sensors

MDPI

Article

# PCPA: A Practical Certificateless Conditional Privacy Preserving Authentication Scheme for Vehicular Ad Hoc Networks

**Yang Ming [1,*] and Xiaoqin Shen [2]**

[1] School of Information Engineering, Chang'an University, Xi'an 710064, China
[2] School of Sciences, Xi'an University of Technology, Xi'an 710054, China; xqshen@xaut.edu.cn
* Correspondence: yangming@chd.edu.cn; Tel.: + 86-136-091-16306

Received: 16 April 2018; Accepted: 12 May 2018; Published: 15 May 2018

**Abstract:** Vehicle ad hoc networks (VANETs) is a promising network scenario for greatly improving traffic efficiency and safety, in which smart vehicles can communicate with other vehicles or roadside units. For the availability of VANETs, it is very important to deal with the security and privacy problems for VANETs. In this paper, based on certificateless cryptography and elliptic curve cryptography, we present a certificateless signature with message recovery (CLS-MR), which we believe are of independent interest. Then, a practical certificateless conditional privacy preserving authentication (PCPA) scheme is proposed by incorporating the proposed CLS-MR scheme. Furthermore, the security analysis shows that PCPA satisfies all security and privacy requirements. The evaluation results indicate that PCPA achieves low computation and communication costs because there is no need to use the bilinear pairing and map-to-point hash operations. Moreover, extensive simulations show that PCPA is feasible and achieves prominent performances in terms of message delay and message loss ratio, and thus is more suitable for the deployment and adoption of VANETs.

**Keywords:** vehicular ad hoc networks; authentication; conditional privacy preserving; security; certificateless signature

## 1. Introduction

With the progress in human civilization and development of industrial technology, vehicles are widely popularized in modern society, which leads to such problems as traffic congestion, accidents, vehicle emissions, etc. Therefore, wide attention has been paid to deal with the abovementioned issues in both the academia and automobile industry.

Vehicular ad hoc networks (VANETs), as a key component of intelligent transport system (ITS) and a particular mobile ad hoc networks (MANETs), is promising in improving traffic management efficiency and road traffic safety [1] . Generally, a typical VANET is mainly comprised of three types of entities, i.e., the trusted authorizers (TAs), the roadside units (RSUs) installed along the roads, and the vehicles rigged with onbroad units (OBUs). The TAs maintain the whole system and communicate with the RSUs using a secure wired communication. The RSUs alleviate the burden of the TAs by performing authentication tasks, while the vehicles (OBUs) provided the wireless communication capability, which communicate with the RSUs (Vehicle-to-Infrastructure, V2I) communication and other vehicles (Vehicle-to-Vehicle, V2V) communication. Here, IEEE 802.11 p standard is used for wireless communication based on Dedicated Short Range Communication (DSRC) protocol [2,3], in which each vehicle (OBU) broadcasts the traffic-related messages (e.g., vehicle's speed, position, turning direction and time) periodically every 300 ms. According to the received traffic-related messages, other vehicles can alter driving routes to avoid emergent braking or traffic accidents, and

the RSU will inform the traffic control center to regulate the traffic for preventing potential traffic jams. Based on the hybrid architecture of V2I and V2V communication, VANETs are conducive to enhancing traffic safety, improving traffic management and optimizing traffic efficiency.

Owing to the inherent broadcast nature of the wireless channels, the communication in VANETs is vulnerable to various attacks such as eavesdropping, replaying, tampering, modification and forgery attacks, etc. Therefore, for the widespread deployment of VANETs, the security and privacy challenges must be solved [4,5].

The authentication mechanism, which consists of identity authentication and message integrity, is the key to ensuring the security of VANETs [1,5,6]. If identity authentication is not satisfied, a malicious vehicle may impersonate as a legal vehicle to broadcast messages for obtaining illegal benefits. If message integrity is not ensured, a malicious vehicle may broadcast falsified or altered messages to seriously disrupt traffic or incur serious consequences for the surrounding vehicles without being caught. Thus, authentication has to be implemented to verify a vehicle's identity and to differentiate trustworthy messages from received ones. The digital signature technology may be used to address this problem in VANETs, the vehicle should make a signature on messages before sending them out, and the receivers will authenticate the messages before employment.

Apart from that, privacy is also important for VANETs [7,8]. The vehicle's privacy information like current position, license number, driver's identity and travel route must be kept confidential for a long time. For example, the leakage of vehicle's route information will incur the grave consequences since the information may be used for crimes or traffic accident. In general, the vehicles wouldn't want their privacy information disclosed in broadcasting messages. Therefore, the vehicle privacy must be protected.

However, the fact is that security sometimes conflicts with privacy. Especially, the former often involves some identity information and message's origin, while the latter requires that no entity can trace a message to its generator. Thus, conditional privacy is usually considered in VANETs. That being said, the vehicle's privacy is usually preserved in the system. If a malicious vehicle does not perform the protocol correctly (e.g., broadcasting false messages), then its privacy is revoked, in which case a trust authority (TA) will be capable to trace or retrieve the real identity of vehicle. The conditional privacy-preserving authentication (CPPA) mechanism [9,10], which is able to achieve message authentication and conditional privacy preservation simultaneously, is fully appropriate for addressing the security and privacy issues in VANETs.

Lots of existing studies on the CPPA schemes in VANETs have been carried out in recent years. We can broadly categorize these schemes into public key infrastructure-based (PKI-based) schemes [1], identity-based (ID-based) schemes [11], and certificateless schemes [12–15].

Despite having solved the key escrow problem in ID-based schemes and the public key certification management problem in PKI-based schemes, the certificateless schemes are still unsuitable for the VANETs. The reason is that such schemes [12–15] have poor performances due to the requirements of map-to-point hash and bilinear pairing operations. Compared to other cryptographic operations, these two operations are complex and time-consuming. Therefore, it is important to design a practical certificateless CPPA scheme for VANETs without using bilinear pairing and map-to-point hash operations.

### 1.1. Our Contributions

This paper proposes a practical certificateless conditional privacy preserving authentication (PCPA) scheme for VANETs. To summarize, the major contributions of this paper are as follows:

- A certificateless signature with message recovery (CLS-MR), which is proved to be secure under the assumption of elliptic curve discrete logarithm (ECDL) in the random oracle, is proposed based on certificateless cryptography [16] and elliptic curve cryptography (ECC) [17,18]. This is of independent interest.

- A practical certificateless conditional privacy preserving authentication (PCPA) scheme for VANETs is proposed based on CLS-MR. The security analysis and comparison indicate that PCPA satisfies all security and privacy requirements.
- The performance in computation and communication cost is evaluated through quantitative calculations. Experimental results depict that PCPA is more efficient than other schemes in [12–15].
- An extensive simulation is performed and the results display that PCPA is more feasible and achieves the low average message delay and message loss ratio.

### 1.2. Organization

Organization of this paper is demonstrated as follows: in Section 2, we survey the related work about CPPA in VANETs. In Section 3, the preliminaries are introduced. We present the concrete PCPA scheme for V2I communication in Section 4. Section 5 analyzes the security of the proposed scheme. Section 6 conducts the performance evaluations and experimental simulation results. Finally, Section 7 concludes the paper.

## 2. Related Works

A lot of researchers have put great efforts on authentication schemes aimed to achieve security, privacy and efficiency. These schemes are roughly classified into three categories: PKI-based authentication schemes, ID-based authentication schemes, and certificateless authentication schemes.

In the first category, the anonymous certificates are used to hidden the vehicle's real identities. In 2004, Hubaux et al. [4] claimed that the PKI technology could be used to address the security and privacy preserving problems in VANETs. In 2007, Raya and Hubaux [1], based on PKI and anonymous certificates, put forward an anonymous authentication scheme for VANETs. In this scheme, each vehicle needs to preload lots of anonymous public/private key pairs and the corresponding public key certificates. In this case, the vehicles need a large storage spaces and a huge verification overhead. Furthermore, a trusted authority (TA) will generate a large certificate revocation list (CRL), making the revocation mechanism very inefficient. In 2008, Lu et al. [10] constructed an efficient conditional privacy preserving (ECPP) mechanism for VANETs, to solve the storage space problem and the CRL growth problem in [11]. Zhang et al. [19] proposed a message authentication scheme based k-anonymity approach and hash message authentication code to achieve the privacy preserving of the vehicles and low communication cost. However, all the PKI-based authentication schemes for VANETs have a bottleneck problem on the management and storage of certificates.

ID-based authentication schemes for VANETs have been proposed so as to solve the problems mentioned above. Incorporating the ID-based cryptography [20], Zhang et al. [11,21] proposed ID-based CPPA schemes supporting batch verification based on bilinear pairing for VANETs. In these schemes, the RSU and the vehicle utilize the pseudo-identity information as the public keys, while the private keys are generated by a trusted third party, namely, the private key generator (PKG). Thus, these schemes avoid the requirements of certificate storage in the entities, and alleviate the certificate management of PKI. Furthermore, the schemes achieve low verification cost because of batch message verification, which allows a large number of messages to be verified simultaneously. In 2009, based on binary authentication tree, an ID-based authentication scheme for V2I communication is proposed by Jiang et al. [22]. This scheme meets the security and privacy requirements, and achieves high efficiency in VANETs. In 2011, Chim et al. [23] pointed out that the schemes proposed in [11,21] were insecure against impersonation and anti-traceability attacks, then constructed a secure communication scheme for VANETs. Based on bilinear pairing, Huang et al. [24] presented a new authentication scheme for VANETs that not only is efficient in performances, but also provides conditional privacy to the vehicles. Based on the pseudo-identity-based signature, Shim [25] proposed an ID-based CPPA scheme for VANETs. In 2013, Shim [26] and Li et al. [27] pointed out that the schemes in [11,22] were insecure against the security attacks, and then established the improved ID-based authentication schemes. Horng et al. [28] showed that scheme in [23] is not secure against

impersonation attack and proposed a secure scheme to make up for the security flaw in [23]. In 2014, Zhang et al. [29], aiming at the weakness mentioned in [27], constructed an improved ID-based CPPA scheme for VANETs. Liu et al. [30] indicated that the underlying ID-based signature scheme in [25] was unable to reach an acceptable security level, and thus the corresponding Coron's technique authentication scheme suffers from a modification attack. In 2015, Bayat et al. [31] further pointed out the security flaws in [27] and designed a new scheme. Based on bilinear pairing, ID-based authentication schemes [32–36] were proposed, which are capable of guaranteeing the security and privacy requirements in VANETs. However, the performance of such schemes is not satisfactory because bilinear pairing operations should be used to implement authentication in VANETs. Based on the ECC, efficient ID-based authentication schemes for VANETs were proposed in [37–43], where bilinear pairing operations and map-to-hash operations are not applied. They achieve high efficiency in terms of computation and communication cost. Although ID-based authentication schemes eliminate the certificates, simplify the key management and reduce the storage overhead, they are confronted with the inherent key escrow challenge. That is to say, PKG has the knowledge on the private keys of all vehicles and RSUs. It appears that this condition may be excessively strong and not appropriate for VANETs.

