An Efficient Anonymous Authentication Scheme with Secure Communication in Intelligent Vehicular Ad-hoc Networks

Xiaojun Zhang[1,2,*], Liming Mu[1,*], Jie Zhao[1], Chunxiang Xu[2]
[1]Research Center for Cyber Security, School of Computer Science, Southwest Petroleum University, Chengdu 610500, China
[E-mail: zhangxjdzkd2012@163.com, mulming@163.com]
[2]Center for Cyber Security, School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
*Corresponding author: Xiaojun Zhang, Liming Mu

Received July 5, 2018; revised October 24, 2018; accepted November 21, 2018; published June 30, 2019

Abstract

Vehicular ad-hoc networks (VANETs) have become increasingly significant in intelligent transportation systems, they play a great role in improving traffic safety and efficiency. In the deployment of intelligent VANETs, intelligent vehicles can efficiently exchange important or urgent traffic information and make driving decisions. Meanwhile, secure data communication and vehicle's identity privacy have been highlighted. To cope with these security issues, in this paper, we construct an efficient anonymous authentication scheme with secure communication in intelligent VANETs. Combing the ElGamal encryption technique with a modified Schnorr signature technique, the proposed scheme provides secure anonymous authentication process for encrypted message in the vehicle-to-infrastructure communication model, and achieves identity privacy, forward security, and reply attack resistance simultaneously. Moreover, except the trusted authority (TA), any outside entity cannot trace the real identity of an intelligent vehicle. The proposed scheme is designed on an identity-based system, which can remove the costs of establishing public key infrastructure (PKI) and certificates management. Compared with existing authentication schemes, the proposed scheme is much more practical in intelligent VANETs.

Keywords: Vehicular ad-hoc networks, anonymous authentication, secure data communication, identity privacy, forward security

http://doi.org/10.3837/tiis.2019.06.028 **ISSN : 1976-7277**

1. Introduction

With the rapid development of wireless communication and network technologies [1-3], the vehicular ad-hoc network (VANET) is a continuously self-configuring, infrastructure-less network, which has upgraded the traditional transportation systems to the intelligent transportation systems. In the deployment of intelligent VANETs [4], there are various types of vehicles equipped with on-board units (OBUs), in which the wireless communication modules are installed, they contribute to message transmission and reception through Wi-Max or Wi-Fi. Moreover, in the intelligent transportation systems, roadside units (RSUs) are established to take responsibility for distributing emergent events efficiently.

In general, the typical structure of a VANET is depicted in **Fig. 1**. Particularly, the short-range wireless communication protocol, termed the Dedicated Short Range Communication (DSRC) protocol, plays a great role in the VANET. The vehicle equipped with an OBU can communicate with other vehicles under the DSRC protocol in the VANET, which is a vehicle-to-vehicle (V2V) communication model [5-6]. In such model, each vehicle can exchange the traffic conditions, including weather conditions, road defects, each vehicle's location and speed, so that they can quickly avoid possible traffic congestion, or traffic accidents. On the other hand, the vehicle equipped with an OBU can communicate with roadside units (RSUs) under the DSRC protocol, which is a vehicle-to-RSU (V2R) communication model [5-6]. This communication model enables the VANET to offer many safety services, RSUs can send information about traffic conditions to the traffic control center. Thus, the traffic control center can also promptly take action to broadcast emergency and traffic sign violation warnings, thereby improving traffic safety and efficiency.

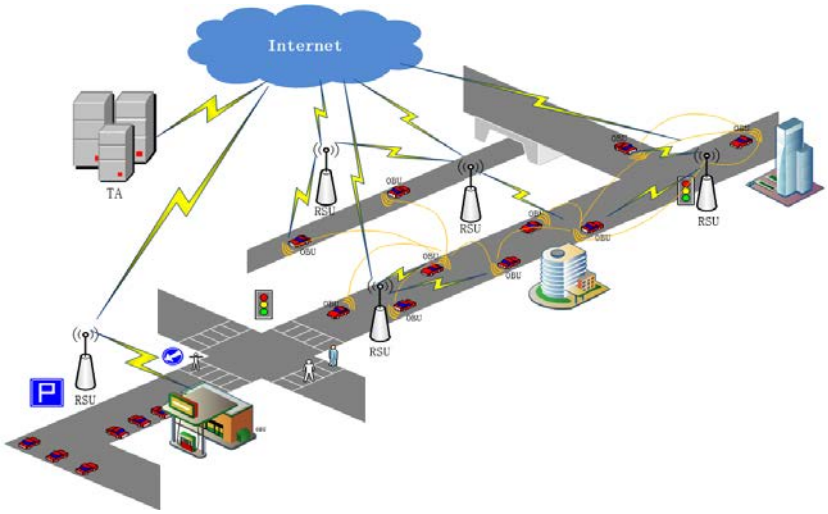

Fig. 1. The Structure of the VANET

Despite the promising features of VANETs have brought many benefits to the intelligent transportation systems, the open-medium nature of these communications may intrigue VANETs to be vulnerable to various kinds of active attacks [7]. More specifically, the identity privacy, message integrity, and authentication are the most significant security concerns [8-9]. A malicious vehicle may impersonate as an emergency vehicle to exceed speed limits without being permitted. Worse still, if the real identity of a vehicle is revealed, the location privacy of the vehicle would be disclosed. Furthermore, if message integrity is not provided, a malicious

vehicle could change the content of a message that is sent by a legitimate vehicle. Thus, the other vehicles and the RSUs cannot estimate the traffic situation according to the received message. Simultaneously, to improve the efficiency in the intelligent transportation systems, an intelligent VANET is also constructed to support batch verification of safety messages in the vehicle-to-infrastructure communication model.

Up to date, many existing anonymous authentication schemes based on public key infrastructure (PKI) have been proposed [10-15]. However, these schemes need the complex certificate management, which might hinder the deployment of anonymous authentication for intelligent VANETs in practice. While an identity-based cryptographic system, first introduced by Shamir [16], can avoid establishing the Public key Infrastructure (PKI). In such a system, a trusted Key Generation Centre (KGC) can generate an entity's private key according to any known information of an entity's identity. Consequently, anonymous identity-based authentication schemes for intelligent VANETs have more advantages, especially in the mobile intelligent VANETs. In the literature [17-21], some identity-based anonymous authentication schemes for intelligent VANETs have been proposed.

Although some of these schemes mentioned above can achieve identity privacy, message integrity and authentication, message confidentiality is also important in some intelligent VANETs. Especially in some sensitive geographic regions, a vehicle needs to send some authenticated encrypted message to nearby RSUs for secure communication. Moreover, traceability is also very essential in secure intelligent VANETs, if an anonymous vehicle in the intelligent VANET turns malicious, its identity privacy should be revoked by the trusted authority (TA) and revealed to other vehicles.

To fill the aforementioned gap, in this paper, we propose an efficient anonymous authentication scheme with secure communication in intelligent VANETs. In particular, we focus on constructing the anonymous authentication scheme from vehicles equipped with the OBUs to nearby RSUs, the contributions of this work are specified as follows.

