Journal of Information Hiding and Multimedia Signal Processing ©2018 ISSN 2073-4212
Ubiquitous International Volume **9**, Number **1**, January **2018**

Research on Secure and Privacy-Preserving Scheme Based on Secure Multi-Party Computation for VANET

Cheng Song, Mingyue Zhang and Weiping Peng

School of Computer Science and Technology, Henan Polytechnic University,
Jiaozuo, Henan, 454000, China
songcheng@hpu.edu.cn; zhangmingyue0118@163.com; pwp9999@hpu.edu.cn

Received July, 2017; revised October, 2017

Abstract. *To solve the security and privacy problem for Vehicular Ad - hoc Network (VANET), we propose an improved anonymous authentication scheme based on secure multi-party computation theory and privacy protection authentication protocol. Because of employing the solution theory of linear equations systems and the oblivious transfer protocol, this scheme effectively avoids traditional public key algorithms which have complex computation. By theoretical analysis and comparison, it is demonstrated that the scheme not only can fulfill multiple security requirements for authentication, anonymity, collusion attack and replay attack, etc. but also can improve authentication efficiency. Consequently, the proposed scheme has great theoretical significance and application value in limited computational performance environments such as the Internet of Things.*

Keywords: VANET; Secure multi-party computation; Privacy protection; Anonymous authentication

1. **Introduction.** With the popularization of vehicles in modern society, a series of traffic-related problems occur frequently, such as parking difficulty, traffic congestion and traffic accidents. Consequently, people are more and more concerned with issues like traffic management, driving safety and exchange of traffic information. In order to better improve traffic environment and build the transportation systems of next generation, VANET[1] has been proposed and hence received great attention from all walks of life. VANET is a special mobile ad hoc network with mobile vehicles as its nodes on the basis of Dedicated Short-Range Communications (DSRC) standard, Wireless Access in Vehicular Environments (WAVE) standard and 802.11p[2]. In VANET, vehicles can not only obtain traffic information and entertainment information, but also improve driving safety, so as to improve driving experience. In recent years, many applications and value-added services of VANET have already brought convenience to people.

However, VANET faces an urgent security challenge. On the one hand, VANETs inherent properties of wireless communication often make the data easily to be monitored, altered and forged; on the other hand, vehicles are located in the open physical space, privacy (such as driver's license number, identity, location, route or distance of driving) leakage will pose a threat to the life and property safety of both drivers and passengers. However, most of these schemes are designed on the basis of digital signature technology in public key infrastructure (PKI), in which the protocols require excessive computation costs but have low authentication efficiency, and the public key certificates are often updated so frequently as to increase storage costs, thus making it unable to meet the needs of VANET environments with rapid changing topology.

Secure multi-party computation is one of the important methods to solve the privacy protection problem. In secure multi-party computation, two or more parties who have secret inputs cant get any extra information except their expected and proper outputs. This feature has a clear advantage in privacy protection. Therefore, secure multi-party computation is gradually being applied to solve those practical applicational problems of privacy protection, such as: electronic voting, secure multiparty matrix applications, data mining, data encryption and its application in database. In this paper, we use anonymous authentication to protect user's identity privacy. In order to avoid the complexity and excessive calculation of traditional privacy protection methods, a secure and efficient privacy protection scheme for vehicular networks is proposed based on the properties of the solutions of nonhomogeneous linear equations and by means of oblivious transmission. Compared with the traditional vehicle network privacy protection schemes, our scheme not only improves the efficiency, but also strengthens the security. This is of great theoretical significance and practical value for high dynamic vehicle networking.

The rest of this paper is organized as follows: In section 2 we introduce the related work. In section 3 we introduce preparation knowledge. The proposed scheme is described in detail in section 4. We give the analyses of security and efficiency in section 5. The last section concludes the paper.

