection.E-mail:yanyan@lut.cn .