(1) We take advantage of the ElGamal encryption technique [22] to achieve message confidentiality, and employs the modified Schnorr signature technique [23] to ensure the authentication of an encrypted message.

(2) In the vehicle-to-RSU (V2R) communication model, we set a fully trusted authority (TA), which generates an anonymous identity of a legitimate vehicle according to its registered real identity and login password. Simultaneously, as the role of the KGC, the TA can generate the private key of the anonymous identity. Once a nearby RSU succeeds in decrypting and verifying the authenticated encrypted message from the anonymous intelligent vehicle, the RSU can accept the legal anonymous identity and the transmitted message. In addition, when a dispute appears, the TA can efficiently trace the real identity of the anonymous intelligent vehicle.

(3) The proposed scheme is designed on an identity-based system, which can remove the costs of establishing public key infrastructure (PKI) and certificates management. In comparison with existing authentication schemes, the proposed scheme owns much lower communication overhead, without time-consuming bilinear pairing operations, the proposed scheme has better efficiency, which is much more practical in intelligent VANETs.

2. Related Work

In order to cope with the security and privacy issues in intelligent VANETs, the conditional privacy-preserving authentication (CPPA) scheme is a good candidate. Raya *et al.* [10] firstly

modified PKI to guarantee message authentication, integrity, and identity privacy. However, in Raya *et al's* scheme, to achieve identity privacy, each intelligent vehicle needs to have a large storage space to keep key pairs and corresponding certificates. To validate their identities and trace them in case of any disputes, the trusted authority (TA) is also required to have a large storage space to save vehicles' certificates. Moreover, a malicious vehicle's real identity will be hard to be found by the TA due to the exhaustive search of all stored certificates. Lu *et al.* [11] proposed another authentication scheme with temporary anonymous certificates generated from the RSUs, but it needs frequent interactions of vehicles with RSUs to get corresponding anonymous certificates. Subsequently, some feasible techniques [12-13] have been proposed to overcome the weakness of [11]. More specifically, Freudiger *et al.* [12] leveraged the idea of mix-zones technique to propose a modified CPPA scheme, while the RSUs and the vehicles also need a large storage space for those anonymous certificates. Zhang *et al.* [13] combined a message authentication code and a key agreement protocol to construct an efficient CPPA scheme for VANETs, which can avoid malicious vehicles entering into the VANETs. After that, some group/ring signature-based authentication schemes [24–26] have been proposed.

To simplify the complex certificate management in above PKI-based CPPA schemes, Zhang *et al.* [17] pioneered an identity-based CPPA scheme. However, the schemes in [27-28] pointed out that the scheme in [17] is vulnerable to the replay attack and cannot satisfy the property of non-repudiation. Chim *et al.* [28] further proposed an improved identity-based CPPA scheme for VANETs. Zhang *et al.* [29] pointed that the scheme in [27] cannot resist impersonation attack or cannot provide non-repudiation, they also proposed the improved model to address these security threats. Moreover, the integrity verification scheme in [30] has succeeded in achieving forward security, in which, the key update technique can also be well applied in post-quantum secure intelligent VANETs. Biswas *et al.* [31] integrated an ID-based proxy signature scheme with the standard ECDSA to generate a new authentication scheme. Shim [32] proposed another identity-based CPPA scheme for vehicle-to-infrastructure communication model. More recently, He *et al.* [20] proposed a new ID-based CPPA scheme, which could be used for both V2V communication model and V2R communication model in VANETs. To improve performance, the function of batch verification of multiple messages is included in the proposed ID-based CPPA scheme. Recently, the small exponent test technology has been exploited [33], to enable perform batch verification. Lo *et al.* [21] proposed a new identity-based signature based on the elliptic curve cryptosystem and further proposed a novel CPPA. Asaar et al. [34] proposed a proxy signature protocol with batch verification function, and integrated it into construct a secure authentication for VANETs. To aviod key escrow and complex certificate management, a practical certificateless conditional privacy-preserving authentication scheme for VANETs has also been given in [35].

3. Preliminaries

3.1 System Network Model of A VANET

Now we introduce the system network model of a VANET in **Fig. 2**. It mainly consists of three entities, vehicle, RSU, and trusted authority (TA).

Vehicle: The intelligent vehicle in the VANET is equipped with an OBU, which enables the vehicle to communicate with a nearby RSU through the DSRC protocol. Each OBU has a tamper-proof device (TPD) to store the sensitive information, such as a private key, a global positioning system (GPS) for providing the location and time information, and an event data recorder (EDR) for recording related information about vehicle crashes.

RSU: The RSU is a fixed infrastructure, it is deployed on the roadside and can communicate with vehicles under the DSRC protocol. It can validate received messages and send them to the traffic management center or process them locally.

Trusted Authority: The TA is responsible for maintaining the whole VANET systems. It is considered to be a fully trusted third party with high computation and communication capabilities. The TA is responsible for the registration of RSUs and vehicles, it generates system security parameters and preloads them in the OBU embedded in the vehicles. In addition, as the role of a Key Generator Centre (KGC) of an identity-based system, the TA can produce the anonymous identity of an intelligent vehicle and its corresponding private key. In the system network model of a VANET, only the TA can trace the real identity of the vehicle.

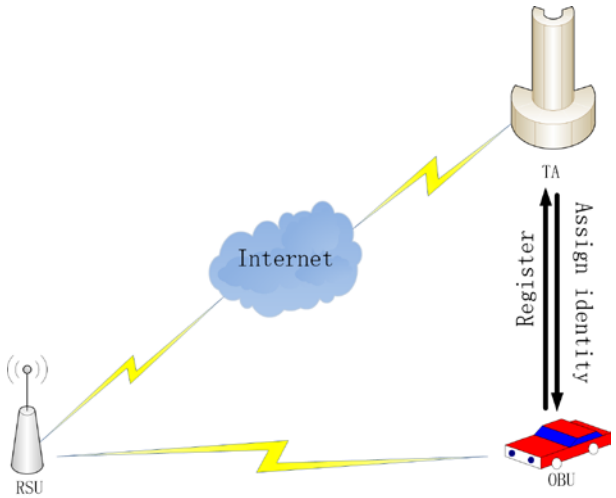

Fig. 2. The System Network Model of A VANET

3.2 Security Requirements

The system network model of a VANET is confronted with various kinds of active attacks, such as denial of service attack, replay attack, impersonation attack and location spoofing. More importantly, an anonymous authentication scheme with secure communication in intelligent VANETs should satisfy the following security requirements.

Message authentication and integrity: The nearby RSU is able to check the validity of the message sent by an intelligent vehicle. In addition, the RSU can detect any modifications of the received message, any outside adversary cannot successfully generate a forged authenticated message to convince the RSU.

Message confidentiality: For the transmission of message, an intelligent vehicle equipped with the OBU needs to generate the authenticated encrypted message, and send it to the RSU. Thus, without the private key of the RSU, any outside adversary cannot decrypt the encrypted message.