2. **Related work.** Currently, a number of privacy protection schemes for VANET have been proposed based on anonymous authentication. However, most of these schemes are designed based on digital signature technology in public key infrastructure (PKI), in which the protocols need excessive computation costs as to have low authentication efficiency, and the public key certificates are often updated so frequently as to increase storage costs. Raya, et al. [3] proposed an anonymous authentication protocol based on pseudonym certificates, in which numerous private keys and relevant anonymous authentication certificates are prestored in each vehicle node, thus making it infeasible for vehicle nodes with limited storage and highly dynamic vehicular ad hoc networks. Lu, et al. [4] devised an ID-based authentication framework that adopts adaptive self-generated pseudonyms as identifiers to protect privacy in VANET, but there would be considerable message delay in authentication among nodes. Beresfords experiment [5] proved that pseudonyms must be periodically updated due to the fact that only one pseudonym fails to satisfy the need for privacy protection because attackers can track users public information. Therefore, the pseudonym should be updated regularly [6][7]. In Ref.[8] an anonymous authentication scheme based on ring signature is proposed. The time required for message authentication increases linearly with the certificate update list (CRL) increasingTherefore, with increasing of vehicles, there would be difficulties in managing and maintaining pseudonym certificates, the periodical update of which also would affect routing efficiency and increase the loss rate of data packets. Some researchers adopted group signature technique to realize anonymous authentication in VANET for sake of protecting privacy, but such schemes are quite low in efficiency [9-12]. In order to improve efficiency, researchers proposed some improved schemes [13-19]. In Ref.[20] the authentication scheme based on group signature reduced the key pairs storage and transmission costs in CRL, but the cost in the process of signature and authentication is still high. Sampigethaya [21] devised a group dynamic scheme based on group signature, in which each group has their own group keys (used for signature and message authentication) and group manager (sending and receiving messages as the agent of group members). This scheme has high energy cost in group managers communications and computation, so it turns out to be the bottleneck

of the system. The highly dynamic property of VANET makes the nodes enter and exit frequently, which calls for effective entrance and exit mechanisms for group members in group signature scheme. In fact, many of current schemes can effectively respond to new applicants access requests, e.g. RSUs in [9]-[19] can generate new key pairs for new applicants and broadcast new public keys. Nevertheless, the schemes in [9][10][18][19] fail to solve revocation problems for previous applicants. And in schemes[10][17] the withdrawal of one group member would affect other group members keys, causing overall change, which fails to meet the highly dynamic demands in VANET.

3. **Preparation knowledge. (1) Theory of linear equations**[22]

Theorem 3.1. *If a system of n linear equations* $\mathrm{Ax} = \mathrm{b}$ *have solutions, a necessary and sufficient condition is that the rank of coefficient matrix* A *equals the rank of augmented matrix* $\bar{\mathrm{A}}$ *, i.e.*$R(A) = R(\overline{A})$ *.*

Theorem 3.2. *Suppose the system of n linear equations* $\mathrm{Ax} = \mathrm{b}$ *has solution and* $R(A) = n$ *, then the solution is unique; if* $R(A) < n$ *, the solutions will be infinite.*

(2) Security assumption. Security assumption: the security of the oblivious transfer(OT) protocol is based on DDH assumption, which means that for any $g \in G_q/\{1\}$ and arbitrary a, b, c belong to finite domains Z_q , the algorithm cannot distinguish the following two distributions:

$$Y_1 = (g, g^a, g^b, g^{ab})$$
$$Y_2 = (g, g^a, g^b, g^c)$$

(3) Symbols description The symbols used in this scheme are explained in Table 1:

Table 1. Symbols explanation

Symbol	Definition
G	multiplication group of prime order q
g, h	generators of group G
Y_1,Y_2	two distributions in DDH
TA	trusted service center
R_s	roadside unit node
V_p	vehicle node
A	$m \times n$ dimension matrix
y	m dimension vector
x	n dimension column vector
D_i	random matrix
m_t	t number of messages possessed by V_p
δ_i	k number of messages selected by R_s

(4) VANET network model. This paper adopts typical VANET structural model, as shown in Figure.1, which are composed of three parts: Trust Authority (TA), On Board Unit (OBU) and Road Side Unit (RSU). There are two types of communications: communication between vehicle and RSU and communication between vehicle and vehicle.

Trusted Authority TA: In order to ensure the normally running of the system, a trusted server TA is required to storing the privacy information for all the authenticated vehicles, generating the overall security parameters and distributing public/private keys to all participants. In general, vehicle manufacturer or transportation management department acts as TA.