To solve the key escrow problem in ID-based authentication schemes, certificateless authentication schemes have been proposed for VANETs. Horng et al. [12], based on certificateless cryptography [16], put forward a secure certificateless CPPA scheme. In this scheme, only the partial private key of the users (RSU and Vehicle) is generated by a trusted party, namely, the Key Generator Center (KGC). A secret value is picked by the user itself, and combines the partial private key to form the private key. Therefore, the KGC has no the private key s of all users. Moreover, in the certificateless CPPA scheme, public key certificates are not needed to guarantee the authenticity of public keys. In 2016, Li et al. [13] found that the scheme in [12] was not secure against a malicious-but-passive KGC under the existing security model. In other words, KGC may maliciously implant a trapdoor in the public system parameters and attempts to forge a signature without the vehicle's private key. Based on bilinear pairing, an efficient certificateless aggregate signature scheme for VANETs was put forward by Malhi et al. [14], which achieves low computation cost s in verification phase. In 2018, Kumar et al. [15] demonstrated that the scheme in [14] was vulnerable to malicious KGC attack and proposed an improved scheme for VANETs, which was able to eliminate the security flaws of scheme in [14] and achieved the same performances.

Upon reviewing the literature, the aforementioned schemes have different problems. The PKI-based schemes suffer from the high cost of certificate management on CA, in which the vehicles could easily disrupt the service of VANETs. As for ID-based schemes, a key escrow problem is inevitable and incurs the security of VANETs. Until now, the existing certificateless schemes solve the above problems in PKI-based and ID-based schemes but are still not efficient and suitable to VANETs because of the huge computation overhead and communication cost.

The proposed scheme had addressed the aforementioned issues simultaneously based on the ECC. It neither requires the certificate management, nor the involves key escrow problem. Moreover, the proposed scheme does not use bilinear pairing and map-to-point hash operations, which achieves outstanding performances and is more suitable for VANETs than other schemes.

## 3. Preliminaries

The elliptic curves and related problem, system model, security requirement and cryptographic primitive used as building blocks are introduced in this section. For readability, the notations adopted in the present paper are listed in Table 1.

**Table 1.** Notations.

| Symbol | Description |
|---|---|
| $p, q$ | two large prime numbers |
| $F_p$ | a finite field over $p$ |
| $\mathbb{G}$ | an additive group |
| $P$ | a generator of $\mathbb{G}$ |
| KGC | a key generation center |
| $(P_{pub}, s)$ | KGC's public key and private key |
| $H_1(\cdot), H_2(\cdot), H_3(\cdot), H_4(\cdot)$ | hash functions: $H_1, H_2, H_3, H_4 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, |
| $F_1(\cdot), F_2(\cdot)$ | $F_1 : \{0,1\}^{l_2} \rightarrow \{0,1\}^{l_1}$, $F_2 : \{0,1\}^{l_1} \rightarrow \{0,1\}^{l_2}$, $l_1 + l_2 = \|q\|$ |
| $V_i$ | the $i$-th vehicle |
| RSU | roadside unit |
| OBU | onboard unit |
| TRA | a trace authority |
| $(T_{pub}, t)$ | TRA's public key and private key |
| $RID_i$ | $V_i$'s real identity |
| $PID_i$ | $V_i$'s pseudo identity |
| $PK_i$ | $V_i$'s public key |
| $R_i, d_i$ | $V_i$'s partial private key |
| $x_i$ | $V_i$'s secret value |
| $T_i$ | the valid period of $PID_i$ |
| $\oplus$ | OR operation |
| $ct_i$ | current timestamp |
| $M_i$ | a message sent from vehicle to RSU |
| $P_i$ | $V_i$'s public key in [12–14] |
| $(R_i, S_i)$ | a signature on $M_i$ in [12,13] |
| $(U_i, V_{ijk})$ | a signature on $M_i$ in [14] |

### 3.1. Elliptic Curves

Miller [17] and Koblitz [18] first proposed the concept of elliptic curve cryptography (ECC).

Let $F_p$ be a finite field with a large prime $p$. The elliptic curve $E$ over $F_p$ is defined as the set of an infinity point $O$ and all points $P = (x, y)$ that meet the equation $y^2 = x^3 + ax + b \,(\mathrm{mod}\, p)$, where the discriminant $\Delta = 4a^3 + 27b^2 \neq 0$ and $a, b \in F_p$. The elliptic curve $E$ forms an additive cyclic group $\mathbb{G}$ under the operation of point addition $P + Q = R$. Scalar multiplication operation over $F_p$ is expressed as $kP = P + P + \cdots + P$ $(k\ times)$. The hard problems based on ECC are shown as follows:

- Elliptic curve discrete logarithm (ECDL) problem: Given two random points $P, Z = yP \in \mathbb{G}$, find an integer $x$, such that $Z = xP$.
- Elliptic curve discrete logarithm (ECDL) assumption problem: There are no polynomial-time algorithms to solve the ECDL problem with non-negligible probability.
- Elliptic curve computational Differ-Hellman (ECCDH) problem: For unknown $x, y$ integers and the given two random points $R = xP, Z = yP \in \mathbb{G}$, calculate the point $xyP$ .
- Elliptic curve computational Differ-Hellman (ECCDH) assumption: There are no polynomial-time algorithms to solve the ECCDH problem with non-negligible probability.

### 3.2. System Model

The system model of the proposed scheme is shown in Figure 1. As is shown in Figure 1, the system is composed of five entities: the Key Generator Center (KGC), the Trace Authority (TRA), the Application Servers (AS), the RSU, and the OBU.

KGC: It is in charge of calculating system parameters and preloading them on RSUs and OBUs in offline mode. In addition, it also produces and distributes the partial private keys for RSUs and OBUs. The KGC is assumed to be a trusted third party with sufficient storage space and computing power.

TRA: It is used for the registration of RSUs and OBUs. It can trace messages to their source and disclose the vehicles' real identity. Similarly, the TRA is assumed to be a trusted third party with sufficient storage space and computing power.

AS: It is a safety-related application server, like a traffic-data analysis center or traffic manage center. It first gathers the traffic-related messages including current location, time, traffic accidents from RSUs, and then conducts further analysis and/or provides feedback to them. The AS communicates with KGC, TRA and RSUs via the wired channel.

RSU: It is located along the roadside and is used for verifying the authenticity and integrity of messages and processing them locally or forwarding them to TAs or AS when received the messages from OBUs. The RSU communicates with the vehicle in a certain coverage region by a wireless channel and communicates with KGC, TRA and AS via a secure wired channel.

OBU: It is installed on the vehicle to communicate with other vehicles and RSUs for sharing traffic-related status information like speed, direction, and position through the Dedicated Short Range Communication (DSRC) [2,3]. Generally, the OBU is assumed to have less computation power than RSU.

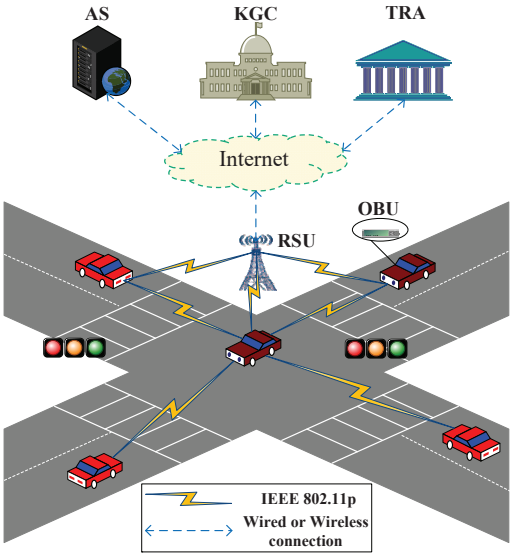


**Figure 1.** System model.

### *3.3. Security Requirements*

In V2I communication, the following security requirements need to be satisfied in the proposed scheme.

**Authentication and message integrity**: The message receiver (RSU) should be able to verify the legality of the vehicle efficiently in the system and detect any modification of the received message.

**Identity privacy preserving**: Any entity should not identify or trace the vehicle's real identity by analyzing the received messages.

**Traceability**: The generator of any mistake message should be traceable. TRA should be able to disclose the real identity of any malicious vehicle, which has broadcasted forged messages to other vehicles in order to disrupt the traffic.

**Unlinkability**: Apart from TRA, neither should the RSU nor the malicious vehicle be able to determine whether two messages are from the same vehicle.

**Key escrow resilience**: KGC, a semi-trusted party, should not impersonate legitimate vehicle to generate a valid signature using the vehicle's private key.

**Role separation**: Two trusted authorities exist in the proposed scheme, i.e., KGC and TRA. KGC is working for creating the vehicle's partial private key on the pseudo identity. TRA is responsible for producing the pseudo identities and tracing the vehicle's real identity.

**Resistance to attack**: The proposed scheme should resist various of popular attacks such as the replay attack, the modification attack, the impersonation attack, and the man-in-the-middle attack in VANETs.

### *3.4. CLS-MR*

The CLS-MR includes the following algorithms: setup, partial-private-key-extract, set-secret-value, set-private-key, set-public-key, sign, and verify.

- **Setup**: Given a security parameter $k$, the KGC generates a group $\mathbb{G}$ of the prime order $q$ based on an elliptic curve $E$ defined over a finite field $F_p$, where $P \in \mathbb{G}$ is a generator. The KGC randomly chooses $s \in \mathbb{Z}_q^*$ and computes $P_{pub} = sP$. The KGC also chooses hash functions $H_1, H_2, H_3 : \{0,1\}^* \rightarrow Z_q^*$, $F_1 : \{0,1\}^{l_2} \rightarrow \{0,1\}^{l_1}$ and $F_2 : \{0,1\}^{l_1} \rightarrow \{0,1\}^{l_2}$, where $l_1$ and $l_1$ are positive integers such that $l_1 + l_2 = |q|$. The system parameter is $params = \{F_p, \mathbb{G}, q, P, P_{pub}, H_1, H_2, H_3, F_1, F_2, l_1, l_2\}$ and the master key is $s$ .
- **Partial-Private-Key-Extract**: Given $params$ and an identity $ID_i$, the KGC chooses at random $r_i \in \mathbb{Z}_q^*$ and computes

  – $R_i = r_i P$,
  – $h_{1i} = H_1(ID_i, R_i)$,
  – $d_i = r_i + h_{1i} s$.

  The partial private key for $ID_i$ is $PPK_i = \{R_i, d_i\}$. The KGC securely returns $PPK_i$ to the user.
- **Set-Secret-Value**: The user $ID_i$ picks a random number $x_i \in \mathbb{Z}_q^*$ as its secret value.
- **Set-Private-Key**: The private key of user $ID_i$ is $SK_i = \{d_i, x_i\}$.
- **Set-Public-Key**: Given $params$ and the user's secret value $x_i$, the user $ID_i$ computes $P_i = x_i P$ and sets $PK_i = \{R_i, P_i\}$ as its public key.
- **Sign**: Given $params$, private key $\{d_i, x_i\}$ for the user $ID_i$ under $\{R_i, P_i\}$ and a message $m \in \{0,1\}^{l_2}$, the user $ID_i$ picks a random number $t_i \in \mathbb{Z}_q^*$ and computes

  – $f = F_1(m) || F_2(F_1(m)) \oplus m$,
  – $u_i = f \oplus (t_i P)$,
  – $h_{2i} = H_2(ID_i, P_{pub}, P_i)$,
  – $h_{3i} = H_3(ID_i, P_{pub}, R_i, u_i)$,
  – $v_i = t_i + h_{2i} x_i + h_{3i} d_i$.