Identity privacy preservation: The RSU and any other vehicle are not able to extract the original intelligent vehicle's real identity by analyzing the intercepted messages.

Traceability: The TA has the ability to trace the real identity of an intelligent vehicle, when a target vehicle disputes its signature associated with corresponding encrypted message.

4. Our Anonymous Authentication Scheme with Secure Communication

4.1 Our Construction

In this section, we focus on constructing an anonymous authentication scheme with secure communication in intelligent VANETs from a vehicle equipped with an OBU to a nearby RSU in some sensitive geographic region. There are four phases in the proposed scheme: the system initialization phase, anonymous identity private key generation phase, authenticated encrypted message generation phase, decryption and verification phase. The process of anonymous authentication with secure communication protocol is depicted in **Fig. 3**.

System initialization phase: The TA generates system parameters, and pre-loads them into each vehicle's tamper-proof device and pre-loads them into the RSU as follows.

(1) The TA chooses two large prime numbers p, q, where q is the large prime number factor of $p-1$. The TA chooses a generator α with the prime order q, $1 \le q \le p-1$, such that $\alpha^q \equiv 1 \bmod p$, $\alpha \ne 1$. The TA sets three secure collision-resistance hash functions, $H_1 : Z_p \times Z_p \times \{0,1\}^* \to \{0,1\}^\kappa$, $H_2 : Z_p \times \{0,1\}^\kappa \to Z_q$, $h : Z_p \times \{0,1\}^\kappa \times \{0,1\}^* \times Z_p \to Z_q$.

(2) The TA chooses a random number $x \leftarrow Z_q^*$ as the master secret key, and computes its public key $P_{pub} = \alpha^x \bmod p$. Meanwhile, the RSU chooses a random number $x_{RSU} \leftarrow Z_q^*$ as the private key, and computes its public key $y_{RSU} \equiv \alpha^{x_{RSU}} \bmod p$.

(3) In order to reduce the computational costs of each intelligent vehicle, the TA provides two pre-computing data sets: $VS_{i1} = \{\mu_0, \mu_1, ...\mu_{l_q-1}\}$, where $\mu_j \equiv \alpha^{2^j} \bmod p, 0 \le j \le l_q - 1$, l_q is the bit length of q; $VS_{i2} = \{v_0, v_1, ...v_{l_q-1}\}$, where $v_j \equiv y_{RSU}^{2^j} \bmod p, 0 \le j \le l_q - 1$.

(4) The TA assigns an identity $vRID_i$ and a corresponding login password $vPWD_i$ to each registered intelligent vehicle and pre-loads them into its tamper-proof device.

Finally, the TA broadcasts system public parameters $\{p, q, \alpha, P_{pub}, y_{RSU}\}$ and pre-computing data sets VS_{i1}, VS_{i2} to the RSUs and each intelligent vehicle.

Anonymous identity private key generation phase: In this phase, the TA firstly needs to validate the real identity $vRID_i \in \{0,1\}^\kappa$ and login password $vPWD_i$, which are sent from the intelligent vehicle. Then the TA creates an anonymous identity for $vRID_i$, and generates the corresponding private key as follows.

(1) The TA selects a random number $r_i \leftarrow Z_q^*$, and employs the master secret key x to generate the anonymous identity $vAID_i = \{vAID_{i1}, vAID_{i2}\}$, where:

$$vAID_{i1} = \alpha^{r_i} \bmod p,\ vAID_{i2} = vRID_i \oplus H_1(vAID_{i1}{}^x, P_{pub}, T_i).$$

Here T_i is the term of validity of an anonymous identity.

(2) With the master secret key x, the TA computes the private key of anonymous identity as follows:

$$SK_{vAID_i} = (r_i + x)H_2(vAID_i) \bmod q .$$

Finally, the TA returns the anonymous identity and corresponding private key $\{vAID_i, SK_{vAID_i}, T_i\}$ to the intelligent vehicle via a secure channel.

Authenticated encrypted message generation phase: In this phase, when an intelligent vehicle arrives at some sensitive geographic region, the intelligent vehicle equipped with an OBU_i generates the authenticated encrypted message to a nearby RSU as follows.

(1) With the pre-computing data sets VS_{i1}, VS_{i2}, the intelligent vehicle equipped with an OBU_i selects a random number $k_i \leftarrow Z_q^*$, and combines the ElGamal encryption technique with the fast square-multiply algorithm to encrypt $M \leftarrow Z_p$ as:

$$C_{i1} = \alpha^{k_i} \bmod p,\ C_{i2} = {y_{RSU}}^{k_i} M \bmod p .$$

(2) The intelligent vehicle equipped with an OBU_i computes $C_{i1}' = C_{i1} \bmod q$, and utilizes the private key SK_{vAID_i} to compute:

$$\sigma_i = h_i(vAID_i \,||\, t_i \,||\, M)k_i - SK_{vAID_i} C_{i1}' \bmod q .$$

Here t_i is the current timestamp.

Finally, the intelligent vehicle sends the authenticated encrypted message $\{C_{i1}, C_{i2}, \sigma_i, vAID_i, t_i\}$ to the nearby RSU.

Decryption and verification phase: Once receiving the authenticated encrypted message $\{C_{i1}, C_{i2}, \sigma_i, vAID_i, t_i\}$ from the intelligent OBU_i, the RSU first validates its timestamp t_i and then utilizes its private key x_{RSU} to decrypt the ciphertext C_{i1}, C_{i2} as follows:

$$M = \frac{C_{i2}}{{C_{i1}}^{x_{RSU}}} \bmod p$$

With the message M and the authenticated encrypted message $\{C_{i1}, C_{i2}, \sigma_i, vAID_i, t_i\}$, the RSU computes $C_{i1}' = C_{i1} \bmod q$ and can further verify the validity of signature in the following verification equation:

$${C_{i1}}^{h_i(vAID_i \| t_i \| M)} = \alpha^{\sigma_i} (vAID_i P_{pub})^{H_2(vAID_i)C_{i1}'} \bmod p .$$

If the above equation holds, it means that the signature is valid, the message M can be accepted by the RSU. Otherwise, the message M will be rejected.

4.2 Correctness

For the authenticated encrypted message $\{C_{i1}, C_{i2}, \sigma_i, vAID_i, t_i\}$, with the private key x_{RSU}, the RSU computes as follows:

$$\frac{C_{i2}}{{C_{i1}}^{x_{RSU}}} \bmod p = \frac{{y_{RSU}}^{k_i} M}{(\alpha^{k_i})^{x_{RSU}}} \bmod p = \frac{{y_{RSU}}^{k_i} M}{{y_{RSU}}^{k_i}} \bmod p = M$$

The correctness of the verification equation is elaborated as follows:

$$\alpha^{\sigma_i} = \alpha^{h_i(vAID_i \| t_i \| M)k_i - SK_{vAID_i} C_{i1}^{'} \bmod q} \bmod p$$

$$\alpha^{\sigma_i} = \alpha^{h_i(vAID_i \| t_i \| M)k_i} \alpha^{-SK_{vAID_i} C_{i1}^{'}} \bmod p$$

$$\alpha^{\sigma_i} \alpha^{(r_i + x)\ H_2(vAID_i) C_{i1}^{'}} = \alpha^{h_i(vAID_i \| t_i \| M)k_i} \bmod p$$

$$\alpha^{\sigma_i} (vAID_{i1} P_{pub})^{H_2(vAID_i) C_{i1}^{'}} = C_{i1}^{\ h_i(vAID_i \| t_i \| M)} \bmod p$$

Thus, the equation $C_{i1}^{\ h_i(vAID_i \| t_i \| M)} = \alpha^{\sigma_i} (vAID_i P_{pub})^{H_2(vAID_i) C_{i1}^{'}} \bmod p$ holds.