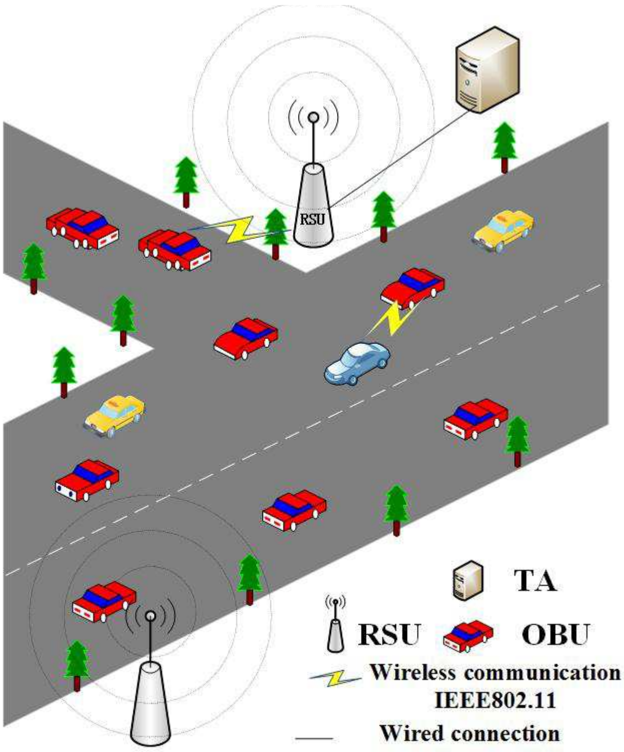

FIGURE 1. VANET network model

Roadside unit RSU: Similar to the access nodes of wireless sensor networks, RSU is the infrastructure installed on both sides of the road, capable of communicating with vehicles via wireless. The RSU communicates with the vehicle using the DSRC protocol which enables RSU to validate the request information sent by the vehicle.

Vehicle unit OBU: In VANET, each vehicle is equipped with wireless communication module OBU, through which vehicles can communicate with RSU or other vehicles equipped with OBU, and then access the corresponding services.

4. **Privacy protection scheme based on SMC.** The scheme includes three phases: the registration phase, the authentication phase and the update phase.

4.1. **Registration phase. Step 1**: TA randomly generates an $m \times n$-matrix $A(2 \leq m < n$) and an m-vector y to satisfy $R(A) = R(\overline{A})$ and $R(A) < n$, then the solutions of the system of linear equations $Ax = y$ is infinite.

Step 2: TA randomly generates a unique n-vector x_i for each valid vehicular node, and x_i satisfies $Ax_i = y$, where x_i is one of all solutions of linear equations system $Ax = y$. TA assigns x_i to the corresponding vehicular node V_p as its true identity. Correspondingly, TA sends matrix A and vector y to each unit node R_s as authentication information via secure channel.

4.2. **Authentication phase.** When V_p needs to communicate with R_s , V_p applied to R_s for identity authentication, then R_s authenticates the identity of V_p, and determines whether it is valid or not. The detail steps are as follows.

Step 1: V_p sends authentication request to R_s , and V_p randomly selects two generators (g, h) of G , then sends (g, h) to R_s.

Step 2:After receiving authentication requests from vehicular node, R_s generates k random matrix D_1 ,D_2 ,$\cdots$, D_k satisfies $A = D_1 + D_2 + \cdots + D_k$. R_s generates a secret random number t satisfies $t > k$, then sends $(H_1, H_2, \cdots, H_t)$ to V_p . $H_i = D_j$ (i and j are random), while the other $H_{\mathrm{j}}(1 \leq j \leq m, j \neq i)$ are random matrix.

