An Efficient Revocable Group Signature Scheme in Vehicular Ad Hoc Networks

Zhen Zhao[1], Jie Chen[1], Yueyu Zhang[1,2] and Lanjun Dang[1]
[1] State Key Laboratory of Integrated Service Networks, Xidian University
Xi'an, Shaanxi, 710071, China
[e-mail: zhaozhenbeyond@163.com; jchen@mail.xidian.edu.cn; yyzhang@xidian.edu.cn; ljdang@mail.xidian.edu.cn]
[2] Department of ECE, Michigan State University
East Lansing, MI 48824, USA
[e-mail: yueyu@msu.edu]
*Corresponding author: Jie Chen

Received May 12, 2015; revised July 26, 2015; accepted August 23, 2015; published October 31, 2015

Abstract

Although many revocable group signature schemes has been proposed in vehicular ad hoc networks (VANETs), the existing schemes suffer from long computation delay on revocation that they cannot adapt to the dynamic VANETs. Based on Chinese remainder theorem and Schnorr signature algorithm, this paper proposes an efficient revocable group signature scheme in VANETs. In the proposed scheme, it only need to update the corresponding group public key when a member quits the group, and in the meanwhile the key pairs of unchanged group members are not influenced. Furthermore, this scheme can achieve privacy protection by making use of blind certificates. Before joining to the VANETs, users register at local trusted agencies (LTAs) with their ID cards to obtain blind certificates. The blind certificate will be submitted to road-side units (RSUs) to verify the legality of users. Thus, the real identities of users can be protected. In addition, if there is a dispute, users can combine to submit open applications to RSUs against a disputed member. And LTAs can determine the real identity of the disputed member. Moreover, since the key pairs employed by a user are different in different groups, attackers are not able to track the movement of users with the obtained public keys in a group. Furthermore, performance analysis shows that proposed scheme has less computation cost than existing schemes.

Keywords: vehicular ad hoc networks (VANETs), group signature, Chinese remainder theorem, Schnorr signature algorithm, blind certificates.

This work was supported by the Natural Science Foundation of China (61102056, 61201132, 61402351), Fundamental Research Funds for the Central Universities of China (K5051301013) and the 111 Project of China (B08038).

http://dx.doi.org/10.3837/tiis.2015.10.027 **ISSN : 1976-7277**

1. Introduction

Due to the extraordinary commercial and social potential, VANETs have been paid more and more attention. VANETs were first proposed at ITU-T standardization in 2003[1]. VANETs are a type of Mobile Ad-hoc Network (MANET) which is the next-generation networking technology to provide communication between vehicles (V2V) or between a vehicle and infrastructure (V2I) using wireless communication. VANETs are aimed to solve problems that traffic congestion and safety etc. In VANETs, moving vehicles send and receive all sorts of messages, such as front brakes, rear-end collision warnings, detailed information of the weather, traffic congestion, and accident rescue information and so on, so that the vehicles on the road can choose a more efficient route and avoid many accidents. However, it would also lead to a threat for the moving vehicle's privacy when it transmits or receives different types of messages on the road in VANETs, as its communication can be used to link its identity to its physical entity. There are many researches on security and privacy-preserving authentication in VANETs [2]-[4]. Anonymous authentication is one of promising solutions for privacy-preserving scheme, which usually can be achieved by applying pseudonym and group signature [5].

In pseudonym scheme, the real identity of a user can be hidden with the pseudonymous communication. And a Trusted Authority (TA) is required to issue the pseudonym to each member and record the corresponding real identity. In VANETs, many existing authentication schemes apply the pseudonym for anonymity [6]-[10]. However, if a member employs only one pseudonym in VANETs, attackers can obtain the complete route of the member and its ordered services in driving then attackers can deduce the real identity of the member. In [11], Beresford has experimental proved that a single pseudonym cannot meet privacy-preserving because attackers are able to trace the public information of users. Therefore, pseudonym should be updated at regular intervals [12]-[14]. However, with the increase of vehicles, the management and maintenance of pseudonym would be a bottleneck of anonymous authentication in VANETs, and regular replacement of pseudonym would effect on routing efficiency and increase packet loss.

Group signature means that each group member is capable of signing messages representing the group, and anyone can authenticate the signed messages with the group public key while the verifier cannot determine which group member is the signer. Moreover, if there is a dispute, group manager can identify the signer. Group signatures are widely used in VANETs to realize anonymous authentication with privacy-preserving authentication [15]-[19]. In order to improve the efficiency of schemes based on group signatures in VANETs, a great quantity of researches have been proposed[20]-[28]. In VANETs, Road Side Units (RSUs) generate groups within their ambit. Owing to the frequent and high speed joining and leaving of vehicles in VANETs, the schemes based on group signatures in VANETs should be able to achieve efficient joining and revocation of group members. In addition, efficient joining has been achieved in most existing schemes [15]-[28], in which RSUs generate key pairs for the new group member and broadcast a new group public key. However, efficient revocation is still a difficult problem for the existing schemes [15],[16],[24]-[27]. In existing schemes based on group signatures in VANETs[16],[24],[26],[27], the key pairs of other group members will be influenced when a member quits the group, which makes excessive traffic load and does not meet the requirements of dynamic VANETs. In this paper, an efficient revocable group signature scheme in VANETs is proposed. If there is a revocation in the group, the key pairs of unrevoked group members are not influenced, and the key pair and certificate of the revoked member are no longer valid. Furthermore, the proposed scheme keeps the forward and

backward security, and it is anti-collusion.

The remainder of paper is organized as follows: Section 2 gives system model and preliminaries of this paper. Section 3 describes the proposed scheme in detail. Section 4 presents security analysis of the scheme and the comparison with the other two revocable schemes. Section 5 makes a conclusion.

2. SYSTEM MODEL AND PRELIMINARIES

2.1 System Model

In this paper, the system model of VANETs consists of a GTA, LTAs, fixed RSUs at the road side, and mobile BVs equipped in vehicles, as shown in **Fig. 1**.

• GTA is a general trusted agency of VANETs. It provides management and generates public/private key pairs for LTAs. As usual, GTA is assumed as powerful enough in terms of communication, computation, and storage capability, and it is unworkable to compromise to any adversary.

• LTAs are local trusted agencies. Suppose that there are I LTAs in the jurisdictional limits of GTA. LTAs generate public/private key pairs for RSUs. In addition, BVs register at the LTA which they belong to before joining VANETs. LTAs issue blind certificates to legal BVs. Then, LTAs are also assumed as powerful enough for communication, computation, and storage capability, and they are infeasible to compromise to any adversary.

• RSUs work as the group manager in groups consisting of BVs. Assume that there are J RSUs in the jurisdictional limits of a LTA. RSUs generate the group public key and update it if there is a join or quit of BVs. They are also responsible for distributing public key materials to BVs in the groups. In this paper, RSUs are assumed to be semi-trust, which means honest but curious, honest for performing operation but curious about real identities of BVs.

• BVs represent vehicle users. They register at the LTA which they attribute to before joining VANETs. They are able to broadcast and receive signed messages in groups. Each vehicle is assumed to have a tamper-proof device (TPD) to store security-related materials. In this paper, it is supposed that each vehicle is uniquely identified by its battery.