OBD_i	RSU
$(vRID_i, vPWD_i, vAID_{i1}, SK_{vAID_i}, VS_{i1}, VS_{i2})$	(x_{RSU}, y_{RSU})
$k_i \in Z_q$	
$C_{i1} \leftarrow 1$	
$C_{i2}^{'} \leftarrow 1$	
For $j = l_q - 1$ to 0 do	
If j -th bit of k_i is 1 then	
$C_{i1} \leftarrow C_{i1} \cdot \mu_j \bmod p$	
$C_{i2}^{'} \leftarrow C_{i2}^{'} \cdot \nu_j \bmod p$	
End if	
End for	
$C_{i1}^{'} = C_{i1} \bmod q$	
$C_{i2} = C_{i2}^{'} \cdot M \bmod p$	
$\sigma_i = h_i(vAID_i \| t_i \| M)k_i - SK_{vAID_i} C_{i1}^{'} \bmod q$	
$\{C_{i1}, C_{i2}, \sigma_i, vAID_i, t_i\}$ $\longrightarrow$	
	If T_i is not allowable
	Return 0
	Else
	$M = \frac{C_{i2}}{C_{i1}^{x_{RSU}}} \bmod p$
	If
	$C_{i1}^{\ h_i(vAID_i \| t_i \| M)} = \alpha^{\sigma_i} (vAID_i P_{pub})^{H_2(vAID_i) C_{i1}^{'}} \bmod p$
	Return 1
	Else
	Return 0

Fig. 3. The Process of Anonymous Authentication with Secure Communication

4.3 Batch Verification of Multiple Authenticated Encrypted Messages

Upon receiving n authenticated encrypted messages $\{C_{11}, C_{12}, \sigma_1, vAID_1, t_1\}, ..., \{C_{n1}, C_{n2}, \sigma_n, vAID_n, t_n\}$ from n different $OBD_1, ..., OBD_n$ simultaneously, the RSU employs the private key x_{RSU} and the system public parameters to verify the validity of those authenticated encrypted messages in the following steps.

(1) The RSU first validates each timestamp t_i, where $i = 1, 2, ..., n$. If it is not fresh, the RSU rejects corresponding authenticated encrypted message.

(2) The RSU decrypts each message as $M_i = C_{i2}(C_{i1}^{x_{RSU}})^{-1} \bmod p$, $i = 1, 2, ..., n$.

(3) The RSU randomly choose a vector $\beta = \{\beta_1, \beta_2, ..., \beta_n\}$, where β_i is a small random integer in $[1, 2^{\lambda}]$ and λ is a small integer and has very little computation overhead. Afterwards, the RSU checks whether the following equation holds:

$$\alpha^{\sum_{i=1}^{n}\beta_i\sigma_i}\prod_{i=1}^{n}(vAID_{i1}P_{pub})^{\beta_i H_2(vAID_i)C_{i1}'} = \prod_{i=1}^{n}C_{i1}^{\beta_i h_i(vAID_i\|t_i\|M)} \bmod p .$$

If the verification equation holds, the RSU accepts n authenticated encrypted messages. Otherwise, the RSU rejects them.

Correctness:

For n authenticated encrypted messages $\{C_{11}, C_{12}, \sigma_1, vAID_1, t_1\}, \cdots, \{C_{n1}, C_{n2}, \sigma_n, vAID_n, t_n\}$, the RSU utilizes private key x_{RSU} to decrypt each message as follows:

$$\frac{C_{i2}}{C_{i1}^{x_{RSU}}} \bmod p = \frac{y_{RSU}^{k_i} M}{(\alpha^{k_i})^{x_{RSU}}} \bmod p = \frac{y_{RSU}^{k_i} M}{y_{RSU}^{k_i}} \bmod p = M_i .$$

The correctness of the verification equation is elaborated as follows:

$$\alpha^{\sum_{i=1}^{n}\beta_i\sigma_i} = \alpha^{\sum_{i=1}^{n}\beta_i h_i(vAID_i\|t_i\|M)k_i - \sum_{i=1}^{n}\beta_i SK_{vAID_i}C_{i1}'} \bmod p$$

$$\alpha^{\sum_{i=1}^{n}\beta_i\sigma_i}\alpha^{\sum_{i=1}^{n}\beta_i SK_{vAID_i}C_{i1}'} = \alpha^{\sum_{i=1}^{n}\beta_i h_i(vAID_i\|t_i\|M)k_i} \bmod p$$

$$\alpha^{\sum_{i=1}^{n}\beta_i\sigma_i}\prod_{i=1}^{n}\alpha^{\beta_i(r_i+x)H_2(vAID_i)C_{i1}'} = \prod_{i=1}^{n}C_{i1}^{\beta_i h_i(vAID_i\|t_i\|M)} \bmod p$$

$$\alpha^{\sum_{i=1}^{n}\beta_i\sigma_i}\prod_{i=1}^{n}(vAID_{i1}P_{pub})^{\beta_i H_2(vAID_i)C_{i1}'} = \prod_{i=1}^{n}C_{i1}^{\beta_i h_i(vAID_i\|t_i\|M)} \bmod p$$

5. Security of the Proposed Scheme

5.1.Security Analysis

In this section, we will provide the security analysis of the proposed scheme, and show that it can achieve message confidentiality, message authentication and integrity, identity privacy and traceability, forward security, replay attack and impersonation attack resistance.

Theorem 1. The proposed anonymous authentication scheme with secure communication in intelligent VANETs can achieve message confidentiality.

Proof. In the proposed scheme, the vehicle generates $\{C_{i1}, C_{i2}, \sigma_i, vAID_i, t_i\}$ as the authenticated encrypted message, where $C_{i1} = \alpha^{k_i} \bmod p$, $C_{i2} = y_{RSU}{}^{k_i} M \bmod p$ generated under the public key y_{RSU} of the RSU, the message M is transmitted as ciphertext. Thus, any outside adversary wants to recover the primitive message M, it must need to know the private key of the RSU, such that $M = C_{i2} / C_{i1}^{x_{RSU}} \bmod p$, this is infeasible. Therefore, the proposed scheme can achieve message confidentiality.

Theorem 2. The proposed scheme achieves message authentication and integrity, provided that the hardness of DL (Discrete Logarithm) problem holds.