Step 3: V_p computes $H_n x + r_j$ for all $n = 1, 2, \ldots t$, where r_j is a random vector. V_p has t messages m_1, m_2 , $\cdots$, m_t , where $m_1 = H_1 x + r_1$, $m_2 = H_2 x + r_2$,$\cdots$, $m_t = H_t x + r_t$. R_s selects k messages m_{δ_1} , m_{δ_2} ,$\cdots$, m_{δ_k} ($\{\delta_1, \delta_2, \ldots \delta_{\mathrm{k}}\} \subset \{1, 2, 3 \cdots t\}$). According the oblivious transfer protocol, R_s retrieves the result $H_i x + r_j = D_j x + r_j$.

① R_s computes $f'(x) = (x - \delta_1)(x - \delta_2) \ldots (x - \delta_k) = b_0 + b_1 x + \ldots + x^k$, then randomly selects a polynomial $f(x) = a_0 + a_1 x + \ldots + a_{k-1} x^{k-1} + x^k$, $a_i \in {}_R Z_q$ $(0 \leq i \leq k)$ for $i = 1, 2, \ldots, k - 1$, R_s computes: $A_0 = g^{a_0} h^{b_0} modp, A_1 = g^{a_1} h^{b_1} modp, \ldots$, A_{k-1} =$g^{a_{k-1}} h^{b_{k-1}} modp$ then sends the results to V_p .

② For $i = 1, 2, \ldots t$, V_p randomly selects $l \in Z_q$, and computes:

$B_i = g^{lf(i)} h^{lf'(i)} = (A_0 A_1^i A_2^{i^2} A_{k-1}^{i^{k-1}} (gh)^{i^k})^l \bmod p$

$C_i = m_i B_i \bmod p$

$r = \sum\limits_{j=1}^{k} r_j$

sends $(r, g^l, C_1, \ldots, C_t)$ to R_s .

③ For $i = \delta_1, \delta_2, \ldots \delta_{\mathrm{k}}$, R_s computes $\mathrm{m}_{\delta_i}{}'$ =$\mathrm{C}_{\delta_{\mathrm{i}}}((g^l)^{f(\delta_{\mathrm{i}})})^{-1}(((g^l)^{f(\delta_{\mathrm{i}})})^{-1}(g^l)^{f(\delta_{\mathrm{i}})} = 1 \bmod p)$, where $(m_{\delta_1}{}', m_{\delta_2}{}', \ldots m_{\delta_k}{}')$ are k messages $H_i x + r_j = D_j x + r_j$ ($i = 1, 2, \ldots, k$) selected by R_s .

Step 4: R_s computes

$W = \sum\limits_{j=1}^{k} (D_j x + r_j) = Ax + \sum\limits_{j=1}^{k} r_j = Ax + r$

$y' = W - r = Ax$

If $y' = y$, then authentication can be passed; otherwise, the authentication is rejected.

4.3. **Update phase.** Known formula:

$$\begin{cases} Ax_1 = y \\ Ax_2 = y \\ \ldots \\ Ax_n = y \end{cases}$$

When $x_1, x_2, \cdots, x_n$ is known, then A and y can be calculated. A is a matrix of $m \times n$ dimensions, and y is a column vector of m dimensions. In the system of equations, there are $m \times n + m$ unknown numbers, whereas the number of equations is only $m \times n$, so A and y are not unique.

In VANET, when new nodes enter or nodes revoked, all the existing nodes x_i can be used to re-calculate A and y by registration server, and then sends the result to R_s as new authentication information.

5. Scheme Analysis.

5.1. Security analysis. (1) Senders privacy security

Theorem 5.1. *Based on DDH assumption, if all receivers are semi-honest, the probability of receiving other* $t - k$ *messages can be ignored.*

If receiver can receive other $t - k$ *messages with non-ignorable probability* ε *via algorithm* B*, then receiver can distinguish (with non-ignorable probability) the two distributions* Y_1 *and* Y_2.

Proof: Let the input of B be (g, u, v, w) (belonging to Y_1 or Y_2)and let B calculate $(g_1, g_2, h_1, h_2, G_q, p)$, in which $g_1 = g$, $g_2 = u$, $h_1 = v$, $h_2 = w$. Then B conducts OT protocol with receiver.

① R selects two polynomials $f'(x) = (x - \delta_1)(x - \delta_2)\ldots(x - \delta_k) = b_0 + b_1 x + \ldots + x^k$, $f(x) = a_0 + a_1 x + \ldots + a_{k-1} x^{k-1} + x^k$, $a_i \in {}_R Z_q$, $0 \le i \le k$.