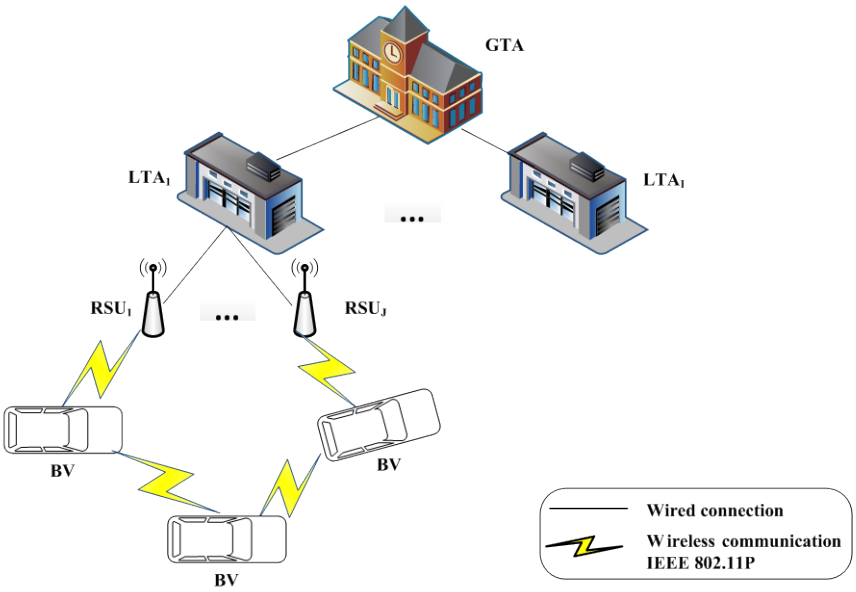

Fig. 1. System Model of VANETs

2.2 Chinese Remainder Theorem

If $p_1, p_2, \cdots, p_k$ are pairwise coprime, where $k \geq 2$, set $P = p_1 p_2 \cdots p_k = p_1 P_1 = p_2 P_2 = \cdots = p_k P_k$, where $P_i = \frac{P}{p_i}, i = 1,2,\cdots,k$. Then the positive integer value of the congruence equations (1) is $c \equiv \sum_{i=1}^{k} y_i P_i P_i^{'} \equiv y_1 P_1^{'} P_1 + y_2 P_2^{'} P_2 + \cdots + y_k P_k^{'} P_k \left(mod\ P\right)$, where $P_i^{'}$ is positive integer and meets the congruence equation $P_i^{'} P_i \equiv 1 (\text{mod } p_i), i = 1,2,\cdots,k$.

$$\begin{cases} c \equiv y_1 (\text{mod } p_1) \\ c \equiv y_2 (\text{mod } p_2) \\ \quad \cdots\cdots \\ c \equiv y_k (\text{mod } p_k) \end{cases} \tag{1}$$

2.3 Hash Function

Hash function is defined as $h: \{0,1\}^* \rightarrow \{0,1\}^n$, where $\{0,1\}^*$ denotes a bit string of arbitrary length, $\{0, 1\}^n$ indicates a string of length with *n*. A one-way hash function is considered to be secure if it satisfies the following properties.

(1) Given x, it is easy to calculate $h(x) = y$. While conversely, given $y = h(x)$, it is hard to compute x.

(2) Given x, it is computationally unworkable to find $x \neq x^{'}$ such that $h(x^{'}) = h(x)$.

2.4 Bilinear Parings

In this paper, the properties of the bilinear operation are defined as follows: G_1 represents an additive cyclic group with order q, G_2 represents a multiplicative cyclic group with the same order, $e: G_1 \times G_1 \rightarrow G_2$ is a bilinear map, which meets the following requirements:

(1) Bilinearity: $\forall R, S, T \in G_1$, there are $e(R, S+T) = e(R,S)e(R,T)$, $e(R+S,T) = e(R,T)e(S,T)$;

(2) Nondegenerative: $\exists R, S \in G_1$, satisfies $e(R,S) \neq 1$;

(3) Computability: $\forall R, S \in G_1$, $e(R,S)$ is computable in polynomial time.

2.5 Notations

There are some symbols mentioned below as **Table 1**.

Table 1. Symbols and Meaning

Symbols	Meaning
V_k	the k^{th} vehicle user
ID_x	the real identity of an entity *x* in VANETs
Q_x / Γ_x	the ID-based public/private key pair of BV *x* corresponding to its real identity ID_x
$SIG_{\Gamma_x}(M)$	the ID-based signature on a message M using the ID-based private key Γ_x of signer *x*
$SYM_k(M)$	the symmetric key encryption on message M using the shared secret key k

$HMAC_k(M)$	a hash-based message authentication code on message M using the shared secret key k

3. PROPOSED SCHEME

3.1. Initialization

(1) Above all, GTA generates its own public/private key pair making use of RSA algorithm. According to RSA algorithm, GTA chooses

• random primes b, c such that $b \geq 2^{512}, c \geq 2^{512}$, let $n = b \times c$;

• a random number $e < \varphi(n)$ as its own public key, where $\varphi(n) = (b-1) \cdot (c-1)$, and $\gcd(e, \varphi(n)) = 1$;

Then GTA computes d as its private key, which satisfies $e \cdot d \equiv 1 (\mathrm{mod}\, \varphi(n))$.

GTA publishes the public parameters (e, n), and keeps (b, c, d) secret.

(2) GTA generates parameters for LTAs using RSA algorithm. For LTA_i, where $1 \leq i \leq I$, GTA chooses

• random primes b_i, c_i such that $b_i \geq 2^{512}, c_i \geq 2^{512}$, let $n_i = b_i \times c_i$;

• a random number $e_i < \varphi(n_i)$ as the public key of LTA_i, where $\varphi(n_i) = (b_i - 1) \cdot (c_i - 1)$, and $\gcd(e_i, \varphi(n_i)) = 1$;

• a random number g_i as the identity code of LTA_i;

GTA computes d_i as the private key of LTA_i, which satisfies $e_i \cdot d_i \equiv 1 (\mathrm{mod}\, \varphi(n_i))$.

Then GTA safely sends the parameters to LTA_i. LTA_i publishes (e_i, n_i, g_i) as its public parameters, and secretly save the tuple (b_i, c_i, d_i).

(3) LTA generates key pairs for RSU_i, where $1 \leq i \leq J$, LTA chooses

• random primes s_i, t_i such that $s_i \geq 2^{512}, t_i \geq 2^{512}$, let $m_i = s_i \times t_i$;

• a random number $u_i < \varphi(m_i)$ as the public key of RSU_i, where $\varphi(m_i) = (s_i - 1) \cdot (t_i - 1)$, and $\gcd(u_i, \varphi(m_i)) = 1$;

Then LTA computes v_i as the private key of RSU_i, which satisfies $u_i \cdot v_i \equiv 1 (\mathrm{mod}\, \varphi(m_i))$. After receiving of these parameters, RSU_i publishes its public parameters (u_i, m_i), and keeps (s_i, t_i, v_i) secret.