Proof. In the proposed scheme, since the authenticated encrypted message is $\{C_{i1}, C_{i2}, \sigma_i, vAID_i, t_i\}$, where the signature $\sigma_i = h_i(vAID_i \| t_i \| M)k_i - SK_{vAID_i} C_{i1}^{'} \bmod q$, which is generated under the private key SK_{vAID_i} of the anonymity identity $vAID_i$. By using Forking Lemma [36], here we assume an outside adversary can forge another valid authenticated encrypted message $\{C_{i1}, C_{i2}, \sigma_i^*, vAID_i, t_i\}$ if we repeat the process with a different choice of $h_i(vAID_i \| t_i \| M) \neq h_i^*(vAID_i \| t_i \| M)$, the forged signature $\sigma_i^* = h_i^* k_i - SK_{vAID_i} C_{i1}^{'} \bmod q$, $h_i^* = h_i^*(vAID_i \| t_i \| M)$. In this case, we get the following equation $\alpha^{\sigma_i^*}(vAID_{i1} P_{pub})^{H_2(vAID_i) C_{i1}^{'}} = C_{i1}^{h_i^*} \bmod p$ holds. Since the verification equation $\alpha^{\sigma_i}(vAID_{i1} P_{pub})^{H_2(vAID_i) C_{i1}^{'}} = C_{i1}^{h^*} \bmod p$ holds. According to the two equations, we get that:

$$\alpha^{\sigma_i - \sigma_i^*} = C_{i1}^{h_i - h_i^*} \bmod p$$

Thus $\alpha^{\sigma_i - \sigma_i^*} = \alpha^{k_i (h_i - h_i^*)} \bmod p$ holds. Thereby the adversary can output $(h_i - h_i^*)^{-1}(\sigma_i - \sigma_i^*)$ as the solution of DL problem between α and C_{i1}, it contradicts to the hardness of DL problem. Therefore, the proposed scheme in intelligent VANETs can achieve message authentication and integrity.

Moreover, by applying Forking Lemma [36], we can also prove the message authentication and integrity for batch authenticated encrypted messages. In the same approach, for n authenticated encrypted messages $\{C_{11}, C_{12}, \sigma_1, vAID_1, t_1\}, ..., \{C_{n1}, C_{n2}, \sigma_n, vAID_n, t_n\}$, we also assume an outside adversary can forge at least a valid authenticated encrypted message. For simplicity, here we assume $\{C_{n1}, C_{n2}, \sigma_n^*, vAID_n, t_n\}$ is forged by the outside adversary, if we repeat the process with a different choice of $h_n \neq h_n^*$, $i = 1, ..., n$, the forged signature $\sigma_n^* = h_n^* k_i - SK_{vAID_n} C_{n1}^{'} \bmod q$. In this case, we get the following equation:

$$\alpha^{\sum_{i=1}^{n} \beta_i \sigma_i} \prod_{i=1}^{n} (vAID_{i1} P_{pub})^{\beta_i H_2(vAID_i) C_{i1}^{'}} = \prod_{i=1}^{n} C_{i1}^{\beta_i h_i}$$

Since the following verification equation holds:

$$\alpha^{\sum_{i=1}^{n-1}\beta_i\sigma_i+\beta_n\sigma_n^*}\prod_{i=1}^{n}(vAID_{i1}P_{pub})^{\beta_i H_2(vAID_i)C_{i1}'}=C_{n1}^{\beta_n h_n^*}\prod_{i=1}^{n-1}C_{i1}^{\beta_i h_i}$$

According to the two equations, we get that $\alpha^{\beta_n(\sigma_n^*-\sigma_n)}=\alpha^{k_n\beta_n(h_n^*-h_n)} \bmod p$.

Therefore the adversary can output $(h_n^*-h_n)^{-1}(\sigma_n^*-\sigma_n)$ as the solution of DL problem between α and C_{n1}, it contradicts to the hardness of DL problem. Therefore, the proposed scheme in intelligent VANETs can also achieve message authentication and integrity for batch authenticated encrypted messages.

Theorem 3. The proposed scheme achieves identity privacy, provided that the hardness of CDH (Computational Differ Hellman) problem holds.

Proof. In the proposed scheme, according to the anonymity identity $vAID_i=\{vAID_{i1},vAID_{i2}\}$, Here $vAID_{i1}=\alpha^{r_i} \bmod p$ includes a random secret number r_i which is selected by TA, and $vAID_{i2}=vRID_i\oplus H_1(vAID_{i1}^x,P_{pub},T_i)$ includes the master secret key x of the TA. Thus, without mastering r_i or x, it is infeasible for any malicious adversary to compute $vAID_{i1}^x$ due to the hardness of CDH problem. Therefore, even if an adversary can identify an anonymity identity $vAID_i$, it will not be able to retrieve the real identity information of the intelligent vehicle.

Theorem 4. The proposed anonymous authentication scheme with secure communication in intelligent VANETs can achieve traceability.

Proof. In the proposed scheme, the TA with its master key x can reveal the real identity $vRID_i$ from the anonymity identity $vAID_i=\{vAID_{i1},vAID_{i2}\}$, since it can compute $vRID_i=vAID_{i2}\oplus H_1(vAID_{i1}^x,P_{pub},T_i)$. Thus, if a target intelligent vehicle disputes its signature associated with corresponding authenticated encrypted message, the TA can trace the intelligent vehicle from the dispute signature.

Theorem 5. The proposed anonymous authentication scheme with secure communication in intelligent VANETs can achieve forward security, replay attack and impersonation attack resistance.

Proof. In the proposed scheme, here we consider the key exposure occurs, it means that the adversary can get the private key SK_{vAID_i} of the anonymity identity $vAID_i$, which is valid in term of validity T_i. We also assume that the outside adversary could intercept the authenticated encrypted message $\{C_{i1},C_{i2},\sigma_i,vAID_i,t_i\}$, where $C_{i1}^{'}=C_{i1} \bmod q$, $C_{i2}=y_{RSU}{}^{k_i}M \bmod p$, $\sigma_i=h(vAID_i\|t_i\|M)k_i-SK_{vAID_i}C_{i1}^{'} \bmod q$, and t_i is a valid timestamp. However, an outside adversary cannot determine whether these messages C_{i1},C_{i2},σ_i are transmitted between the intelligent vehicle and the RSU, since it cannot master the random number k_i, or it cannot generate a forged signature σ_i^* in the short timestamp t_i to pass the verification executed by the RSU. Thus the proposed scheme can achieve forward security, the replay attack.

Moreover, without mastering the secret key x of the TA, the adversary cannot recover the real identity $vRID_i$ by computing $vRID_i=vAID_{i2}\oplus H_1(vAID_{i1}^x,P_{pub},T_i)$, it cannot get the real private key SK_{vAID_i} of the $vAID_i$ by interacting with the TA in the register process. Thus,

the adversary cannot generate the authenticated encrypted message $\{C_{i1}, C_{i2}, \sigma_i, vAID_i, t_i\}$ by personating a real intelligent vehicle $vRID_i$. Therefore, the proposed scheme can resist impersonation attack.