  Finally, the signature on $m$ for $ID_i$ is $\sigma_i = \{u_i, v_i\}$.
- **Verify**: Given $params$ , the public key $\{R_i, P_i\}$, the user's identity $ID_i$ and the signature $\sigma_i$, any verifier recovers the message and checks the validity of signature. To recover message $m$, the verifier computes

  – $h_{1i} = H_1(R_i, ID_i)$,
  – $h_{2i} = H_2(ID_i, P_{pub}, P_i)$,
  – $h_{3i} = H_3(ID_i, P_{pub}, R_i, u_i)$,
  – $f = u_i \oplus (v_i P - h_{2i} P_i - h_{3i} R_i - h_{3i} h_{1i} P_{pub})$,
  – $m = [f]_{l_2} \oplus F_2({}_{l_1}[f])$ where $\oplus$ is exclusive or operation, ${}_{l_1}[f]$ and $[f]_{l_2}$ are the most significant $l_1$-bit of $f$ and the least significant $l_2$-bit of $f$, respectively.

  **Correctness**:

  Given a signature $\sigma_i = \{u_i, v_i\}$ for $ID_i$ under $\{R_i, P_i\}$, compute $h_{1i} = H_1(ID_i, R_i)$, $h_{2i} = H_2(ID_i, P_{pub}, P_i)$, $h_{3i} = H_3(ID_i, P_{pub}, R_i, u_i)$, and

$$\begin{aligned} & u_i \oplus (v_i P - h_{2i} P_i - h_{3i} R_i - h_{3i} h_{1i} P_{pub}) \\ &= [f \oplus (t_i P)] \oplus [(t_i + h_{2i} x_i + h_{3i} d_i) P - h_{2i} P_i - h_{3i} R_i - h_{3i} h_{1i} P_{pub}] \\ &= [f \oplus (t_i P)] \oplus [t_i P + h_{2i}(x_i P) + h_{3i}(r_i + h_{1i} s) P - h_{2i} P_i - h_{3i} R_i - h_{3i} h_{1i} P_{pub}] \\ &= f. \end{aligned}$$

Then, one can recover

$$\begin{aligned} m &= [f]_{l_2} \oplus F_2({}_{l_1}[f]) \\ &= [F_1(m) || F_2(F_1(m)) \oplus m]_{l_2} \oplus F_2({}_{l_1}[F_1(m) || F_2(F_1(m)) \oplus m]) \\ &= F_2(F_1(m)) \oplus m \oplus F_2(F_1(m)) \\ &= m. \end{aligned}$$

### *3.5. Security Proof*

According to certificateless cryptography [16], two types of adversaries, i.e., Type I adversary $A_1$ and Type II adversary $A_2$, are considered in CLS-MR. The adversary $A_1$ models an outside adversary and acts as a malicious third party while the adversary $A_2$ models an inside adversary and serves as a malicious-but-passive KGC.

- **Type I adversary** $A_1$: The adversary $A_1$ is not in possession of the master key, but is capable of replacing the public key of the user with a value chosen by itself.
- **Type II adversary** $A_2$: The adversary $A_2$ is in possession of the master key, but cannot replace the public key of the user.

The formal security model of CLS-RM is depicted in detail in [16].

**Theorem 1.** *The proposed CLS-MR is existentially unforgeable under the ECDL assumption in the random oracle model.*

**Proof.** Theorem 1 is proved according to Lemma 1 and Lemma 2 listed below. □

**Lemma 1.** *In the random oracle model, CLS-MR is existential unforgeable against Type I adversary $A_1$ under the ECDL assumption.*

**Lemma 2.** *In the random oracle model, CLS-MR is existential unforgeable against Type II adversary $A_2$ under the ECDL assumption.*

The security proof of Lemma 1 and Lemma 2 can be found in the appendix.

## 4. The Proposed Scheme

This section proposes a practical certificateless conditional privacy-preserving authentication (PCPA) scheme for VANETs based on CLS-MR. Specifically, the proposed scheme includes system initialization, pseudo identity generation and partial private key extraction, public/private key generation and message signing, and message verification phases.

### *4.1. System Initialization*

The system initialization, which is carried out by TAs (KGC and TRA), is to produce system parameters for all RSUs and OBUs. The following steps are performed in this phase:

(1) The TAs randomly choose a prime p, an elliptic curve $E$ over the finite field $F_p$, which is defined by the equation $y^2 = x^3 + ax + b \bmod p$, where $4a^3 + 27b^2 \neq 0$ and $a, b \in F_p$ .
(2) The TAs pick a group $\mathbb{G}$ of prime order $q$ based on $E$ and denote $P \in \mathbb{G}$ a generator.

(3) The KGC calculates its public key $P_{pub} = sP$, where $s \in \mathbb{Z}_q^*$ is the master key for partial private key generation.

(4) The TRA chooses a random number $t \in \mathbb{Z}_q^*$ as the master key for identity traceability and computes $T_{pub} = tP$ .

(5) The TAs choose hash functions: $H : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $H_3 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $F_1 : \{0,1\}^{l_2} \rightarrow \{0,1\}^{l_1}$ and $F_2 : \{0,1\}^{l_1} \rightarrow \{0,1\}^{l_2}$, where $l_1$ and $l_1$ are positive integers such that $l_1 + l_2 = |q|$.

The TAs publish the system parameters $\{p, q, \mathbb{G}, P, P_{pub}, T_{pub}, H, H_1, H_2, H_3, F_1, F_2\}$ and send them to all RSUs and vehicles (OBUs). Here, the system parameters are preloaded into the all vehicles' tamper-proof devices (TPD) for VANETs. The master keys $s$ and $t$ are kept secretly by KGC and TRA, respectively.

### *4.2. Pseudo Identity Generation and Partial Private Key Extraction*

This phase is performed between the TAs (TRA and KGC) and the vehicles. Receiving the real identity $RID_i$ from $V_i$, where $RID_i$ uniquely identifies the vehicle $V_i$, the KGC calculates partial private keys on them after the TRA generates pseudo identities for the vehicle $V_i$. Then, the partial private keys and pseudo identities are preloaded in TPD of vehicle $V_i$. The details of this phase are as follows:

(1) The vehicle $V_i$ sends the real identity $RID_i$ to the TRA in secure mode.

(2) Upon receiving the real identity $RID_i$, the TRA randomly chooses $w_i \in \mathbb{Z}_q^*$ and computes

- $PID_{i,1} = w_i P$,
- $PID_{i,2} = RID_i \oplus H(w_i T_{pub}, T_i)$, where $T_i$ defines the valid period of the pseudo identity $PID_i$.

Then, a pseudo identity $PID_i = \{PID_{i,1}, PID_{i,2}, T_i\}$ is transmitted to the KGC via a secure way.

(3) When receiving the pseudo identity $PID_i = \{PID_{i,1}, PID_{i,2}, T_i\}$, the KGC randomly chooses $r_i \in \mathbb{Z}_q^*$ and calculates the partial private key $PPK_i = \{R_i, d_i\}$ using the master key $s$ where

- $R_i = r_i P$,
- $d_i = r_i + sH_1(PID_i, R_i, P_{pub}, T_{pub})$.

(4) After that, the KGC sends the partial private key and pseudo identity $\{PPK_i, PID_i\}$ to the vehicle $V_i$.

### *4.3. Public/Private Key Generation and Message Signing*

During this phase, the vehicle $V_i$ generates public/private key and signs messages. Then, the vehicle $V_i$ broadcasts a final message, including the pseudo identity, public key, timestamp, and signature, to nearby RSUs. The details of this phase are as follows:

(1) The vehicle $V_i$ randomly picks $x_i \in \mathbb{Z}_q^*$ as the secret value and computes $P_i = x_i P$. Then, the vehicle $V_i$'s private key is $SK_i = \{d_i, x_i\}$ and the public key is $PK_i = \{R_i, P_i\}$.

(2) The vehicle $V_i$ randomly chooses a pseudo identity $PID_i$ from its storage and a current timestamp $ct_i$, which is used to ensure the freshness of message so as to resist the replay attack. Given a traffic-related message $m_i \in \{0,1\}^{l_2}$, the vehicle $V_i$ randomly picks $t_i \in \mathbb{Z}_q^*$, and calculates

- $f = F_1(m_i)||F_2(F_1(m_i)) \oplus m_i$,
- $u_i = f \oplus (t_i P)$,
- $h_{2i} = H_2(PID_i, P_{pub}, T_{pub}, P_i, ct_i)$,
- $h_{3i} = H_3(PID_i, P_{pub}, T_{pub}, R_i, u_i, ct_i)$,
- $v_i = t_i + h_{2i} x_i + h_{3i} d_i$.

The signature of a traffic-related message $m_i$ is $\{u_i, v_i\}$. Then, the vehicle $V_i$ broadcasts the final message $M_i = \{PID_i, PK_i, ct_i, u_i, v_i\}$ to nearby RSUs.

### *4.4. Message Verification*

In this phase, after receiving the final message $\{PID_i, PK_i, ct_i, u_i, v_i\}$, the verifier (RSU) recovers the messages and checks the validity of the signature. Based on this, it is a guarantee that the corresponding vehicle cannot broadcast false messages or masquerading as other legal vehicles. This phase is described as follows:

(1) The verifier checks whether $T_i$ is valid and $ct_i$ is fresh. If $T_i$ is not valid or $ct_i$ is not fresh, the message will be rejected.

(2) The verifier computes

- $h_{1i} = H_1(PID_i, R_i, T_{pub}, P_{pub})$,
- $h_{2i} = H_2(PID_i, P_{pub}, T_{pub}, P_i, ct_i)$,
- $h_{3i} = H_3(PID_i, P_{pub}, T_{pub}, R_i, u_i, ct_i)$,
- $f_i = u_i \oplus (v_i P - h_{2i} P_i - h_{3i} R_i - h_{3i} h_{1i} P_{pub})$,
- $m_i = [f_i]_{l_2} \oplus F_2({}_{l_1}[f_i])$.

(3) Checks whether ${}_{l_1}[f_i] = F_1(m_i)$.

## 5. Security Analysis

In this section, an analysis on the security of the proposed scheme as well as its comparison with the latest schemes is conducted.

**Authentication and message integrity**: To ensure the authentication and message integrity, a new CLS-MR scheme is employed in the proposed PCPA. According to Theorem 1, the underlying CLS-MR is secure against adaptive chosen message and identity attacks under the ECDL assumption in the random oracle model. Through a Message Verification algorithm, a verifier (RSU) can confirm the validity and integrity of $\{PID_i, PK_i, ct_i, u_i, v_i\}$. That is to say, any polynomial-time adversary is unable to forge or modify a valid signature. Therefore, the message integrity and authentication can be ensured in the proposed scheme.

**Identity privacy preserving**: According to the description of the proposed scheme, the real identity $RID_i$ of the vehicle $V_i$ is only included in random pseudo identity $PID_i = \{PID_{i1}, PID_{i2}, T_i\}$, where $PID_{i1} = w_i P$, $PID_{i,2} = RID_i \oplus H(w_i T_{pub}, T_i)$ and $T_{pub} = tP$. To extract the vehicle $V_i$'s real identity $RID_i$, the adversary has to compute $RID_i = PID_{i,2} \oplus H_1(w_i T_{pub}, T_i) = PID_{i,2} \oplus H_1(w_i \cdot t \cdot P, T_i)$. However, without knowing $w_i$ and $t$, it is impossible for any adversary to obtain $RID_i$ as it is an instance of a ECCDH problem to solve $w_i \cdot t \cdot P$. Therefore, the identity privacy preserving can be ensured in the proposed scheme.