3.2. Registration

Before accessing to VANETs, a user should register at the LTA which it belongs to for getting a blind certificate, which will be submitted to RSUs to prove its legitimacy without disclosing its real identity. In reality, ID cards are used to complete registration. ID-based restrictive partially blind signature technique [29] had been combined to generate *permit* in [30]. In this paper, we also adopt the *permit* to generate blind certificates as **Fig. 2**. Suppose the BV registers at LTA_1. LTA_1 chooses 3 random generators $R, R_1, R_2 \in G_1$.

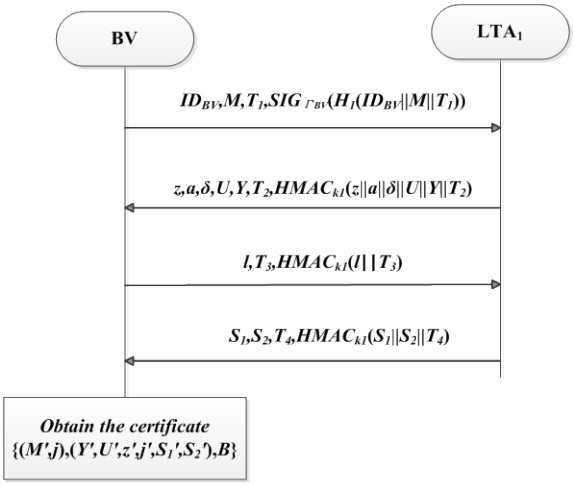

Fig. 2. Certificate Generation

(1) BV randomly generates a number ξ_{BV} and computes $M = A_{BV} = \xi_{BV} R_1 + R_2$, $\rho = e(R, Q_{LTA_1})$, $\rho_1 = e(R_1, Q_{LTA_1})$, $\rho_2 = e(R_2, Q_{LTA_1})$ and $y = e(P_{pub}, Q_{LTA_1})$. Then BV sends $ID_{BV}, M, T_1, SIG_{\Gamma_{BV}}\left(H_1\left(ID_{BV} \| M \| T_1\right)\right)$ to LTA$_1$.

(2) LTA$_1$ randomly chooses $Q \in G_1$ and $r \in Z_q^*$, and computes $z = e(M, \Gamma_{LTA_1})$, $a = e(R, Q)$, $\delta = e(M, Q)$, U=rR and $Y = rQ_{LTA_1}$. Then LTA$_1$ sends z, a, δ, U, Y, T_2, $HMAC_{k1}\left(z \| a \| \delta \| U \| Y \| T_2\right)$ to BV.

(3) BV randomly chooses $\alpha, \beta, \gamma, \lambda, \mu, \sigma, u, v \in Z_q^*$, and computes $M' = \alpha M$, $A = e\left(M', Q_{LTA_1}\right)$, $B = \rho_1^{\beta} \rho_2^{\sigma}$, $\delta' = \delta^{u\alpha} A^{v}$, $z' = z^{\alpha}$, $a' = a^{u} \rho^{v}$, $Y' = \lambda Y + \lambda\mu Q_{LTA_1} - \gamma H_1(j)$, $U' = \lambda U + \gamma P_{pub}$, $l = \lambda^{-1} H_2(M', Y', U', A, B, z', a', \delta') + \mu$, $j' = lu$ and $k_1 = e(\Gamma_{BV}, Q_{LTA_1})$. Then BV sends $l, T_3, HMAC_{k1}(l \| T_3)$ to LTA$_1$.

(4) LTA computes $S_1 = Q + l\Gamma_{LTA_1}$, $S_2 = (r + l)\Gamma_{LTA_1} + rH_1(j)$ and sends $S_1, S_2, T_4, HMAC_{k1}(S_1 \| S_2 \| T_4)$ to BV.

(5) If the equations hold with $e(R, S_1) = ay^l$, $e(M, S_1) = \delta z^l$, BV computes $S_1' = uS_1 + VQ_{LTA_1}$, $S_2' = \alpha S_2$. The restrictive partially blind signature on (M', j) is $(Y', U', z', j', S_1', S_2')$ and the requested blind certificate is $\left\{(M', j), (Y', U', z', j', S_1', S_2'), B\right\}$, where B will be used in the verification of the certificate.

The blind certificates can protect the privacy of users and prevent the users' real identity from revealing on the move. Thus a secure drive is successfully established for users in terms of communication.

The scheme defines j to be the expiration time of the certificates, T_i to be a precise timestamp for preventing replay attack.

3.3. Groups Establishment

RSUs establish groups consisting of BVs in their corresponding area. In this paper, Chinese remainder theorem is utilized to generate group public keys. Upon the public keys of group members, a RSU generates a group public key. Any user can authenticate signed messages with the group public key. If there is a join or quit for users, RSU will update the group public key using Chinese remainder theorem. Moreover, RSU need not to change the key pairs of other unchanged efficient group members when RSU adds or deletes a member in the group. That is, whether there is a join or quit, the key pairs of old members in the group are unaffected. For greater security, Schnorr signature algorithm is applied in this paper. As a result, it is high-speed on updating in groups and secure on protecting the privacy of users.

It is assumed that the establishment occurs at RSU_1 and there are s vehicle users in the original time.

(1) RSU_1: User V_i submits its request and blind certificate to RSU_1, where $1 \le i \le s$. That is, there are s vehicles and V_i represents the i^{th} member. RSU_1 verifies the validity of the blind certificate above all. The verification process is as **Fig. 3**.

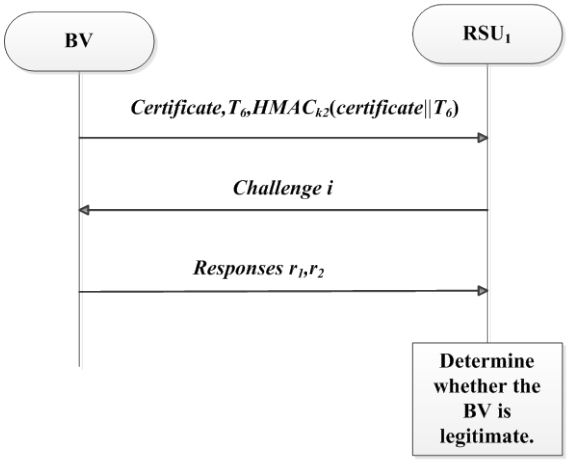

Fig. 3. Certificate Authentication

(1.1) BV sends $certificate, T_6, HMAC_{k2}(certificate \| T_6)$ to RSU_1.

(1.2) RSU_1 computes $A = e(M', Q_{LTA1})$. If $A \neq 0$, computes $i = H_4(A, B, Q_{RSU1}, time)$, where $time$ is the binary representation of the current time. RSU_1 sends the challenge i to BV.

(1.3) BV computes $r_1 = i(\xi_x \alpha) + \beta$ and $r_2 = i\alpha + \sigma$. Then BV sends r_1, r_2 to RSU_1.

(1.4) RSU_1 computes $a' = e(P, S_1')y^{-j'}$ and $\delta' = e(M', S_1')z^{i-j'}$. The signature is valid if $e(S_2', R) = e(Y' + H_3(M', Y', U', A, z', a', \delta')Q_{LTA1}, P_{pub}) \times e(H_1(j), U')$ holds. RSU_1 accepts this certificate if and only if $\rho_1^{r_1}\rho_2^{r_2} = A^i B$.