5.2 Security Comparison

Now we evaluate the security level in terms of message confidentiality, message authentication, message integrity, impersonation attack resistance, identity privacy, traceability, reply attack resistance, and forward security. The detailed security comparison is listed in **Table 1**. In particular, we get that Maria's scheme [15] cannot achieve message confidentiality, reply attack resistance, or forward security. Neither He's scheme [20] nor Lo's scheme [21] can achieve message confidentiality. While the proposed scheme can achieve all of these security properties simultaneously.

Table 1. Security Comparison

	Maria's scheme	He's scheme	Lo's scheme	Our scheme
Message confidentiality	no	no	no	yes
Message authentication	yes	yes	yes	yes
Message integrity	yes	yes	yes	yes
Identity privacy	yes	yes	yes	yes
Impersonation attack resistance	yes	yes	yes	yes
Traceability	yes	yes	yes	yes
Reply attack resistance	no	yes	yes	yes
Forward security	no	yes	yes	yes

6. Performance Comparison

In this section, we provide an elaborate performance comparison among our anonymous authentication scheme with secure communication in intelligent VANETs and existing schemes [15, 20, 21]. For convenience, we firstly define some notations about the execution time of some cryptographic operations in **Table 2**. In the implementations, the cryptographic operations are run using C programming language on MIRACL of library version is 5.6.1. Our hardware platform consists of an Intel Core (TM) i5-2320 processor with 3.00GHz clock frequency, 8GB memory (7.04GB available) and a Window 10 operating system.

Table 2. Notations

Notation	Description of cryptographic operations
T_{Bp}	the execution time of a bilinear pairing operation
T_{Ex}	the execution time of a modular exponentiation

T_{Mu}	the execution time of a scale multiplication operation $x \cdot P$ related to the ECC, where $x \in Z_q^*$ and $P \in G$
T_{ad}	the execution time of a point addition operation $R + P$ related to the ECC, where $P, R \in G$
T_h	the execution time of a general hash function operation
T_{mu}	the execution time of a general addition operation

6.1 Computational Costs Comparison

We firstly evaluate the comparison of the computational costs, including the signature generation, signature verification, and the computational costs of batch signature verification in **Table 3**. We give the implementation about the execution time for the single signature generation and verification in **Fig. 4**. It can be observed that the proposed scheme takes the lowest computational costs among those schemes to perform signature generation and verification process. Furthermore, we also give the implementation about the execution time for batch verification of multiple messages in **Fig. 5**. The implementation comparison result shows that with the growth of the number of messages, the proposed scheme is much more efficient and takes the lowest verification time compared with existing the schemes. This is mainly because the proposed scheme does not need time-consuming bilinear pairing operations.

Table 3. Computational Costs Comparison

	Signature generation	Signature verification	n Signature batch verification
[15]	$7T_{Ex} + 2T_h + 3T_{mu} = 8.2083(ms)$	$2T_{Bp} + 7T_{Ex} + 2T_h + 6T_{mu} = 19.0650(ms)$	$(n+1)T_{Bp} + (2n+6)T_{Ex} + (2n+1)T_h + 2(n+1)T_{mu} = 7.7844n + 12.4566(ms)$
[20]	$3T_{Mu} + 3T_h = 6.5190(ms)$	$3T_{Mu} + 2T_{ad} + 2T_h = 6.5376(ms)$	$(2n+2)T_{Mu} + (2n-1)T_{ad} + 2nT_h + 3nT_{mu} = 4.3751n + 4.3172(ms)$
[21]	$T_{Mu} + T_h + T_{mu} = 2.1739(ms)$	$3T_{Mu} + 2T_{ad} + 2T_h = 6.5376(ms)$	$(2n+2)T_{Mu} + 2nT_{ad} + 2nT_h + 3nT_{mu} = 4.3751n + 4.3304(ms)$
Our scheme	$2T_{Ex} + T_h + 2T_{mu} = 2.3496(ms)$	$4T_{Ex} + 2T_h + 5T_{mu} = 4.7001(ms)$	$(3n+1)T_{Ex} + 2nT_h + 8nT_{mu} = 3.5328n + 1.1700(ms)$

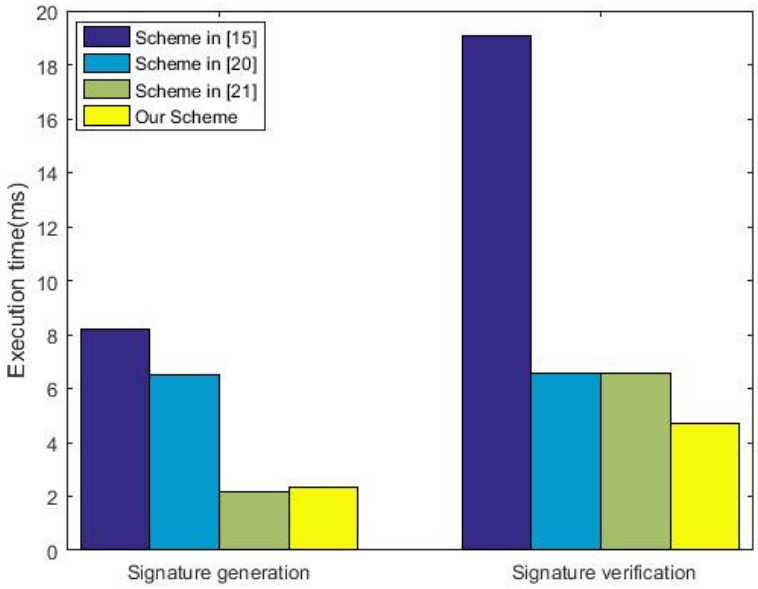

Fig. 4. Execution Time for the Single Generation and Verification

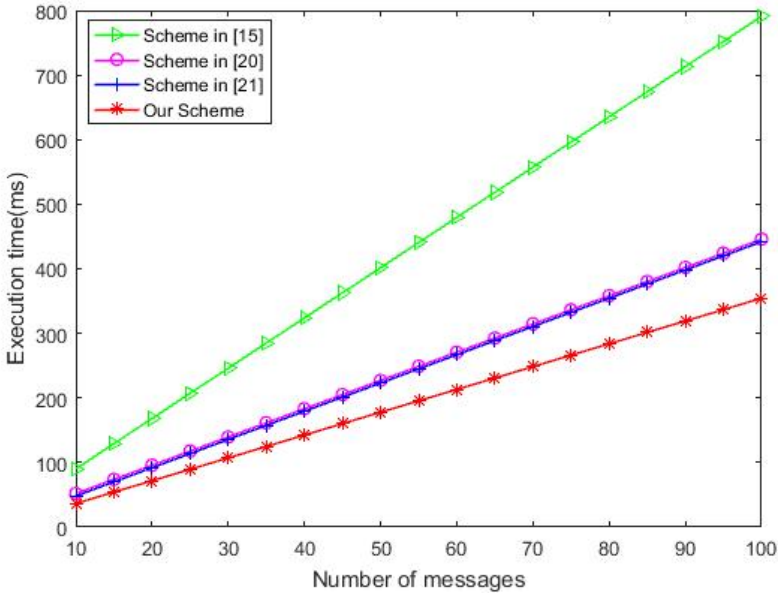

Fig. 5. Execution Time for Batch Verification of Multiple Messages

6.2 Communication Overhead Comparison

Now we compare the proposed scheme with existing schemes [15, 20, 21] in terms of communication overhead. We denote $|G|$ by the length of an element in a cyclic group G based on an elliptic curve, denote $|p|,|q|$ by the length of an element in Z_p, Z_q, respectively.