**Traceability**: According to the description of the proposed scheme, the TRA can use its own master key $t$ to compute $t \cdot PID_{i1} = t \cdot w_i \cdot P = w_i \cdot t \cdot P = w_i \cdot T_{pub}$ and $RID_i = PID_{i,2} \oplus H_1(w_i T_{pub}, T_i)$. TRA can extract the real identity $RID_i$ from a pseudo identity $PID_i = \{PID_{i,1}, PID_{i,2}, T_i\}$ involved in the broadcast messages. Therefore, the proposed scheme satisfies the traceability.

**Unlinkability**: According to the description of the proposed scheme, the TRA, KGC, and the vehicle randomly choose $w_i \in \mathbb{Z}_q^*$, $r_i \in \mathbb{Z}_q^*$ and $t_i \in \mathbb{Z}_q^*$ respectively, and generates $\{PID_i, PK_i, ct_i, u_i, v_i\}$, where $PID_{i1} = w_i P$, $PID_{i,2} = RID_i \oplus H_1(w_i T_{pub}, T_i)$, $PID_i = \{PID_{i,1}, PID_{i,2}, T_i\}$, $R_i = r_i P$, $d_i = r_i + s H_1(PID_i, R_i, T_{pub}, P_{pub})$, $f = F_1(m) || F_2(F_1(m)) \oplus m$, $u_i = f \oplus (t_i P)$ and $v_i = t_i + x_i H_2(PID_i, P_{pub}, T_{pub}, P_i, ct_i) + d_i H_3(PID_i, P_{pub}, T_{pub}, R_i, u_i, ct_i)$. Due to the randomness of $w_i$, $r_i$ and $t_i$, any adversary is unable to link two messages sent from the same vehicle or two anonymous pseudo identities, through which the unlinkability of the proposed scheme is satisfied.

**Role separation**: According to the description of the proposed scheme, there are two trusted authorities with different functions, i.e., TRA and KGC. The real identity of a vehicle can only be revealed by TRA rather than KGC by using the master key $t$. Here, $t$ have to be well safeguarded for the vehicle's privacy preserving. However, there is no need to give strong protection to the master

key $s$ of KGC, since no adversaries can generate a valid signature without the vehicle's secret value. Therefore, the role separation can be provided in the proposed scheme.

**Key escrow resilience**: According to the Lemma 2, the malicious KGC cannot impersonate a vehicle successfully under the ECDLP assumption. The basic reason is that the vehicle $V_i$ calculates the secret value $x_i$ itself, and it cannot be accessed by the KGC. Therefore, the key escrow resilience is satisfied in the proposed scheme.

**Resistance to attacks**: The proposed scheme is secure against the main attacks of network. The details are as follows:

- **Replay attack**: It can be known from the description of the proposed scheme, the timestamp $ct_i$ is included in $\{PID_i, PK_i, ct_i, u_i, v_i\}$, which ensures the message freshness to guards against the replay attacks. This requires loose synchronization of the clocks, which could be provided by widely used GPS devices.
- **Modification attack**: Following the depiction of the proposed scheme, we realized that $\{u_i, v_i\}$ is a signature of the traffic-related message $m_i$ under $\{PID_i, PK_i, ct_i\}$. Based on the CLS-MR and Theorem 1, any polynomial adversary can not forge a valid signature and RSU can find any modification on $\{PID_i, PK_i, ct_i, u_i, v_i\}$ by the Message Verification algorithm.
- **Impersonation attack**: It can be known from Theorem 1 that no adversary is able to fabricate the legal message $\{PID_i, PK_i, ct_i, u_i, v_i\}$ without the vehicle's private key. By means of the validity checking on the received message, RSU can find the impersonation attack.
- **Man-in-the-middle attack**: As is shown in the analysis on the modification attack, any modification about $\{PID_i, PK_i, ct_i, u_i, v_i\}$ in transmission can be found.

We compare the security of the proposed PCPA scheme for VANETs with that of the schemes put forwarded by Horng et al. [12], Li et al. [13], Malhi et al. [14], and Kumar et al. [15]. Details on the security comparisons between the proposed scheme and the abovementioned schemes are given in Table 2, where ✓ indicates "satisfy" and ✗ refers to "not satisfy".

**Table 2.** Security comparisons.

| Security | [12] | [13] | [14] | [15] | The Proposed Scheme |
|---|---|---|---|---|---|
| Authentication and Message integrity | ✗ | ✓ | ✗ | ✓ | ✓ |
| Identity privacy preserving | ✓ | ✓ | ✓ | ✓ | ✓ |
| Traceability | ✓ | ✓ | ✓ | ✓ | ✓ |
| Unlinkability | ✓ | ✓ | ✓ | ✓ | ✓ |
| Role separation | ✓ | ✓ | ✗ | ✗ | ✓ |
| Key escrow resilience | ✓ | ✓ | ✗ | ✓ | ✓ |
| Resistance to attacks | ✗ | ✓ | ✗ | ✓ | ✓ |

## 6. Performance Evaluation and Simulation

Here, we analyze the computation and communication costs of the proposed PCPA and evaluate its performance with the existing schemes in [12–14]. It should be pointed out that the analysis and comparison of Kumar et al.'s scheme [15] are omitted, as it has only made a small change in the signing phase to fix the security flaw in [14]. Moreover, a comprehensive simulation is carried out using simulation of urban mobility (SUMO) [44] and ns-3.26 simulator [45]. SUMO is a traffic simulation tool that can provide the realistic traffic mobility model and ns-3.26 is used for wireless network simulation. Based on the simulations, we give concrete evaluation on average message delay and average message loss ratio in real scenarios.

### *6.1. Computation Cost*

The computation cost for the message signing and verification in the proposed scheme is analyzed and the results are compared with those obtained from the schemes put forward by Horng et al. [12], Li et al. [13], and Malhi et al. [14].

For the pairing-based schemes [12–14], the symmetric bilinear pairing for the 80-bit security can be defined as follows: $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_T$, where $\mathbb{G}_1$ is an additive group formed by a generator $P$ with the order $q$ on a super singular elliptic curve $E : y^2 = x^3 + x \bmod p$ with embedding degree 2. $q$ is 160-bit Solinas prime number and $p$ is 512-bit prime number, which satisfy $q \cdot 12 \cdot r = p + 1$. For the proposed scheme, the ECC for the same security level can be constructed as follows: $\mathbb{G}$ with order $q$ is an additive group generated by a point $P$ on a non-singular elliptic curve $E : y^2 = x^3 + ax + b \bmod p$, where $p$, $q$ are two 160-bit prime numbers, $a = -3$, and $b$ is a random 160-bit prime number.

The time cost for performing the cryptographic operations is defined below. Let $T_p$ be the time to perform a bilinear pairing operation, $T_{m-bp}$ and $T_{m-ecc}$ be the time to perform a scale multiplication operation in bilinear pairing and ECC, respectively. The time to perform a map-to-point hash function operation is denoted as $T_{mtp}$. Other lightweight operations (point addition, and one-way hash function operation) are not taken into account.

Using the MIRACL Crypto SDK [46], the running time of the above cryptographic operations can be quantified. The experiment is run on Intel Corei5-4590 (Intel Corporation, Santa Clara, CA, USA), 3.3 GHz CPU, 8 gigabytes memory with Windows 7 (Microsoft Corporation, Redmond, WA, USA). The average execution times of those operations are listed in Table 3.

**Table 3.** Execution time of cryptographic operation (in Milliseconds).

| Cryptographic Operation | Execution Time |
|---|---|
| Bilinear pairing $T_p$ | 9.0791 |
| Scalar multiplication in bilinear pairing $T_{m-bp}$ | 3.7770 |
| Scalar multiplication in ECC $T_{m-ecc}$ | 0.8310 |
| Map-to-point hash function in bilinear pairing $T_{mtp}$ | 9.7052 |

Based on the experiment results, the computation costs of Horng et al.'s scheme [12], Li et al.'s scheme [13], Mahli et al.'s scheme [14] and the proposed PCPA are compared and shown in Table 4.

**Table 4.** Comparison of computation cost.

| Scheme | A Message Signing | A Message Verification | $n$ Message Signing | $n$ Message Verification (Batch) |
|---|---|---|---|---|
| Hong et al's scheme [12] | 7.5540 ms | 40.7195 ms | 7.5540$n$ ms | 13.4822$n$ + 27.2373 ms |
| Li et al's scheme [13] | 17.2592 ms | 50.4247 ms | 17.2592$n$ ms | 13.4822$n$ + 36.9425 ms |
| Malhi et al's scheme [14] | 15.1080 ms | 38.5683 ms | 15.1080$n$ ms | 11.3310$n$ + 27.2373 ms |
| The proposed scheme | 0.8310 ms | 3.3240 ms | 0.8310$n$ ms | 3.3240$n$ ms |

For the computation cost of one message signing, Horng et al.'s scheme [12] requires two scalar multiplication operations in bilinear pairing. Therefore, the total signing time is $2T_{m-bp} = 7.5540$ ms. Li et al.'s scheme [13] requires one map-to-point hash operation and two scalar multiplication operations in bilinear pairing. Thus, the total signing time is $T_{mtp} + 2T_{m-bp} = 17.2592$ ms. Malhi et al.'s scheme [14] requires four scalar multiplication operations in bilinear pairing. Thus, the total signing time is $4T_{m-bp} = 15.1080$ ms. The proposed scheme requires one scalar multiplication operation in ECC. Thus, the total signing time is $1T_{m-ecc}$ = 0.8310 ms.

For the computation cost of one message verification, Horng et al.'s scheme [12] requires one map-to-point hash operation, one scalar multiplication operation in bilinear pairing and three bilinear pairing operations. Thus, the total verification time is $T_{mtp}$ + $T_{m-bp}$ + $3T_p$ = 40.7195 ms.

Li et al.'s scheme [13] requires two map-to-point hash operations, one scalar multiplication operation in bilinear pairing and three bilinear pairing operations. Thus, the total verification time is $2T_{mtp} + T_{m-bp} + 3T_p = 50.4247$ ms. Mahli et al.'s scheme [14] requires three scalar multiplication operations in bilinear pairing and three bilinear pairing operations. Thus, the total verification time is $3T_{m-bp} + 3T_p = 38.5683$ ms. The proposed scheme requires four scalar multiplication operations in ECC. Therefore, the total verification time is $4T_{m-ecc} = 3.3240$ ms.

Figure 2 clearly indicates the computation cost for one message and that with an increasing number of messages, respectively. As is shown in Table 4 and Figure 2a, the computation cost of a message signing is 0.8310 ms in the proposed scheme, which decreases by 88.9%, 95.2% and 94.5% compared with those in [12–14], respectively. In terms of the computation overhead of one message verification, the proposed scheme needs 3.3240 ms, which decreases by 91.8%, 93.4% and 91.4% compared with those in [12–14], respectively.