If the certificate is valid and not expired, the verification is successful. Therefore, RSU_1 allows V_i joining to the group and stores its blind certificate into database, $1 \le i \le s$.

(2) $RSU_1 \to V_i$: After confirming the validity of the presented certificate, RSU_1 generates key materials for vehicle user V_i based on Schonorr signature algorithm. RSU_1 randomly selects primes p_i, q_i, where $q_i \mid p_i - 1, p_i \geq 2^{512}, q_i \geq 2^{160}$, and $p_i \geq g_1$, g_1 is the identity code of LTA_1. After which, RSU_1 sends the tuple $(g_1, p_i, q_i, p_i^{v_1}, q_i^{v_1})$ to V_i in a secure environment, where v_1 is the private key of RSU_1.

(3) V_i: After receiving the parameters from RSU_1, V_i primarily verifies its legality. If the equations $(p_i^{v_1})^{u_1} \equiv p_i (\text{mod } m_1), (q_i^{v_1})^{u_1} \equiv q_i (\text{mod } m_1)$ are satisfied, V_i believes the parameters are valid and produced by RSU_1, where u_1 is the public key of RSU_1, m_1 is the public parameter of RSU_1. V_i will product its own public/private key pair employing the key materials as step (4).

(4) $V_i \to RSU_1$: V_i randomly selects $x_i \in z_{p_i}^*$ as its private key, and computes $y_i = g_1^{x_i} (\text{mod } p_i)$ as its public key. Then, V_i sends y_i to RSU_1 via a secure channel, such as a Secure Socket Layer.

(5) RSU_1: RSU_1 reserves the public key of all group members with their corresponding blind certificate in database and public **Table 2**.

Table 2. The Public Keys of the Existing Group Members

The public key	y_1	y_2	…	y_i	…	y_s

For member V_i, RSU_1 transmits (y_i, *certification*) to LTA_1 via a secure channel. LTA_1 stores (y_i, *certification*) in its reserve.

(6) RSU_1 generates the group public key. Taking advantage of the obtained public keys of s members, RSU_1 computes the group key according to the congruence equations (2).

$$\begin{cases} c \equiv y_1 (\text{mod } p_1) \\ \quad \cdots\cdots \\ c \equiv y_i (\text{mod } p_i) \\ \quad \cdots\cdots \\ c \equiv y_s (\text{mod } p_s) \end{cases} \tag{2}$$

The value to the equations (2) is $c \equiv \sum_{i=1}^{s} y_i P_i P_i^{'} (\text{mod } P)$, where $P = p_1 p_2 \cdots p_s = p_1 P_1 = p_2 P_2 = \cdots = p_s P_s$, $P_i = \frac{P}{p_i}, i = 1,2,\cdots,s$ and $P_i^{'}$ is positive integer and satisfies the congruence equation $P_i^{'} P_i \equiv 1 (\text{mod } p_i), i = 1,2,\cdots,s$. Here c is the group public key. Then RSU_1 chooses a secure hash function h, and publishes (g_1, m_1, u_1, c, h).

When member V_i is willing to broadcast a message, V_i will sign the message M as 3.4.

3.4. Signature

For greater security, this paper uses Schnorr signature algorithm [31] to sign messages. If Vk wants to sign a message M, Vk will sign it by using Schnorr signature algorithm. V_k randomly chooses $\omega \in z_{p_k}^*$ and computes $f = g_1^{\omega} (mod\ p_k)$, $\pi = h(f \| M)$,

$\zeta = \omega - x_k \pi \left(mod\ q_k\right)$, where g_1 is the identity code of LTA_1, x_k is the private key of V_k, p_k, q_k are the primes chosen by RSU_1 for V_k. Then, (π, ζ, p_k) is the signature of V_k on M.

3.5. Verification

Anyone else can verify the signed message with the signature (π, ζ, p_k) and the group public key (g_1, m_1, u_1, c, h) as Algorithm 1.

Algorithm 1: Message authentication algorithm for any verifier

Require: (π, ζ, p_k), (g_1, m_1, u_1, c, h)

1: Computes $c \equiv y_k \pmod{p_k}$ and obtains the public key y_k of V_k.

2: Check whether the obtained public key y_k is in **Table 2**, if y_k is in the **Table 2**, go to step 3.

3: Computes $f' \equiv g_1^{\zeta} y_k^{\pi} \equiv g_1^{\omega - x_k \pi} g_1^{x_k \pi} \equiv g_1^{\omega} \pmod{p_k}$.

4: **if** the equation $\pi = h\left(f' \| M\right)$ holds, **then** accept the message is signed by V_k and opens the message.

5: **end if**

3.6. Joining

It is supposed that vehicle user V_{s+1} wants to join to the group of RSU_1. V_{s+1} performs the following steps to join the group.

(1) V_{s+1} submits its accession request and blind certificate to RSU_1. RSU_1 verifies the validity of V_{s+1} using **Fig. 3**. For eligible V_{s+1}, RSU_1 generates key parameters for V_{s+1}. Based on Schnorr signature algorithm, RSU_1 randomly selects primes p_{s+1}, q_{s+1}, where $q_{s+1} \mid p_{s+1} - 1, p_{s+1} \geq 2^{512}, q_{s+1} \geq 2^{160}$, and $p_{s+1} \geq g_1$. Then, RSU_1 sends $(g_1, p_{s+1}, q_{s+1}, p_{s+1}^{v_1}, q_{s+1}^{v_1})$ to V_{s+1} via a secure channel.

(2) V_{s+1} verifies the legality of the received parameters. If the equations (3) hold, V_k believes the parameters are valid and produced by RSU_1.

$$\begin{cases} \left(p_{s+1}^{v_1}\right)^{u_1} \equiv p_{s+1} \left(mod\ m_1\right) \\ \left(q_{s+1}^{v_1}\right)^{u_1} \equiv q_{s+1} \left(mod\ m_1\right) \end{cases} \tag{3}$$

Then V_{s+1} randomly chooses $x_{s+1} \in z_{p_{s+1}}^*$ as its private key, and computes $y_{s+1} = g_1^{x_{s+1}} \pmod{p_{s+1}}$ as its public key. And V_{s+1} sends y_{s+1} to RSU_1 via a secure channel.

(3) RSU_1 reserves y_{s+1} with its corresponding certificate in database and updates **Table 2** to **Table 3**.

Table 3. The Public Keys of the Existing Group Members

The public key	y_1	y_2	…	y_k	…	y_s	y_{s+1}

Then RSU_1 securely transmits (y_{s+1}, *certification*) to LTA_1. LTA_1 stores (y_{s+1}, *certification*) in its reserve.