We also denote ξ by the fixed length of a general hash function value, denote ζ by the fixed length of a timestamp. The detailed communication overhead comparison is listed in **Table 4**. Furthermore, we implement the communication overhead of sending a single authenticated message in **Fig. 6**. To ensure the security of all the schemes, we set $|p|$ and $|q|$ to be 128bytes and 20bytes, respectively, we also set the length of an element in G to be 128bytes. For simplicity, we set the fixed length of a general hash function value and a timestamp to be 16bytes and 4bytes, respectively. **Fig 6** shows that the proposed scheme owns much lower communication overhead compared with existing schemes.

Table 4. Communication Overhead Comparison

	Sending a single authenticated message	Sending n authenticated messages
[15]	$11\|G\|$	$11n\|G\|$
[20]	$3\|G\|+2\|q\|+\zeta$	$3n\|G\|+2n\|q\|+n\zeta$
[21]	$4\|G\|+2\|q\|+\zeta$	$4n\|G\|+2n\|q\|+n\zeta$
Our Scheme	$3\|G\|+\|q\|+\xi+\zeta$	$3n\|G\|+n\|q\|+n\xi+n\zeta$

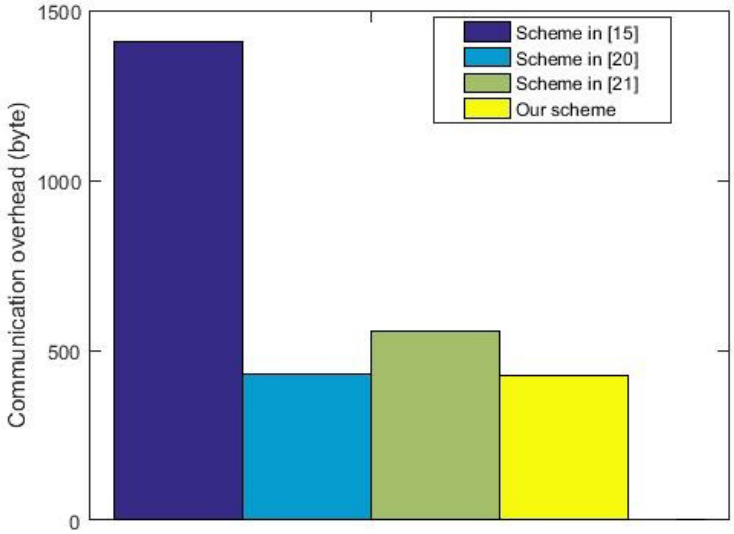

Fig. 6. The Comparison of Communication Overhead

7. Conclusions

In this paper, we have proposed an efficient anonymous authentication scheme with secure communication in intelligent VANETs. The proposed scheme enables a legitimate vehicle to anonymously send an authenticated message to a nearby RSU, and it achieves message confidentiality, forward security, and reply attack resistance simultaneously. In particular, except the trusted authority (TA), any outside entity cannot trace the real identity of an intelligent vehicle in case of disputes. Moreover, the proposed scheme is designed on an

identity-based cryptographic system, which can remove the costs of establishing public key infrastructure (PKI) and certificates management. Compared with existing schemes, the proposed scheme is much more efficient, since it does not need time-consuming bilinear pairing operations, and it also owns much lower communication overhead. Thus, the proposed scheme is much more practical in intelligent VANETs. In our future work, we will further investigate how to construct a new anonymous authentication scheme with secure communication, which can be well deployed both in vehicle-to-RSU (V2R) and vehicle-to vehicle (V2V) communication model of intelligent VANETs.

Acknowledgements

This work is supported by National Key R&D Program of China (No.2017YFB0802000), National Natural Science Foundation of China (No.61872060), China Postdoctoral Science Foundation Funded Project (No.2017M623008), Sichuan Science and Technology Program (No. 2018GZ0102), Scientific Research Starting Project of SWPU (No.2017QHZ023).

References

[1] S. Zeadally, R. Hun, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETs): Status, results, and challenges," *Telecommunication Systems*, vol. 50(4), pp. 217-241, 2012. Article(CrossRef Link).

[2] M. Ghosh, A. Varghese, A. Gupta, A. A. Kherani, and S. N. Muthaiah, " Detecting misbehaviors in VANET with integrated root-cause analysis," *Ad Hoc Networks*, vol. 8(7), pp. 778–790, 2010. Article(CrossRef Link).

[3] Y. Toor, P. Muhlethaler, and A. Laouiti, "Vehicle ad hoc networks: Applications and related technical issues," *IEEE Communications Surveys & Tutorials*, vol. 10(3), pp. 74–88, 2008. Article(CrossRef Link).

[4] J. A. Misener, "Vehicle-infrastructure integration (VII) and safety: Rubber and radio meets the road in California," *Intellimotion*, vol. 11(2), pp. 1–3, 2005. Article(CrossRef Link).

[5] R. Lu, X. Lin, T. H. Luan, X. Liang, and X.S. Shen, "Anonymity analysis on social spot based pseudonym changing for location privacy in VANETs," in *Proc. of IEEE ICC*, pp. 1–5, 2011. Article(CrossRef Link).

[6] X. Lin, R. Lu, C. Zhang, H. Zhu, P. H. Ho, and X. Shen, "Security in vehicular ad hoc networks," *IEEE Communications Magazine*, vol. 46(4), pp. 88–95, 2008. Article(CrossRef Link).

[7] M. Azees, P. Vijayakumar, and L. J. Deborah, "Comprehensive survey on security services in vehicular ad-hoc networks," *Iet Intelligent Transport Systems*, vol. 10(6), pp. 379-388, 2016. Article(CrossRef Link).

[8] Y. Zhang, C. Xu, H. Li, K. Yang, J. Zhou, X. Lin, "HealthDep: An efficient and secure deduplication scheme for cloud-assisted eHealth systems," in *Proc. of IEEE Transactions on Industrial Informatics*, pp. 1-1, 2018. Article(CrossRef Link).

[9] Y. Zhang, C. Xu, X. Liang, H. Li, Y. Mu, X. Zhang, "Efficient public verification of data integrity for cloud storage systems from indistinguishability obfuscation," *IEEE Transactions on Information Forensics & Security*, vol. 12(3), pp. 676-688, 2017. Article(CrossRef Link).

[10] M. Raya, P. Papadimitratos, and J.P. Hubaux, "Securing vehicular communications," *IEEE Wireless Communications*, vol. 13(5), pp. 8-15, 2006. Article(CrossRef Link).