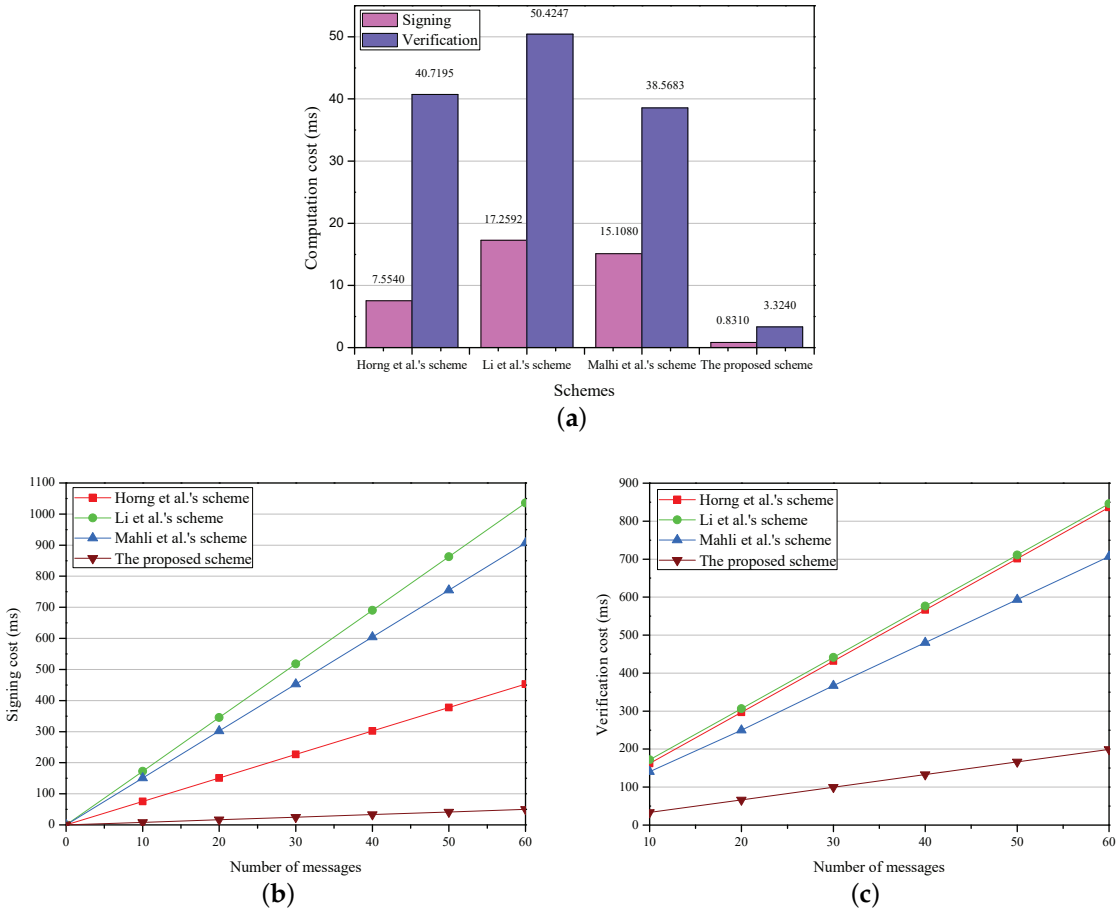


**Figure 2.** Computation cost. (**a**) computation cost in one message signing and verification; (**b**) signing cost versus number of messages; (**c**) verification cost versus number of messages.

To obtain the computation cost of multiple ($n$) messages signing, the computation delay of one message signing should be repeated $n$ times. Therefore, the computation costs of $n$ messages signing in [12–14] and the proposed scheme are $7.5540n$ ms, $17.2592n$ ms, $15.1080n$ ms, and $0.8310n$ ms, respectively.

For computation cost of multiply ($n$) messages verification, Horng et al.'s scheme [12] requires $n$ map-to-point hash operations, $n$ scalar multiplication operations in bilinear pairing and three bilinear pairing operations. Thus, the total verification time is $nT_{mtp} + nT_{m-bp} + 3T_p = 13.4822n + 27.2373$ ms. Li et al.'s scheme [13] requires $(n+1)$ map-to-point hash operations, $n$ scalar multiplication operations in bilinear pairing and three bilinear pairing operations. Thus, the total verification time is

$(n+1)T_{mtp} + nT_{m-bp} + 3T_p = 13.4822n + 36.9425$ ms. Mahli et al.'s scheme [14] requires $3n$ scalar multiplication operations in bilinear pairing and three bilinear pairing operations. Thus, the total verification time is $3nT_{m-bp} + 3T_p = 11.3310n + 27.2373$ ms. The proposed scheme requires $4n$ scalar multiplication operations in ECC. Therefore, the total verification time is $4nT_{m-ecc} = 3.3240n$ ms.

It is known from Figure 2b,c that the signing cost together with verification cost grows linearly with the increase of the number of messages. In addition, the proposed scheme has the lowest slope. As is shown in Figure 2b, when $n = 60$, the signing costs of the schemes in [12–14] and the proposed scheme respectively are 453.2400 ms, 1035.5520 ms, 906.4800 ms, 49.8600 ms. As is shown in Figure 2c, the verification costs of the schemes in [12–14] and the proposed scheme respectively are 162.0593 ms, 171.7645 ms, 140.5473 ms, and 33.2400 ms when $n = 10$, and 836.1693 ms, 845.8745 ms, 707.0973 ms, and 199.4400 ms when $n = 60$.

Therefore, the proposed PCPA achieves lower computation cost than the schemes in [12–14] in the signing and verification phases, regardless of the number of messages.

### 6.2. Communication Cost

In this subsection, the communication costs of Horng et al.'s scheme [12], Li et al.'s scheme [13], Malhi et al.'s scheme [14] and the proposed scheme are evaluated. In V2I communication, the communication cost refers to the size of message transmitted from a vehicle (OBU) to an RSU.

As is mentioned above, the length of $q$ is 160 bits and that of $p$ is 512 bits, so the length of elements in $\mathbb{G}$ and $\mathbb{G}_1$, respectively, are 20 bytes and 64 bytes. Assuming that the output length of general one-way hash function is 160 bits (20 bytes), and the length of the timestamp is 32 bits (4 bytes). According to IEEE Trial-Use standard [47] for VANETs security, the length of the traffic-related message is 67 bytes. The comparison of communication cost is shown in Table 5 and analyzed as follows.

**Table 5.** Comparison of communication cost.

| Scheme | Send a Message | Send $n$ Messages |
|---|---|---|
| Horng er al.'s scheme [12] | 351 bytes | $351n$ bytes |
| Li et al.'s scheme [13] | 351 bytes | $351n$ bytes |
| Malhi et al.'s scheme [14] | 323 bytes | $323n$ bytes |
| **The proposed scheme** | **128 bytes** | **$128n$ bytes** |

In [12,13], $\{M_i, PID_i, P_i, ct_i, R_i, S_i\}$ is sent from the vehicle (OBU) to a RSU, where $PID_i = \{PID_{i,1}, PID_{i,2}, T_i\}$, $PID_{i,1} \in \mathbb{G}_1$, $PID_{i,2} \in \mathbb{Z}_q$ and $T_i$ denotes a timestamp. Thus, the communication cost of these two schemes is 351 bytes as

$$|M_i| + |PID_i| + |P_i| + |ct_i| + |R_i| + |S_i| = 67 + 88 + 64 + 4 + 64 + 64 = 351\ bytes.$$

In [14], $\{M_i, PID_i, P_i, U_i, V_{ijk}\}$ is sent from the vehicle (OBU) to a RSU, where $PID_i = PS1_i \in \mathbb{G}_1$. Thus, the communication cost of this scheme is 323 bytes as

$$|M_i| + |PID_i| + |P_i| + |U_i| + |V_{ijk}| = 67 + 64 + 64 + 64 + 64 = 323\ bytes.$$

In the proposed PCPA, $\{PID_i, PK_i, ct_i, u_i, v_i\}$ is sent from the vehicle (OBU) to a RSU, where $PID_i = \{PID_{i,1}, PID_{i,2}, T_i\}$, $PID_{i,1} \in \mathbb{G}$, $PID_{i,2} \in \mathbb{Z}_q$ and $T_i$ denotes a timestamp. Thus, the communication cost of the proposed scheme is 195 bytes as

$$|PID_i| + |PK_i| + |ct_i| + |u_i| + |v_i| = 44 + 40 + 4 + 20 + 20 = 128\ bytes.$$

The comparisons on the communication costs of one message and multiply $(n)$ messages is shown in Figure 3. The communication costs increase linearly with the growth of the number of messages in all schemes. The schemes in [12,13] are the same in communication costs. The communication

costs of the proposed scheme are the lowest in all schemes, which significantly decreases by 63.5%, 63.5%, and 60.4% compared with those of the schemes in [12–14], respectively. When the number of messages is 30,000, the proposed scheme can save 6.38 MB and 5.58 MB bandwidth compared with the schemes [12–14], respectively.

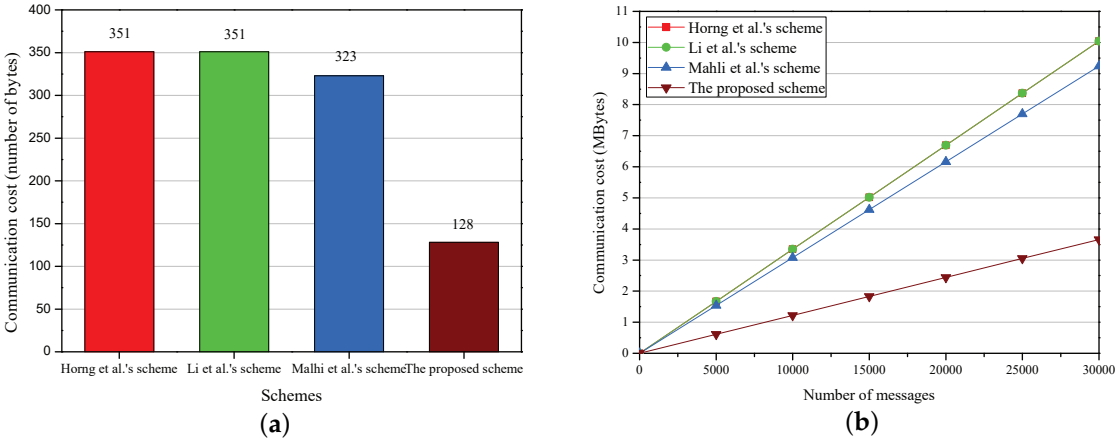


**Figure 3.** Communication cost. (**a**) communication cost of one message; (**b**) communication cost versus number of messages.

### *6.3. Simulation*

Exploring SUMO [44] and ns-3.26 [45], we evaluate the performances of the schemes of Horng et al. [12], Li et al. [13], and Malhi et al. [14] as well as the proposed PCPA scheme. The SUMO is used to generate detailed vehicle movement traces by employing models, and then these traces is put into the ns-3.26 simulator to assess the efficiency and applicability of the schemes.

The simulation road scenario is shown in Figure 4, in which the RSUs are distributed every 500 m along the road, and each vehicle broadcasts messages every 300 ms. The vehicles are distributed on the road and move to the crossings randomly. The parameters for the simulation are listed in Table 6.

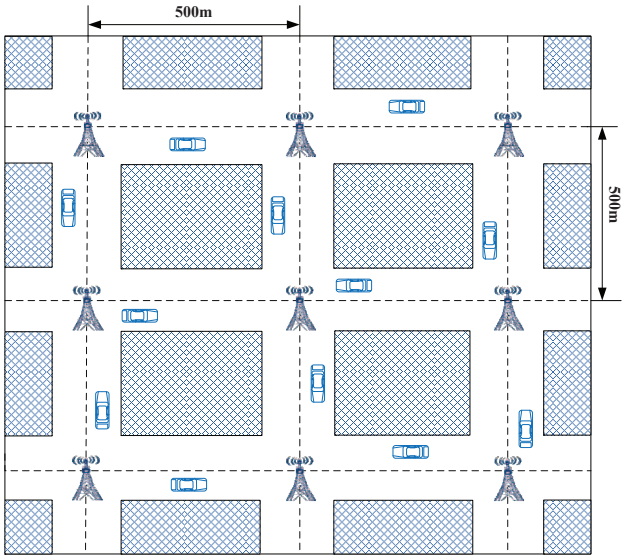


**Figure 4.** Road scenario for simulation.

The average message delay (aMD) and average message loss ratio (aMLR) are defined through the notions below:

- $N_R$: The number of RSUs within the simulation area.
- $N_V$: The number of vehicles within the simulation area.
- $N_M^i$: The number of messages sent by vehicle $V_i$.
- $T^S_{V_i \to RSU_j, M_k}$: The time for $V_i$ sending a message $M_k$ to $RSU_j$.
- $T^R_{V_i \to RSU_j, M_k}$: The time for $RSU_j$ receiving a message $M_k$ from $V_i$.
- $T^V_{avg}$: The average verification time for each message.
- $N_A^j$: The number of messages received by $RSU_j$ in the media access control (MAC) layer.
- $N_D^j$: The number of messages dropped by $RSU_j$ in the application layer.