(4) RSU_1 computes the new group key according to the congruence equations (4).

$$\begin{cases} c_{new} \equiv y_1 (\text{mod } p_1) \\ \cdots\cdots \\ c_{new} \equiv y_s (\text{mod } p_s) \\ c_{new} \equiv y_{s+1} (\text{mod } p_{s+1}) \end{cases} \tag{4}$$

the value to the equations (4) is $c_{new} \equiv \sum_{i=1}^{s+1} y_i P_{i\,new} P_{i\,new}^{'} (\text{mod } P_{new})$, where $P_{new} = p_1 p_2 \cdots p_s p_{s+1} = P p_{s+1}$. The value of P_{inew} and $P_{inew}^{'}$ can be calculated by using Algorithm 2, where $1 \le i \le s+1$.

Algorithm 2: The process of calculating P_{inew} and P'_{inew}.

Require: P_i, P_i', p_i $(1 \le i \le s+1)$

1: **if** $1 \le i \le s$ **then** compute $P_{i\,new} = P_i p_{s+1}$, $P_{i\,new}^{'} = P_i^{'} p_{s+1}^{-1}$, where $p_{s+1} p_{s+1}^{-1} \equiv 1 (\text{mod } p_i)$, since $P_{i\,new}^{'} P_{i\,new} \equiv 1 (\text{mod } p_i)$ and $P_i P_i^{'} \equiv 1 (\text{mod } p_i)$.

2: **if** $i = s+1$, **then** compute $P_{(s+1)new} = \prod_{i=1}^{s} p_i = p_1 p_2 \cdots p_s$, $P_{(s+1)new}^{'} \equiv P_{(s+1)new}^{-1} (\text{mod } p_{s+1})$.

3: **Output:** P_{inew} and P'_{inew} $(1 \le i \le s+1)$

Thereby, c_{new} is the new group public key. But if $c \equiv c_{new} (\text{mod } P_{new})$, RSU_1 returns to step (1) to generate key parameters again for user. Finally RSU_1 publishes $(g_1, m_1, u_1, c_{new}, h)$.

3.7 Revocation

Assume that V_k represents an arbitrary group member and there are s members in the group. If the vehicle user V_k $(1 \le k \le s)$ wants to quit the group, V_k only needs to transmit the quit request to RSU_1. And RSU_1 changes the public key of V_k in the database to compute a new group public key $c^{'}$. Substituting $y_k^{'}$ for y_k, RSU_1 computes the new group public key according to the congruence equations (5).

$$\begin{cases} c^{'} \equiv y_1 (\text{mod } p_1) \\ \cdots\cdots \\ c^{'} \equiv y_k^{'} (\text{mod } p_k) \\ \cdots\cdots \\ c^{'} \equiv y_s (\text{mod } p_s) \end{cases} \tag{5}$$

For equations (5), the value is $c^{'} \equiv \sum_{i=1, i \ne k}^{s} y_i P_i P_i^{'} + y_k^{'} P_k P_k^{'} (\text{mod } P) \equiv c - y_k P_k P_k^{'} + y_k^{'} P_k P_k^{'} (\text{mod } P)$, where $y_k^{'} \equiv y_k (\text{mod } p_k)$ should not hold. Then RSU_1 updates **Table 3** to **Table 4**.

Table 4. The Public Keys of the Existing Group Members

The public key	y_1	y_2	…	y_{k-1}	y_{k+1}	…	y_s

By the above steps, there is only one change for computing the new group public key that y_k is altered to $y_k^{'}$ in calculation formula, where $c^{'}$ is the new group public key after the revocation of V_k.

After the revocation, both $c^{'} \equiv y_k (\text{mod } p_k)$ and $\pi = h(f \| M)$ will not hold, then the messages signed by V_k will no longer be verified to be legal.

In the revocation, the keys of unrevoked group members do not need to update.

3.8 Opening

Assume that users find there are something false or malicious in messages which is signed by V_k, they can combine to submit an open application with the message (π, ζ, p_k, M) to RSU_1. There should be a specific number of users in reality, which is a measure of whether RSU_1 will accept the application.

With enough users, RSU_1 accept the application and compute the public key y_k of V_k by $c \equiv y_k (\text{mod } p_k)$. Then, RSU_1 searches its database to find the corresponding blind certificate of V_k and submits (*application, certificate*) to LTA_1.

LTA_1 firstly checks the open application. Then LTA_1 retrieves its database to find the real identity of V_k by search its certificate. In reality, there are different punishments for this case according to different policies in each area.

4. SECURITY AND PERFORMANCE ANALYSIS

4.1 Security Analysis

Anonymity. Due to the application of restrictive partially blind signature technique in the generation of blind certificates, attackers cannot deduce the real identity of BVs from the blind certificate [30]. Further, blind certificates of BV update regularly, thus attackers are not able to track a specific blind certificate. Moreover, since the key pairs of group members are not related to their real identity, it is also impossible for attackers to obtain the identity information of members.

Integrity. Since the signature is generated by Schnorr signature algorithm, and the Schnorr signature scheme has been known to be provably secure in the Random Oracle Model[31],[32], the integrity of messages is guaranteed.

Traceability. In dispute cases, LTAs are able to trace the real identity of BV_i. RSU transmits the public key and the blind certificate of BV_i to the corresponding LTA. Then LTA retrieves its database and find out the real identity of BV_i.

Unforgeability. By unforgeability meant that a signed message proved to be generated by V_k can only be generated by V_k. In our scheme, if a vehicle user V_j receives a signed message (π, ζ, p_k, M), with the group public parameters (g_1, m_1, u_1, c, h), V_j will firstly compute the public key y_k of V_k by using equation $c \equiv y_k (\text{mod } p_k)$. Then V_j computes $f^{'} \equiv g_1^{\zeta} y_k^{\pi} \equiv g_1^{\omega - x_k \pi} g_1^{x_k \pi} \equiv g_1^{\omega} (\text{mod } p_k)$ and checks whether the equation $\pi = h(f \| M)$ holds or not, if holds, V_j believes the message is signed by V_k, otherwise abandons the message.

Since p_k is a public parameter of V_k and c is also pubic, the public key y_k of V_k obtained by equation $c \equiv y_k \pmod{p_k}$ is unique.

If an attacker Eve attends to forge a signature (π', ζ', p_k, M') of V_k, Eve randomly chooses $\omega' \in z_{p_k}^*$ and computes $f' = g_1^{\omega'} (mod\ p_k)$, $\pi' = h(f', M')$, $\zeta' = \omega' - x_k' \pi' (mod\ q_k')$, where $q_k' \mid p_k - 1$. However, x_k' is necessary to compute ζ', and x_k' should meet $y_k \equiv g_1^{x_k'} \pmod{p_k}$. Since the discrete logarithm problem, Eve cannot forge a signature of V_k.

Nonrepudiation. By nonrepudiation meant that V_k cannot deny its own signed messages. Since the signed messages are unforgeable, and the public key y_k of V_k can be computed by $c \equiv y_k \pmod{p_k}$ for all the valid messages signed by V_k, V_k cannot deny its own signed messages.