[11] R. Lu, X. Lin, H. Zhu, P.H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. of IEEE INFOCOM*, pp. 1229-1237, 2008. Article(CrossRef Link).

[12] J. Freudiger, M. Raya, M. Felegyhazi, P. Papadimitratos, and J.-P. Hubaux, "Mix-zones for location privacy in vehicular networks," in *Proc. of In WiN-ITS 07*, 2007. Article(CrossRef Link).

[13] C. Zhang, X. Lin, R. Lu, and P. H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in *Proc. of IEEE International Conference on Communications, IEEE*, pp. 1451-1457, 2008. Article(CrossRef Link).

[14] D. Huang, S. Misra, M. Verma, and G. Xue, "PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12(3), pp. 736-746, 2011. Article(CrossRef Link).

[15] M. Azees, P. Vijayakumar, L. J. Deboarh, "EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad-hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18(9), pp. 2467-2476, 2017. Article(CrossRef Link).

[16] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. of Advances in cryptology-CRYPTO*, pp. 47-53, 1984. Article(CrossRef Link).

[17] C. Zhang, R. Lu, X. Lin, P.H. Ho, and X. Shen, "An efficient identity based batch verification scheme for vehicular sensor networks," in *Proc. of IEEE INFOCOM*, pp. 246-250, 2008. Article(CrossRef Link).

[18] C. Zhang, P. H. Ho, and J. Tapolcai, "On batch verification with group testing for vehicular communications," *Wireless Networks*, vol. 17(8), pp. 1851-1865, 2011. Article(CrossRef Link).

[19] S. Biswas, J. Misic, and V. Misic, "ID-based safety message authentication for security and trust in vehicular networks," in *Proc. of International Conference on Distributed Computing Systems Workshops, IEEE Computer Society*, pp. 323-331, 2011. Article(CrossRef Link).

[20] D. He, S. Zeadally, B. Xu, X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad-hoc networks," *IEEE Transactions on Information Forensics & Security*, vol. 10(12), pp. 2681-2691, 2015. Article(CrossRef Link).

[21] N. W. Lo, J. L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Transactions on Intelligent Transportation Systems*, 2016, vol. 17(5), pp. 1319-1328. Article(CrossRef Link).

[22] T. Elgamal. "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Proc. of Workshop on the Theory and Application of Cryptographic Techniques*, pp. 10-18, 1984. Article(CrossRef Link).

[23] C. P. Schnorr, "Efficient signature generation by smart cards. Journal of Cryptology," vol. 4(3), pp. 161-174, 1991. Article(CrossRef Link).

[24] X. Lin, X. Sun, P. H. Ho, and X. Shen, "GSIS: A secure and privacypreserving protocol for vehicular communications," in *Proc. of IEEE Transactions on Vehicular Technology*, vol. 56(6), pp. 3442-3456, 2007. Article(CrossRef Link).

[25] S. Gupta, M. Chakraborty, "TACKing together efficient authentication, revocation, and privacy in VANETs," in *Proc. of IEEE Communications Society Conference on IEEE*, pp. 1-9, 2008. Article(CrossRef Link).

[26] H. A. Man, J. K. Liu, Z. Zhang, W. Susilo, J. Li, J. Zhou, "Anonymous announcement system (AAS) for electric vehicle in VANETs," *Computer Journal*, vol. 60(4), pp. 588-599, 2018.

[27] C. C. Lee and Y. M. Lai, "Toward a secure batch verification with group testing for VANET," *Wireless Networks*, vol. 19(6), pp. 1441-1449, 2013. Article(CrossRef Link).

[28] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs," *Ad Hoc Networks*, vol. 9(2), pp. 189-203, 2011. Article(CrossRef Link).

[29] J. Zhang, M. Xu, and L. Liu, "On the security of a secure batch verification with group testing for VANET," *International Journal of Network Security*, vol. 16(5), pp. 355-362, 2014. Article(CrossRef Link).

[30] X. Zhang, H. Wang, C. Xu, "Identity-based key-exposure resilient cloud storage public auditing scheme from lattices," *Information Sciences*, vol. 472, pp. 223-234, 2019. Article(CrossRef Link).

[31] S. Biswas and J. Mišić, "A cross-layer approach to privacy-preserving authentication in WAVE-enabled VANETs," *IEEE Transactions on Vehicular Technology*, vol. 62(5), pp. 2182-2192, 2013. Article(CrossRef Link).

[32] K. A. Shim, "CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 61(4), pp. 1874-1883, 2012. Article(CrossRef Link).

[33] S. J. Horng, S. F. Tzeng, Y. Pan, P. Z. Fan, X. Wang, T. R. Li, M. K. Khan, "b-SPECS+: Batch verification for secure pseudonymous authentication in VANET," *IEEE Transactions on Information Forensics & Security*, vol. 8(11), pp. 1860-1875, 2013. Article(CrossRef Link).

[34] M. R. Asaar, M. Salmasizadeh, W. Susilo, A. Majidi, "A secure and efficient authentication technique for vehicular Ad-Hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 67(6), pp. 5409-5423, 2018. Article(CrossRef Link).

[35] Y. Ming, X. Shen, "PCPA: a practical certificateless conditional privacy-preserving authentication scheme for vehicular ad-hoc networks," *Sensors*, vol. 18(5), pp. 1573, 2018. Article(CrossRef Link).

[36] D. Pointcheval, J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13(3), pp. 361-396, 2000. Article(CrossRef Link).

Xiaojun Zhang, received the B.S. degree in mathematics and applied mathematics from Hebei Normal University in 2009 and received M.S. degree in pure mathematics from Guangxi University in 2012. He received Ph.D. degree in infor- mation security at University of Electronic Science Technology of China in 2015. He is a lecturer in the School of Computer Science, Southwest Petroleum University, he also works as a Postdoctoral Fellow at University of Electronic Science Technology of China from 2016. He is now presently engaging in cryptography, network security and cloud computing security. (Email: zhangxjdzkd2012@163.com)

Liming Mu received the B.S. degree in network engineering from Chengdu Technological University in 2017. He is currently a postgraduate student for M.S. degree in computer science and technology, in the School of Computer Science, Southwest Petroleum University. He is now presently engaging in cryptography, network security, cloud computing security and big data security. (Email: mulming@163.com)

Jie Zhao received the B.S. degree in network engineering from Southwest Petroleum University in 2017. He is currently a postgraduate student for M.S. degree in computer science and technology, in the School of Computer Science, Southwest Petroleum University. He is now presently engaging in cryptography, network security, cloud computing security and big data security. (Email: zhaojswpu2017@163.com)

Chunxiang Xu received her B.Sc., M.Sc. and Ph.D. degrees at Xidian University, in 1985, 1988 and 2004 respectively, P.R.C. She is presently engaged in information security, cloud computing security and cryptography as a professor at University of Electronic Science Technology of China (UESTC). She is now presently engaging in cryptography, cloud computing security. (Email: chxxu@uestc.edu.cn)