**Table 6.** Simulation parameters.

| Parameters | Values |
|---|---|
| Simulation area | 1000 m×1000 m |
| Wireless protocol | 802.11 p |
| Channel bit rate | 6 Mbs |
| Buffer size | 1 M bytes |
| Number of RSU | 9 |
| Simulation time | 200s |
| Traffic simulation tool | SUMO |
| Network simulation tool | ns-3.26 |
| Vehicle speed | 10–50 m/s |

Average Message Delay (aMD)

The aMD reflects the average time latency for a message to be received by the RSU after it is generated, which is defined as

$$aMD = \frac{\sum_{i=1}^{N_V} \sum_{j=1}^{N_R} \sum_{k=1}^{N_M^i} (T^R_{V_i \to RSU_j, M_k} - T^S_{V_i \to RSU_j, M_k})}{\sum_{i=1}^{N_V} N_M^i} + T^V_{avg}.$$

Two experiments are conduced to analyze that how aMD with the density and speed of vehicles. The results of simulation are demonstrated in Figure 5.

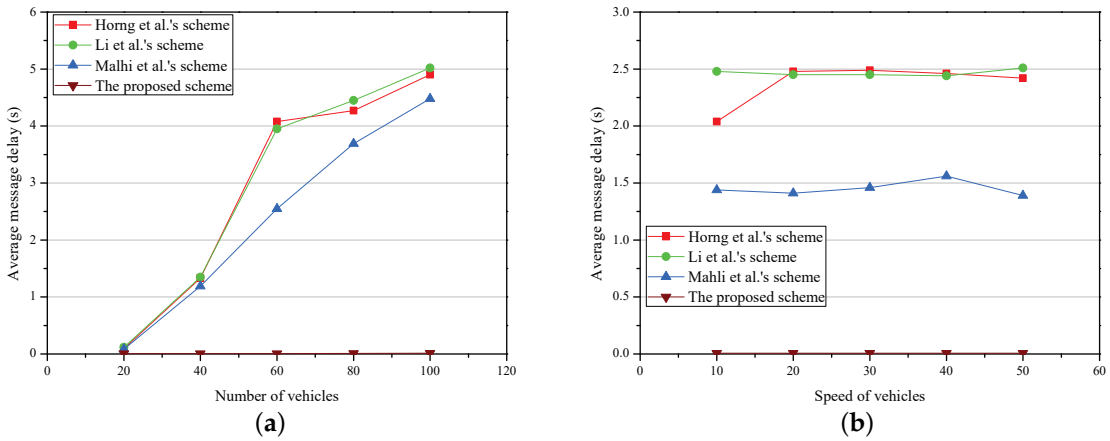


**Figure 5.** Average message delay. (**a**) average message delay versus number of vehicles; (**b**) average message delay versus speed of vehicles.

The relationship between aMD and the number of vehicles is described in Figure 5a, where the number of vehicles varies from 20 to 100, and the average speed of vehicles is approximately 20 m/s

(72 km/h). As is shown in Figure 5a, the aMD for RSUs increases with the number of vehicles in all schemes. The aMD is 2.94 s, 2.98 s, 2.40 s and 0.009 s in Horng et al.'s scheme [12], Li et al.'s scheme [13], Mahli et al.'s scheme [14] and the proposed scheme, respectively. In addition, the aMD of the proposed scheme is the lowest, which is slightly influenced by vehicle density.

The relationship between aMD and the speed of vehicles is shown in Figure 5b. The average speed of vehicles varies from 10 to 50 m/s (36 to 180 km/h) and the number of vehicles is 50. Obviously, when the vehicle density is constant, the aMD hardly changes, indicating that it is scarcely affected by the vehicle speed. This is only a theoretical simulation result with no practical implementation.

Average Message Loss Ratio (aMLR)

The aMLR expresses the ratio of the number of messages dropped to the total number of messages received by the RSUs, which is defined as

$$aMLR = \frac{1}{N_R} \sum_{j=1}^{N_R} \frac{N_D^j}{N_A^j}.$$

Two experiments are conducted to analyze aMLR with the density and speed of vehicles. The results of simulation are shown in Figure 6.

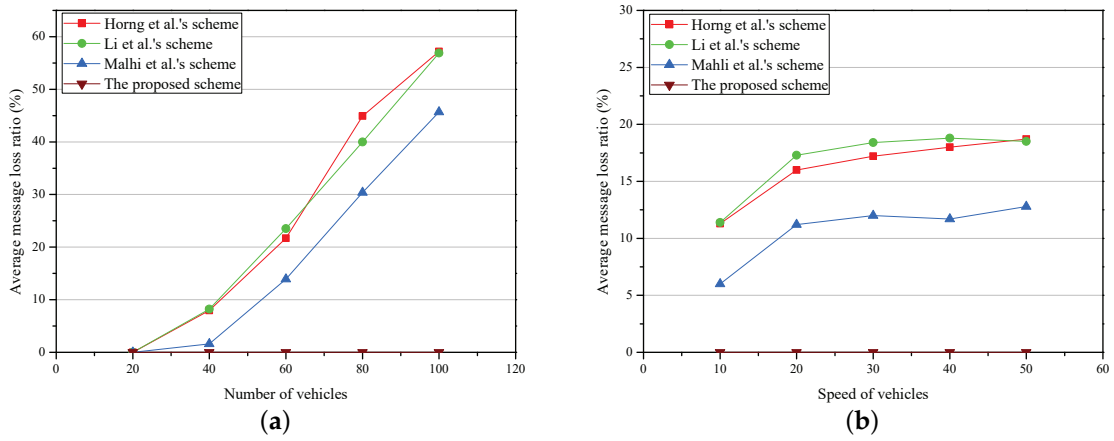


**Figure 6.** Average message loss ratio. (**a**) average message loss ratio versus number of vehicles; (**b**) average message loss ratio versus speed of vehicles.

The relationship between aMLR and the number of vehicles is shown in Figure 6a, where the number of vehicles varies from 20 to 100 and the average speed of vehicles is approximately 20 m/s (72 km/h). Under the fixed vehicle speed, when the number of vehicles is larger than 20, the aMLR grows with the number of vehicles in Horng et al.'s scheme [12], Li et al.'s scheme [13] and Malhi et al.'s scheme [14]. Furthermore, the aMLRs respectively hit 57%, 57%, 46% in the schemes of [12–14] when the number of vehicles is 100. No matter the density of the vehicles, the aMLR is almost 0.

Figure 6b shows the relationship between aMLR and the speed of vehicles. The speed of vehicles varies from 10 to 50 m/s (36 to 180 km/h) and the number of vehicles is 50. It is easy to see that, when the speed of vehicles is higher than 20 m/s, the aMLRs in the schemes of Horng et al. [12], Li et al. [13], and Malhi et al. [14] are slightly influenced. The aMLR in the proposed scheme is 0% regardless of how the vehicle speed changes.

## 7. Conclusions

In this paper, a new efficient certificateless signature with message recovery (CLS-MR) is first presented. Under the ECDLP assumption, this scheme is secure in the random oracles. Based on the

invented CLS-MR, a practical certificateless conditional privacy-preserving authentication (PCPA) scheme for VANETs is put forward. The security analysis indicates that PCPA satisfies the security and privacy-preserving requirements in VANETs. The performance evaluation and comparison show that the PCPA scheme is more efficient in both computation cost and communication cost since it does not employ map-to-point hash function and bilinear pairing operations. Furthermore, the simulation experimental results demonstrate the superiority of PCPA compared to other schemes in average message delay and message loss ratio, and thus PCPA is more suitable for VANETs.

**Author Contributions:** Y.M. and X.S. conceived of the work, designed the concrete scheme and wrote the paper.

**Acknowledgments:** This work was supported by the National Natural Science Foundation of China (61202438), the Key Project of Industry Science and Technology of Shaanxi Province (2015GY014) and the Project of Science and Technology of Xi'an City (2017088CG/RC051(CADX002)).

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

## Appendix A.

**Proof of Lemma 1.** Assuming that a Type I adversary $A_1$ can break the proposed CLS-MR in time $t$ with probability $\varepsilon$, there exists an algorithm $B$ that can solve ECDL problem by utilizing $A_1$ as subroutine. Given a random instance $\{P, xP = Q\}$ of the ECDL problem, the task of $B$ is to compute $x$.

Setup: The algorithm $B$ sets $P_{pub} = Q$ and sends system parameters *params* to $A_1$. Here, hash functions $H_1, H_2, H_3$ are considered as random oracles in the proof.

To keep the consistency and rapidly response, $B$ maintains the initially empty lists as follows:

- $H_1$ list $L_{H_1}^{list}$: This list consists of tuples $(ID_i, R_i, c_i)$.
- $H_2$ list $L_{H_2}^{list}$: This list consists of tuples $(ID_i, P_{pub}, P_i, l_i)$.
- $H_3$ list $L_{H_3}^{list}$: This list consists of tuples $(ID_i, P_{pub}, R_i, u_i, h_i)$.
- $L_{PPK}^{list}$: This list consists of tuples $(ID_i, R_i, d_i)$.
- $L_{SK}^{list}$: This list consists of tuples $(ID_i, P_i, x_i)$.

$H_1$ queries: Suppose $A_1$ submits a query on $(ID_i, R_i)$, $B$ checks $L_{H_1}^{list}$ and executes as follows:

- If the list $L_{H_1}^{list}$ includes $(ID_i, R_i, c_i)$, $B$ responds with previous value $c_i = H_1(ID_i, R_i)$ to $A_1$.
- If the list $L_{H_1}^{list}$ does not include $(ID_i, R_i, c_i)$, $B$ randomly chooses $c_i \in \mathbb{Z}_q$ , adds $(ID_i, R_i, c_i)$ in $L_{H_1}^{list}$ and sends $c_i = H_1(ID_i, R_i)$ to $A_1$.

$H_2$ queries: Suppose $A_1$ submits a query on $(ID_i, P_{pub}, P_i)$, $B$ checks $L_{H_2}^{list}$ and executes as follows:

- If the list $L_{H_2}^{list}$ includes $(ID_i, P_{pub}, P_i, l_i)$, $B$ responds with previous value $l_i = H_2(ID_i, P_{pub}, P_i)$ to $A_1$.
- If the list $L_{H_2}^{list}$ does not include $(ID_i, P_{pub}, P_i, l_i)$, $B$ randomly chooses $l_i \in \mathbb{Z}_q$, adds $(ID_i, P_{pub}, P_i, l_i)$ in $L_{H_2}^{list}$ and sends $l_i = H_2(ID_i, P_{pub}, P_i)$ to $A_1$.