Forward security. If a user V_{s+1} joins to the group, its public/private key pair y_{s+1}/x_{s+1} are generated by the public parameters, where $y_{s+1} = g_1^{x_{s+1}} \pmod{p_{s+1}}$. Moreover, the group public key is changed from c to c_{new} by equations (6).

$$\begin{cases} c \equiv y_1 \pmod{p_1} \\ \cdots\cdots \\ c \equiv y_i \pmod{p_i} \\ \cdots\cdots \\ c \equiv y_s \pmod{p_s} \end{cases} \text{ and } \begin{cases} c_{new} \equiv y_1 \pmod{p_1} \\ \cdots\cdots \\ c_{new} \equiv y_s \pmod{p_s} \\ c_{new} \equiv y_{s+1} \pmod{p_{s+1}} \end{cases} \tag{6}$$

It is necessary that the forward security should be protected, that is, messages signed by a new group member should not be verified to be legal with the old group public key. If the messages are verified to be valid, the congruence equation $c \equiv y_{s+1} \pmod{p_{s+1}}$ also holds, so that the congruence equation $c \equiv c_{new} \pmod{P_{new}}$ should hold. In section 3.6, there is the restriction on the new group public key that the equation $c \equiv c_{new} \pmod{P_{new}}$ should not hold. Therefore, in proposed scheme, the forward security is guaranteed.

Backward Security. After the revocation of vehicle V_k, the group public key is refreshed from c to c' by using equations (7).

$$\begin{cases} c \equiv y_1 \pmod{p_1} \\ \cdots\cdots \\ c \equiv y_i \pmod{p_i} \\ \cdots\cdots \\ c \equiv y_s \pmod{p_s} \end{cases} \text{ and } \begin{cases} c' \equiv y_1 \pmod{p_1} \\ \cdots\cdots \\ c' \equiv y_k' \pmod{p_k} \\ \cdots\cdots \\ c' \equiv y_s \pmod{p_s} \end{cases} \tag{7}$$

In order to satisfy backward security, the messages signed by revoked members should not be legal for the new group public key. If the messages can be verified to be legal, there are two scenarios. The congruence equation $c' \equiv y_k \pmod{p_k}$ holds that the revoked member is still able to sign messages with its old private key x_k. Or the revoked member can obtain x_k' which meets the equation $y_k' = g_1^{x_k'} \pmod{p_k}$ that the revoked member can sign messages with the private key x_k'. If the congruence equation $c' \equiv y_k \pmod{p_k}$ holds, then the congruence equation $y_k' \equiv y_k \pmod{p_k}$ holds, while a significant restriction on y_k' is that the

equation $y_k^{'} \equiv y_k (\mathrm{mod}\ p_k)$ should not holds. The revoked member still can obtain the new group public key $c^{'}$ and compute $c^{'} \equiv y_k^{'} (\mathrm{mod}\ p_k)$ to get $y_k^{'}$. If the revoked member can obtain $x_k^{'}$ which meets the equation $y_k^{'} = g_1^{x_k^{'}} (\mathrm{mod}\ p_k)$, then the member can solve the discrete logarithm problem.

In conclusion, the backward security of the proposed scheme is guaranteed.

Anti-collusion. By anti-collusion meant that several group members can together forge a signed message $\left(\pi^{'}, \zeta^{'}, p_k, M^{'}\right)$ by an existing group member or generate a valid signed message $\left(\pi^{''}, \zeta^{''}, p^{'}, M^{''}\right)$.

As mentioned in unforgeability, group members will solve the discrete logarithm problem if they can forge a signed message of an existing group member.

Suppose that there are s group members V_1, V_2,…, V_s and the group public key is c. For V_i, $y_i \equiv g_1^{x_i} (\mathrm{mod}\ p_i)$, where $1 \le i \le s$. If V_1, V_2,…, V_m wants to generate a new valid signed message $\left(\pi^{''}, \zeta^{''}, p^{'}, M^{''}\right)$, it is necessary to get parameters $y^{'}$ and $x^{'}$, where $y^{'} \equiv g_1^{x^{'}} \left(\mathrm{mod}\ p^{'}\right)$. Each verifier needs to compute $y^{'}$ by using $c \equiv y^{'} \left(\mathrm{mod}\ p^{'}\right)$ and then check whether $y^{'}$ is in the table of the existing group member's public keys, hence $y^{'}$ should be able to equal to one of y_i, where $1 \le i \le s$. Then, if V_1, V_2,…, V_m can forge a signed message successfully, they can forge a signed message of an existing group member, accordingly they can solve the discrete logarithm problem.

4.2 Performance Analysis

Function. In this section, a comparison of function between our scheme and some other group signature schemes in VANETs is made as **Table 5**.

Table 5. Comparison of Function

Function	Ours	Shao Jun[17]	Chae Duk Jung[18]	Yong Hao[20]	Zhu Xiaoyan[23]	Wei Lingbo[26]	Mamun, M.S.I.[28]
Member joining	√	√	√	√	√	√	√
Member revocation	√	√			√	√	√
Anonymity	√	√	√	√	√	√	√
Traceability	√	√	√	√	√	√	√
Unforgeability	√	√					
Forward security	√						
Backward security	√						
Anti-collusion	√			√	√		

Computation. In this section, we analyze the performance of the proposed scheme in terms of computational loads.

Table 6 gives the test time for the involved cryptography operations [33]. The experiments are conducted on a computer with Intel i5-3210 -2.5GHz CPU and 4-GB RAM.

Table 6. Execution Time for Operations

Denotation		Time(ms)
T_{Ex}	An exponentiation in Z_p^*	0.067
T_{Ad}	An addition in Z_p	0.001
T_{Mu}	A multiplication in Z_p^*	0.001
T_{In}	An inverse operation in Z_p^*	0.004
T_P	A pairing operation	16.064

In the proposed scheme, if a member V_k quits the group, RSU only needs to substitute $y_k^{'}$ for y_k as the equations (5), and calculate the new group public key $c^{'} \equiv c - \left(y_k - y_k^{'}\right) P_k P_k^{'} \left(\mathrm{mod}\, P\right)$ while key pairs of other group members are not influenced. The revocation costs 2 addition, 2 multiplication, 2 modular arithmetic to calculate the new group public key. Since for CPU modular arithmetic is more efficient than multiplication, we assume that execution time for modular arithmetic is T_{Mu} as multiplication. Hence the computational load is $2T_{Ad}+4T_{Mu}$.

A comparison between the proposed scheme and two other revocable schemes [26],[28] is made on the revocation complexity of a group member, respectively. Here we assume that there are n_{gr} members in the group.

In [26], RSU can revoke a member x_j by broadcasting a revocation list *RL*, and upon receiving a *RL*, each unrevoked member updates its parameters accordingly. There are 1 addition, 1 division and 1 exponentiation on each unrevoked member for RSU, and 3 addition, 1 inverse operation, 2 multiplication, 3 division and 4 exponentiation for each unrevoked member. Since for CPU division is as efficient as multiplication, the total computational load of this scheme is $(4T_{Ad}+T_{In}+6T_{Mu}+5T_{Ex})(n_{gr}-1)$.

In [28], if a member leaves the group, RSU needs to update credential element and publish the corresponding public key parameters for each unrevoked member. There are 1 addition, 1 multiplication, 1 division and 2 exponentiation for RSU on each unrevoked member, and 1 multiplication, 2 exponentiation and 1 pairing operation for each unrevoked member. The total computational load of this scheme is $(T_{Ad}+3T_{Mu}+4T_{Ex}+T_p)(n_{gr}-1)$.