$H_3$ queries: Suppose $A_1$ submits a query on $(ID_i, P_{pub}, R_i, u_i)$, $B$ checks $L_{H_3}^{list}$ and executes as follows:

- If the list $L_{H_3}^{list}$ includes $(ID_i, P_{pub}, R_i, u_i, h_i)$, $B$ responds with previous value $h_i = H_3(ID_i, P_{pub}, R_i, u_i)$ to $A_1$.
- If the list $L_{H_3}^{list}$ does not include $(ID_i, P_{pub}, R_i, u_i, h_i)$, $B$ randomly chooses $h_i \in \mathbb{Z}_q$, adds $(ID_i, P_{pub}, R_i, u_i, h_i)$ in $L_{H_3}^{list}$ and sends $h_i = H_3(ID_i, P_{pub}, R_i, u_i)$ to $A_1$.

Partial private key queries: Suppose $A_1$ submits a partial private key query on the identity $ID_i$, $B$ checks $L_{PPK}^{list}$ and executes as follows:

- If the list $L_{PPK}^{list}$ includes $(ID_i, R_i, d_i)$, $B$ responds with previous value $(R_i, d_i)$ to $A_1$.

- If the list $L_{PPK}^{list}$ does not include $(ID_i, R_i, d_i)$, $B$ picks random numbers $d_i, c_i \in \mathbb{Z}_q$ and sets $c_i = H_1(ID_i, R_i)$ and $R_i = d_iP - c_iP_{pub}$. Finally, $B$ outputs the $(R_i, d_i)$ to $A_1$, and inserts the $(ID_i, R_i, c_i)$ and $(ID_i, R_i, d_i)$ to $L_{H_1}^{list}$ and $L_{PPK}^{list}$, respectively.

Secret value queries: Suppose $A_1$ submits a secret value query on the identity $ID_i$, $B$ checks $L_{SK}^{list}$ and executes as follows:

- If the list $L_{SK}^{list}$ includes $(ID_i, P_i, x_i)$, $B$ responds with previous value $x_i$ to $A_1$.
- If the list $L_{SK}^{list}$ does not include $(ID_i, P_i, x_i)$, $B$ randomly chooses $x_i \in \mathbb{Z}_q^*$ and computes $P_i = x_iP$. Finally, $B$ returns $x_i$ to $A_1$, and inserts the $(ID_i, P_i, x_i)$ to $L_{SK}^{list}$.

Public key queries: Suppose $A_1$ submits a public key query on the identity $ID_i$, $B$ checks $L_{PPK}^{list}$, $L_{SK}^{list}$ and executes as follows:

- If the list $L_{PPK}^{list}$ includes $(ID_i, R_i, d_i)$ and the list $L_{SK}^{list}$ includes $(ID_i, P_i, x_i)$, $B$ responds with previous value $(R_i, P_i)$ to $A_1$.
- If the list $L_{PPK}^{list}$ does not include $(ID_i, R_i, d_i)$ or $L_{SK}^{list}$ does not include $(ID_i, P_i, x_i)$, $B$ issues a partial private key query or secret value query itself on $ID_i$. Finally, $B$ returns $(R_i, P_i)$ to $A_1$, and inserts the corresponding values to $L_{PPK}^{list}$ and $L_{SK}^{list}$.

Public key replacement queries: Suppose $A_1$ submits a public key replacement query on $\{ID_i, R_i', P_i'\}$, $B$ checks $L_{PPK}^{list}$, $L_{SK}^{list}$ and executes as follows:

- If the list $L_{PPK}^{list}$ includes $(ID_i, R_i, d_i)$ and the list $L_{SK}^{list}$ includes $(ID_i, P_i, x_i)$, $B$ sets $R_i = R_i'$, $P_i = P_i'$, $d_i = \perp$, $x_i = \perp$ and updates $(ID_i, R_i, d_i)$, $(ID_i, P_i, x_i)$ to the list $L_{PPK}^{list}$ and $L_{SK}^{list}$, respectively.
- If the list $L_{PPK}^{list}$ does not include $(ID_i, R_i, d_i)$ or the list $L_{SK}^{list}$ does not include $(ID_i, P_i, x_i)$, $B$ sets $R_i = R_i'$, $P_i' = P_i'$, $d_i = \perp$, $x_i = \perp$ and inserts $(ID_i, R_i, d_i)$, $(ID_i, P_i, x_i)$ to the list $L_{PPK}^{list}$ and $L_{SK}^{list}$, respectively.

Sign queries: Suppose $A_1$ submits a sign query on $(m, ID_i, R_i, P_i)$, $B$ firstly conducts a partial private key query itself to generate $(R_i, d_i)$. $B$ randomly chooses $v_i \in \mathbb{Z}_q^*$ and computes $f = F_1(m)||F_2(F_1(m)) \oplus m$, $u_i = f \oplus (v_iP - l_iP_i - h_iR_i - h_ic_iP_{pub})$. If the tuple including $h_i$ already appears on $L_{H_3}^{list}$, $B$ selects another $v_i \in \mathbb{Z}_q^*$ and tries again. Finally, $B$ returns $\{u_i, v_i\}$ to $A_1$.

Forgery: $A_1$ outputs a valid signature $(u_i^*, v_i^*)$ on $m^*$ under $(ID_i^*, R_i^*, P_i^*)$. Using the Forking Lemma [48], $B$ can obtain another valid signature $(u_i^*, v_i^{*\prime})$ under $(ID_i^*, R_i^*, P_i^*)$ by replaying the process with the same random tape, yet with a different choice of $H_1$. Then, we have

$$v_i^*P - l_i^*P_i - h_i^*R_i - h_i^*c_i^*P_{pub} = v_i^{*\prime}P - l_i^*P_i - h_i^*R_i - h_i^*c_i^{*\prime}P_{pub},$$

$$v_i^*P - h_i^*c_i^*P_{pub} = v_i^*P_i - h_i^*c_i^*P_{pub}.$$

From the above equation, we obtain

$$(v_i^* - v_i^{*\prime})P = (h_i^*c_i^* - h_i^*c_i^{*\prime})xP.$$

Finally, $B$ outputs the solution to ECDL problem $x = h_i^{*-1}(c_i^* - c_i^{*'})^{-1}(v_i^* - v_i^{*'})$.

After completing the above simulation, we will analyze the $B$'s probability and time for solving the ECDL problem.

Let us assume that $A_1$ can make at most $q_{H_i}$ $H_i(i = 1, 2, 3)$ queries, $q_{pp}$ partial private key queries, $q_{sv}$ secret value queries, $q_{pk}$ public key queries, $q_{pr}$ public key replacement queries, and $q_s$ times sign queries.

The probability of failure in making a partial private key query caused by a conflict on is $H_1$ most $\frac{q_{H_1}q_{pp}}{q}$. The probability of failure in issuing a sign query resulting from a conflict on $H_3$ is at most $\frac{q_s(q_{H_3}+q_s)}{q}$. In addition, the probability of $A_1$ outputs a valid forgery without asking the

corresponding $H_1, H_2, H_3$ is at most $\frac{3}{q}$. The probability of $B$ correctly guesses it as the point of rewind is at least $\frac{1}{q_{H_1}}$. Therefore, the success probability of $B$ for solving the ECDL problem is at least $\frac{\varepsilon-(q_{H_1}q_{pp}+q_s(q_{H_3}+q_s)+3)/q}{q_{H_1}}$.

The running time of $B$ is equal to the running time of $A_1$ plus the time it takes to respond to $q_{pp}$ partial private key queries, $q_{sv}$ secret value queries, $q_{pk}$ public key queries and $q_s$ sign queries. Each partial private key query requires 2 scale multiplication operations in $\mathbb{G}$. Each secret value query requires 1 scale multiplication operation in $\mathbb{G}$. Each public key query requires 1 scale multiplication operation in $\mathbb{G}$. Each sign query requires 4 scale multiplication operations in $\mathbb{G}$. Assuming that each scale multiplication in $\mathbb{G}$ needs time $t_{sm}$, the total running time of $B$ is at most $t + (2q_{pp} + q_{sv} + q_{pk} + 4q_s)t_{sm}$. □

## Appendix B.

**Proof of Lemma 2.** Assuming that a Type II adversary $A_2$ can break the proposed CLS-MR in time $t$ with probability $\varepsilon$, there exists an algorithm $B$ that can solve ECDL problem by utilizing $A_2$ as subroutine. Given a random instance $\{P, xP = Q\}$ of the ECDL problem, the task of $B$ is to compute $x$.

Setup: The algorithm $B$ randomly selects $\theta \in \mathbb{Z}_q$ and defines $\theta P = P_{pub}$; then, $B$ sends the system parameters *params* and master key $\theta$ to $A_2$. Note that $A_2$ has the master key and does not require to issue any partial private key query. Similar to Lemma 1, the lists $L_{H_1}^{list}$, $L_{H_2}^{list}$, $L_{H_3}^{list}$, $L_{PPK}^{list}$ and $L_{SK}^{list}$ are maintained by $B$. $B$ also keeps a list $L^{list} = (ID_i, P_i, x_i, z_i)$, which is initial-empty.

$H_1$, $H_2$ and $H_3$ queries: It is the same as Lemma 1.

Secret value queries: Suppose $A_2$ submits a secret value query on the identity $ID_i$, $B$ checks $L^{list}$ and executes as follows:

- If the list $L^{list}$ includes $(ID_i, P_i, x_i, z_i)$, if $z_i = 0$, $B$ halts; if $z_i = 1$, $B$ responds with previous value $x_i$ to $A_2$.
- If the list $L^{list}$ does not include $(ID_i, P_i, x_i, z_i)$, using the Coron's technique [49], $B$ tosses a coin $z_i \in \{0, 1\}$ that produces 0 with probability $\delta$ and 1 with probability $1 - \delta$. $B$ randomly chooses a value $x_i \in \mathbb{Z}_q$. If $z_i = 0$, $B$ sets $P_i = x_iQ$ ; if $z_i = 1$, $B$ sets $P_i = x_iP$. Finally, $B$ inserts the $(ID_i, P_i, x_i, z_i)$ to $L^{list}$. If $z_i = 0$, $B$ halts; if $z_i = 1$, $B$ responds the value $x_i$ to $A_2$.

Public key queries: Suppose $A_2$ submits a public key query on the identity $ID_i$, $B$ checks $L^{list}$ and executes as follows:

- If the list $L^{list}$ includes $(ID_i, P_i, x_i, z_i)$, $B$ responds with previous value $P_i$ to $A_2$.
- If the list $L^{list}$ does not include $(ID_i, P_i, x_i, z_i)$, $B$ submits a secret value query on $ID_i$ and returns $P_i$ to $A_2$ . Here, $A_2$ can obtain $R_i$ corresponding to $D_i$ using the master key.

Sign queries: It is the same as Lemma 1.

Forgery: $A_2$ outputs a valid signature $(u_i^*, v_i^*)$ on $m^*$ under $(ID_i^*, R_i^*, P_i^*)$. Using the Forking Lemma [48], $B$ can obtain another valid signature $(u_i^*, v_i^{*\prime})$ on $m^*$ under $(ID_i^*, R_i^*, P_i^*)$ by replaying process under the same random tape with a different choice of $H_2$. Then, we have

$$v_i^*P - l_i^*P_i - h_i^*R_i - h_i^*c_i^*P_{pub} = v_i^{*\prime}P - l_i^{*\prime}P_i - h_i^*R_i - h_i^*c_i^*P_{pub},$$

$$v_i^*P - l_i^*P_i = v_i^{*\prime}P_i - l_i^{*\prime}P_i.$$

From the above equation, $B$ checks the $L^{list}$, if $c_i^* = 1$, $B$ aborts; if $c_i^* = 0$, the above equation, we have

$$(v_i^* - v_i^{*\prime})P = (l_i^* - l_i^{*\prime})x_ixP.$$

Finally, $B$ outputs $x$ by computing $x = x_i^{*^{-1}}(l_i^* - l_i^{*'})^{-1}(v_i^* - v_i^{*'})$, which is the solution to the ECDL problem.

The same as Lemma 1, the analysis on the probability and time of $B$ is as follows, assuming that $A_2$ can make at most $q_{H_i}$ $H_i(i = 1, 2, 3)$ queries, $q_{sv}$ secret value queries, $q_{pk}$ public key queries, and $q_s$ sign queries.

The probability of failure in handing a sign query because of a conflict on $q_{H_3}$ is at most $\frac{q_s(q_{H_3}+q_s)}{q}$. In a secret value query and forgery phase, the probability of success is $(1-\delta)^{q_{sv}}\delta$ according to Coron's technique [49]. When the optimal probability is $\delta = \frac{1}{q_{sv}+1}$, it is greater than $\frac{1}{e(q_{sv}+1)}$. The probability of $A_2$ outputs a valid forgery signature without asking the corresponding $H_1$ or $H_2$ or $H_3$ is at most $\frac{3}{q}$. The probability of $B$ correctly guesses it, as the point of rewind is at least $\frac{1}{q_{H_2}}$. Therefore, the success probability of $B$ for solving the ECDL problem is at least $\frac{\varepsilon - (q_s(q_{H_3}+q_s)+3)/q}{e(q_{sv}+1)q_{H_2}}$.

The running time of $B$ is equal to the running time of $A_2$ plus the time it takes to respond to $q_{sv}$ secret value queries, $q_{pk}$ public key queries and $q_s$ sign queries. Each secret value query requires one scale multiplication operation in $\mathbb{G}$. Each public key query requires one scale multiplication operation in $\mathbb{G}$. Each sign query requires four scale multiplication operations in $\mathbb{G}$. Assuming that each scale multiplication in $\mathbb{G}$ needs time $t_{sm}$, the total running time of $B$ is at most $t + (q_{cv} + q_{pk} + 4q_s)t_{sm}$. □

## References


1. Raya, M.; Hubaux, J.P. Securing vehicular ad hoc networks. *J. Comput. Secur.* **2007**, *15*, 39–68. [CrossRef]
2. Dedicated Short Range Communications (DSRC). Available online: http://grouper.ieee.org/groups/scc32/dsrc/index.html (accessed on 10 April 2018).
3. Oh, H.; Yae, C.; Ahn, D.; Cho, H. 5.8 GHz DSRC packet communication system for ITS services. In Proceedings of Vehicular Technology Conference-VTC'99, IEEE, Amsterdam, The Netherlands, 9–22 September 1999; pp. 2223–2227.
4. Hubaux, J.P.; Capkun, S.; Luo, J. The security and privacy of smart vehicles. *IEEE Secur. Priv.* **2004**, *2*, 49–55. [CrossRef]
5. Lin, X.; Lu, R.; Zhang, C.; Zhu, H.; Ho, P.H.; Shen, X. Security in vehicular ad hoc networks. *IEEE Commun. Mag.* **2008**, *46*, 88–95.
6. Kargl, F.; Papadimitratos, P.; Buttyan, L. Secure vehicular communication systems: Implementation, performance, and research challenges. *IEEE Commun. Mag.* **2008**, *46*, 110–118. [CrossRef]
7. Qu, F.; Wu, Z.; Wang, F.Y.; Cho, W. A security and privacy review of VANETs. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 2985–2996. [CrossRef]
8. Petit, J.; Schaub, F.; Feiri, M.; Kargl, F. Pseudonym schemes in vehicular networks: A survey. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 228–255. [CrossRef]
9. Lin, X.D.; Sun, X.T.; Ho, P.H. GSIS: Secure vehicular communications with privacy preserving. *IEEE Trans. Veh. Technol.* **2007**, *56*, 3442–3456.
10. Lu, R.; Lin, X.; Zhu, H. ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. In Proceedings of the INFOCOM 2008, the 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008; pp. 1229–1237.
11. Zhang, C.; Lu, R.; Lin, X. An efficient identity-based batch verification scheme for vehicular sensor networks. In Proceedings of the INFOCOM 2008, the 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008; pp. 246–250.
12. Horng, S.J.; Tzeng, S.F.; Huang, P.H. An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks. *Inf. Sci.* **2015**, 317, 48–66. [CrossRef]
13. Li, J.; Yuan, H.; Zhang, Y. Cryptanalysis and Improvement of Certificateless Aggregate Signature with Conditional Privacy-Preserving for Vehicular Sensor Networks. Available online: http://eprint.iacr.org/2016/692.pdf (accessed on 10 April 2018).
14. Malhi, A.K.; Batra, S. An efficient certificateless aggregate signature scheme for vehicular ad-hoc networks. *Discret. Math. Theor. Comput.* **2015**, *17*, 317–338.

15. Kumar, P.; Sharma, V. On the security of certificateless aggregate signature scheme in vehicular ad hoc networks. In *Soft Computing Theories and Applications*; Springer: Singapore, 2018; pp. 715–722.
16. Al-Riyami, S.S.; Paterson, K.G. Certificateless public key cryptography. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, 30 November–4 December 2003; pp. 452–473.
17. Miller, V.S. Use of elliptic curves in cryptography. In Proceedings of Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 1985; pp. 417–426.
18. Koblitz, N. Elliptic curve cryptosystems. *J. Math. Comput.* **1987**, *48*, 203–209. [CrossRef]
19. Zhang, C.; Lin, X.; Lu, R.; Ho, P.-H. RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks. In Proceedings of the IEEE International Conference on Communications, ICC '08, Beijing, China, 19–23 May 2008; pp. 1451–1457.
20. Shamir, A. Identity-based cryptosystems and signature schemes. In Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Santa Barbara, CA, USA, 19–22 August 1984; pp. 47–53.
21. Zhang, C.; Ho, P.H.; Tapolcai, J. On batch verification with group testing for vehicular communications. *Wirel. Netw.* **2011**, *17*, 1851–1865. [CrossRef]
22. Jiang, Y.; Shi, M.; Shen, X. BAT: A robust signature scheme for vehicular networks using binary authentication tree. *IEEE Trans. Wirel. Commun.* **2009**, *8*, 1974–1983. [CrossRef]
23. Chim, T. W.; Yiu, S.M.; Hui, L.C.; Li, V.O. SPECS: Secure and privacy enhancing communications schemes for VANETs. *Ad Hoc Netw.* **2011**, *9*, 189–203. [CrossRef]
24. Huang, D.; Misra, S.; Verma, M. PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs. *IEEE Trans. Intell. Transp. Syst.* **2011**, *12*, 736–746. [CrossRef]
25. Shim, K.A. CPAS: An Efficient conditional privacy-preserving authentication scheme for vehicular sensor networks. *IEEE Trans. Veh. Technol.* **2012**, *61*, 1874–1883. [CrossRef]
26. Shim, K.A. Reconstruction of a secure authentication scheme for vehicular ad hoc networks using a binary authentication tree. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 5386–5393. [CrossRef]
27. Lee, C.C.; Lai, Y.M. Toward a secure batch verification with group testing for VANET. *Wirel. Netw.* **2013**, *19*, 1441–1449. [CrossRef]
28. Horng, S.J.; Tzeng, S.F.; Pan, Y. b-SPECS+: Batch verification for secure pseudonymous authentication in VANET. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1860–1875. [CrossRef]
29. Zhang, J.; Xu, M.; Liu, L. On the security of a secure batch verification with group testing for VANET. *Int. J. Netw. Secur.* **2014**, *16*, 351–358.
30. Liu, J. K.; Yuen, T.H.; Au, M.H.; Susilo, W. Improvements on an authentication scheme for vehicular sensor networks. *Expert Syst. Appl.* **2014**, *41*, 2559–2564. [CrossRef]
31. Bayat, M.; Barmshoory, M.; Rahimi, M.; Aref, M.R. A secure authentication scheme for VANETs with batch verification. *Wirel. Netw.* **2015**, *21*, 1733–1743. [CrossRef]
32. Li, J.; Lu, H.; Guizani, M. ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. *IEEE Trans. Parallel Distrib.* **2015**, *26*, 938–948. [CrossRef]
33. Wang, F.; Xu. Y.; Zhang, H. 2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET. *IEEE Trans. Veh. Technol.* **2016**, *65*, 896–911. [CrossRef]
34. Zhang, L.; Hu, C.; Wu, Q. Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response. *IEEE Trans. Comput.* **2016**, *65*, 2562–2574. [CrossRef]
35. Jiang, S.; Zhu, X.; Wang, L. An efficient anonymous batch authentication scheme based on HMAC for VANETs. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 2193–2204. [CrossRef]
36. Tzeng, S.F.; Horng, S. J.; Li, T. Enhancing security and privacy for identity-based batch verification scheme in VANETs. *IEEE Trans. Veh. Technol.* **2017**, *66*, 3235–3248. [CrossRef]
37. He, D.; Zeadally, S.; Xu, B.; Huang, X. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2681–2691. [CrossRef]
38. Xie, Y.; Wu, L.; Shen, J.; Alelaiwi, A. EIAS-CP: New efficient identity-based authentication scheme with conditional privacy preserving for VANETs. *Telecommun. Syst.* **2016**, *65*, 229–240. [CrossRef]
39. Xie, Y.; Wu, L.; Zhang, Y.; Shen, J. Efficient and secure authentication scheme with conditional privacy-preserving for VANETs. *Chin. J. Electron.* **2016**, *25*, 950–956. [CrossRef]

40. Zhong, H.; Wen, J.; Cui, J.; Zhang, S. Efficient conditional privacy-preserving and authentication scheme for secure service provision in VANET. *Tsinghua Sci. Technol.* **2016**, *21*, 620–629. [CrossRef]
41. Lo, N.W.; Tsai, J.L. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 1319–1328. [CrossRef]
42. Wu, L.; Fan, J.; Xie, Y.; Wang, J.; Liu, Q. Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks. *Int. J. Distrib. Sens. Netw.* **2017**, *13*, 1–12. [CrossRef]
43. Cui, J.; Zhang, J.; Zhong, H. SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter. *IEEE Trans. Veh. Technol.* **2017**, *66*, 10283–10295. [CrossRef]
44. Sumo Project. Available online: http://sourceforge.net/projects/sumo/ (accessed on 10 April 2018).
45. Network Simulator NS-3. Available online: http://www.nsnam.org/ (accessed on 10 April 2018).
46. Shamus Software Ltd. Multi Precision Integer and Rational Arithmetic Cryptographic Library (MIRACL). Available online: http://www.certivox.com/miracl/ (accessed on 10 April 2018).
47. IEEE Std. 1609.2. *IEEE Trial-User Standard for Wireless Access in Vehicular Environments. Security Services for Applications and Management Messages*; IEEE: Piscataway Township, NJ, USA, 2006; doi:10.1109/IEEESTD.2006.243731. [CrossRef]
48. Pointcheval, D.; Stern, J. Security proofs for signature schemes. In Proceedings of the nternational Conference on the Theory and Applications of Cryptographic Techniques, Saragossa, Spain, 12–16 May 1996; pp. 387–398.
49. Coron, J.S. On the exact security of full domain hash. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2000; pp. 229–235.