We compare the revocation computational load of a group member in this scheme with [26] and [28] in **Table 7**.

Table 7. Comparison on Revocation Computational Load of a Group Member

	Ours	Wei Lingbo[26]	Mamun, M.S.I.[28]
Total computational load	$2T_{Ad}+4T_{Mu}$	$(4T_{Ad}+T_{In}+6T_{Mu}+5T_{Ex})(n_{gr}-1)$	$(T_{Ad}+3T_{Mu}+4T_{Ex}+T_p)(n_{gr}-1)$
Computational load for each unrevoked member	0	$3T_{Ad}+T_{In}+5T_{Mu}+4T_{Ex}$	$T_{Mu}+2T_{Ex}+T_p$
Computational load for RSU	$2T_{Ad}+4T_{Mu}$	$(T_{Ad}+T_{Mu}+T_{Ex})(n_{gr}-1)$	$(T_{Ad}+2T_{Mu}+2T_{Ex})(n_{gr}-1)$

As shown in **Table 7**, regardless of the quantity of group members, the revocation computational load is a constant in the proposed scheme which has lower computational load than the other two schemes. The comparison between our scheme and the two schemes on total computational load, computational load for each unrevoked member and computational load for RSU are shown in **Fig. 4**, **Fig. 5** and **Fig. 6**, respectively.

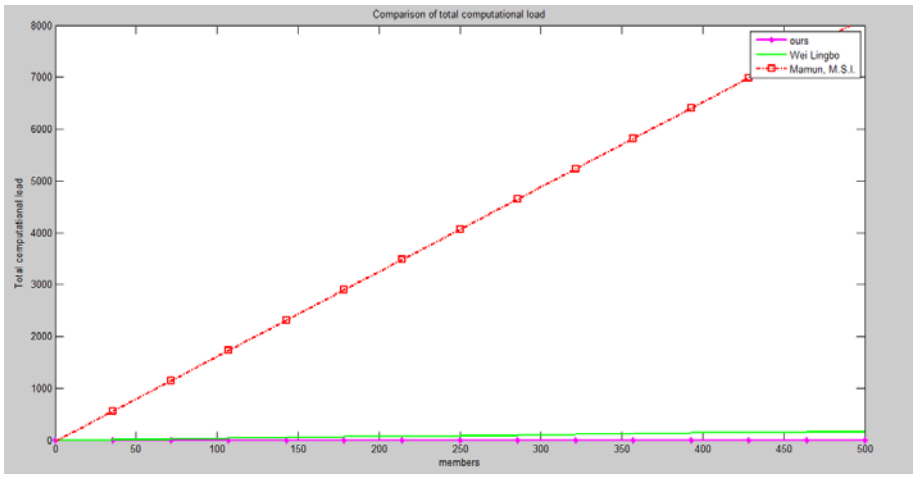

Fig. 4. Comparison of Total Computational Load

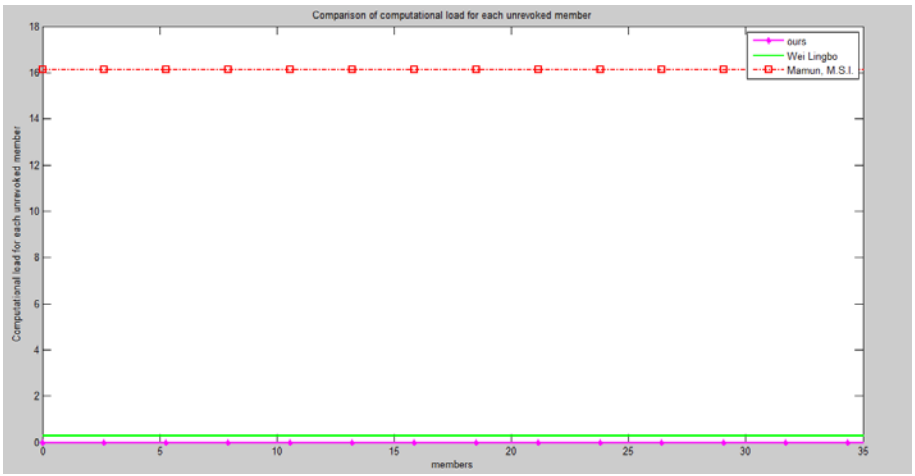

Fig. 5. Comparison of Computational Load for Each Unrevoked Member

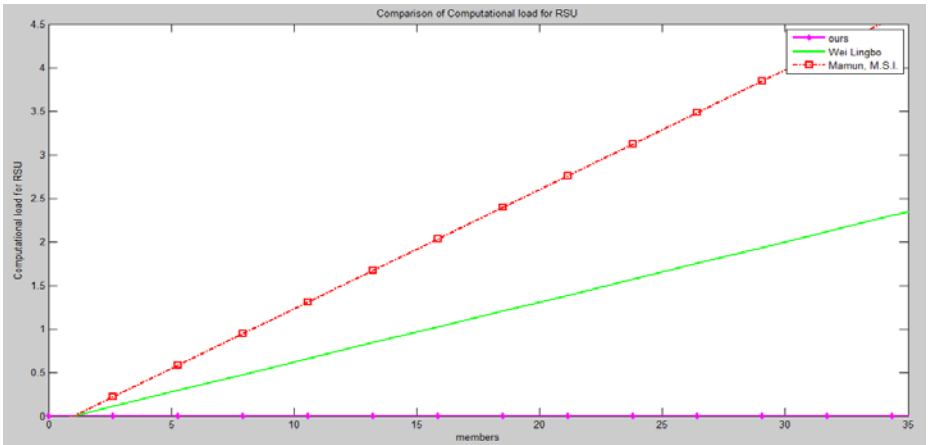

Fig. 6. Comparison of Computational Load for RSU

5. CONCLUSION

In this paper, an efficient revocable group signature scheme in VANETs is proposed. When a member quits the group, RSU only needs to compute 1 module arithmetic to compute the new group public key. On the security analysis, our scheme keeps the forward and backward security. Furthermore, our scheme has a lower computation load. Owing to the frequent and high speed joining and leaving of vehicles in VANETs, this scheme with the property of efficient revocation is suitable for the dynamic VANETs. Moreover, the scheme is suitable for most dynamic scenes.

References

[1] FIEBIG B. , "European traffic accidents and purposed solutions," in *Proc. of the ITU-T Workshop on Standardization in Telecommunication for Motor Vehicles. Geneva: ITU-T*, pp. 24-25, 2003.

[2] V. Daza and J. Domingo-Ferrer, "Trustworthy privacy preserving car-generated announcements in vehicular *ad hoc* networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 4, pp. 1876–1886, May 2009. Article(CrossRefLink)

[3] M. Raya and A. Aziz, "Efficient secure aggregation in VANETs," in *Proc. of 3rd Int.Workshop VANETs*, pp. 67–75, 2006. Article(CrossRefLink)

[4] M. Raya and J. Hubaux, "The security of vehicular ad hoc networks," in *Proc. of 3rd ACM Workshop SASN*, pp. 11–21, 2005. Article(CrossRefLink)

[5] J. Ren and J. Wu. , "Survey on Anonymous communications in computer networks," *Computer Communications, Elsevier*, vol. 33, issue 4, pp. 420-431, May 2010. Article(CrossRefLink)

[6] Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, 24(2): pp. 84-90, 1981. Article(CrossRefLink)

[7] Sun and Jinyuan Zhang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," *IEEE Trans on Parallel and Distributed Systems*, vol. 21, pp.1227-1239, Sept. 2010. Article(CrossRefLink)

[8] Dijing Huang and Misra, S, "PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs," *IEEE Trans on Intelligent Transportation Systems*, vol. 12, pp. 736-746, 2011. Article(CrossRefLink)

[9] Jonathan Petit and Florian Schaub, "Pseudonym Schemes in Vehicular Networks: A Survey," *IEEE Communication Surveys & Tutorials*, vol. 17, pp. 228-255, 2015. Article(CrossRefLink)

[10] Jie Li and Huang Lu, "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs," *IEEE Trans on Parallel and Distributed Systems*, vol. 26, pp. 938-948, 2015. Article(CrossRefLink)

[11] Beresford A R and Stajano F., "Location privacy in pervasive computing," *Pervasive Computing*, 2(1): pp. 46-55, 2003. Article(CrossRefLink)

[12] Elmer Schoch and Frank Kargl, "Impact of Pseudonym Changes on Geographic Routing in VANETs," *Springer*, LNCS. 4357, pp. 43-57, 2006. Article(CrossRefLink)

[13] Rongxing Lu and Xiaodong Li, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs," *IEEE Trans on Vehicular Technology*, vol. 61, pp. 86-96, 2012. Article(CrossRefLink)

[14] Sam, M.M. and Vijayashanthi, N. ,"An effective strategy for pseudonym generation & changing scheme with privacy preservation for vanet," *International Conference on ICICA*, pp. 109-117, May. 2014. Article(CrossRefLink)

[15] Hui Liu and Hui Li, "Efficient and Secure Authentication Protocol for VANET," *IEEE 2010 International Conference on CIS*, pp. 523-527, 2010. Article(CrossRefLink)
[16] Mamun, M.S.I. and Miyaji, A. , "A Multi-purpose Group Signature for Vehicular Network Security," in *Proc. of IEEE 2014 17th International Conference on NBiS*, pp. 511-516, Sept. 2014. Article(CrossRefLink)
[17] Jun Shao and Xiaodong Lin, "A Threshold Anonymous Authentication Protocol for VANETs," *IEEE Trans on Vehicular Technology*, 2015. Article(CrossRefLink)
[18] Jung, Chae Duk and Sur, Chul, "A robust and efficient anonymous authentication protocol in VANETs," *IEEE Journal of Communication and Networks*, vol. 11, pp. 607-614, Dec. 2009. Article(CrossRefLink)
[19] Yong Hao and Yu Cheng, "Distributed Key Management with Protection Against RSU Compromise in Group Signature Based VANETs," *IEEE GLOBECOM 2008*, pp. 1-5, 2008. Article(CrossRefLink)
[20] Yong Hao and Yu Cheng, "A Distributed Key Management Framework with Cooperative Message Authentication in VANETs," *IEEE Journal on Selected Areas in Communications*, vol. 29, pp. 616-629, May, 2011. Article(CrossRefLink)
[21] Xiaoyan Zhu and Shunrong Jiang, "Privacy-preserving authentication based on group signature for VANETs," *IEEE GLOBECOM*, pp. 4609-4614, Dec. 2013. Article(CrossRefLink)
[22] Chaurasia, B.K. and Verma, S. , "Message broadcast in VANETs using group signature," *IEEE WCSN*, pp. 131-136, Dec. 2008. Article(CrossRefLink)
[23] Xiaoyan Zhu and Shunrong Jiang, "Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks," *IEEE Trans. Veh. Technol.* vol. 63, no. 2, Feb. 2014. Article(CrossRefLink)
[24] Li He and Wen Tao Zhu, "Mitigating DoS attacks against signature-based authentication in VANETs," *IEEE International Conference on CASE*, vol. 3, pp. 261-265, May 2012. Article(CrossRefLink)
[25] Chun-I Fan and Wei-Zhe Sun, "Strongly Privacy-preserving Communication Protocol for VANETs," *IEEE 2014 Ninth ASIA JCIS*, pp. 119-126, Sept. 2014. Article(CrossRefLink)
[26] Lingbo Wei and Jianwei Liu, "On a Group Signature Scheme Supporting Batch Verification for Vehicular Networks," in *Proc. of IEEE 2011 Third International Conference on MINES*, pp. 436-440, 2011. Article(CrossRefLink)
[27] Toru Nakanishi and Hiroki Fujii, "Revocable Group Signature Schemes with Constant Costs for Signing and Verifying," *International Association for Cryptologic Research*, pp. 463–480, 2009. Article(CrossRefLink)
[28] Mamun, M.S.I. and Miyaji, A., "Secure VANET applications with a refined group signature," in *Proc. of IEEE 2014 Twelfth ANNUAL International Conference on PST*, pp. 199-206, 2014. Article(CrossRefLink)
[29] X.Chen, F.Zhang, and S.Liu, "ID-based restrictive partially blind signatures and applications," *J. Syst. Softw*, vol. 80, no. 2, pp. 164-171, 2007. Article(CrossRefLink)
[30] Zhenyu Yang and Shucheng Yu, " P^2 :Privacy-Preserving Communication and Precise Reward Architecture For V2G Networks in Smart Grid," *IEEE Trans. Smart Grid*, Vol. 2, pp. 697-706, Dec. 2011. Article(CrossRefLink)
[31] Pointcheval, D. and Stern, J., "Security Proofs for Signature Schemes," *EUROCRYPT, LNCS*, vol. 1070, pp. 387–398. Springer, Heidelberg, 1996. Article(CrossRefLink)
[32] Yannick Seurin, "On the Exact Security of Schnorr-Type Signatures in the Random Oracle Model", *EUROCRYPT, LNCS*, Springer, Heidelberg, vol. 7237, pp.554-571. 2012.

Article(CrossRefLink)
[33] http://crypto.stanford.edu/pbc/.

Zhen Zhao was born in Shanxi, Changzhi, P.R. China in 1993. At present, she is pursuing her master degree in Xidian University, Xi'an, China. Her main research interests include key management, group signature, smart grid and wireless network security.

Jie Chen is an associate professor of Xidian University. She received her MS and PhD degree from Xidian University in 2005 and 2007. Her research interests include cryptographic protocols, design and analysis of cipher algorithm, security in Smart Grid. Email: jchen@mail.xidian.edu.cn.

Yueyu Zhang received his MS and PhD degree from Xidian University in 2005 and 2008. He is currently a visiting scholar at Michigan State University. Now he is an associate professor of Xidian University. His research interests include cryptographic protocols, security in Internet of Things and wireless network. Email: yyzhang@xidian.edu.cn.

Lanjun Dang received her M.E. degree and PH.D. degree in Communication and Information Systems from Xidian University, Xi'an, China, in 2005 and 2008, respectively. Now she is an associate professor of Xidian University. Her research interests included the security of mobile IP networks, authentication in wireless sensor networks, and information security.