② R → B: $A_0 = g_2^{a_0} h_2^{b_0} \bmod p, \ldots A_{k-1} = g_2^{a_{k-1}} h_2^{b_{k-1}} \bmod p$

③ B randomly selects $l \in Z_q$, for $i = 1, 2, \ldots, t$ calculate:

$B_i = g_2^{lf(i)} h_2^{lf'(i)} = (A_0 A_1^i A_2^{i^2} A_{k-1}^{i^{k-1}} (g_2 h_2)^{i^k})^l \bmod p$, $C_i = m_i B_i \bmod p$

④ B → R: $g_2^l = g_1^{al}$, $C_1, C_2, \ldots, C_t$

⑤ R → B: Any $k + 1$ messages $\{m_{\beta_1}, \ldots, m_{\beta_{k+1}}\} \subseteq \{m_1, \ldots, m_t\}$

If these $k+1$ messages are correct, then B outputs 1, otherwise, outputs 0. (Obviously, if R only obtains other messages by guess, the probability of B outputting 1 is $1/q$)

If (g, u, v, w) is from Y_1, then $B_i = g_2^{lf(i)} h_2^{lf'(i)} = u^{lf(i)} w^{lf'(i)} = g^{alf(i)} g^{ablf'(i)} = (g_1^{lf(i)} h_1^{lf'(i)})^{al}$ is a valid encryption; If (g, u, v, w) is from Y_2, then $B_i = g_2^{lf(i)} h_2^{lf'(i)} = u^{lf(i)} w^{lf'(i)} = g^{alf(i)} g^{a'blf'(i)} \ne (g_1^{lf(i)} h_1^{lf'(i)})^{al}$ is not valid data. Since l is selected randomly, and B_i is evenly distributed in G_q, so the probability of receiver receiving other messages is $1/q$. Apparently, receiver can still receive the k messages it selects.

If the probability of B outputting 1 is greater than $\varepsilon + 1/q$, then B is able to calculate that (g, u, v, w) is from distribution Y_1 ; If the probability of B outputting 1 is less than $\varepsilon + 1/q$, then B is able to conclude that (g, u, v, w) is from distribution Y_2 . Thus, B is able to distinguish DDH with non-ignorable probability, and the privacy of sender can be protected. Moreover, although R_s can frequently obtain the calculated result $D_j x + r_j$ with x_i , yet r_j is a vector generated randomly by V_p , so r_j is a secret vector for R_s. Consequently, it cannot conclude x_i from $D_j x + r_j$, and x_i is unconditionally secure for R_s. And, r_j is a random number and is able to resist to replay attack.

(2) Receivers privacy security

For any different $\delta'_1, \delta'_2, \ldots \delta'_{\mathrm{k}}$, there is a polynomial with order k : $f'_1(x) = (x - \delta'_1)(x - \delta'_2)\ldots(x - \delta'_k) = b'_0 + b'_1 x + \ldots + x^k$. And a polynomial with order k :$f_1(x) = a'_0 + a'_1 x + \ldots + a'_{(k-1)} x^{k-1} + x^k$, which satisfies $A_i = g^{a'_i} h^{b'_i}$, and $(0 \le i \le k-1)$ so the privacy of receiver is unconditionally secure. Considering the concrete application situations and collision attack, the probability of V_p accurately guessing receivers messages is $1/C_t^k$, which is closely associated with k and t. Suppose sender V_p can guess accurately via collision attack, employ this formula: $W = \sum_{j=1}^{k} (D_j x + r_j) = Ax + \sum_{j=1}^{k} r_j = Ax + r$, since r_i is generated randomly by V_p , so V_p knows w, r, x and only need to solve A. A is the matrix of $m \times n$ dimension, x is n dimensional column vector, and y is m dimensional column vector, so there are totally m equations and $m \times n$ unknown numbers. Consequently, the solutions are infinite. It is impossible to solve A . It is secure for receiver R_s.

(3) Collusion attack

Suppose there are n vehicles conspiring with one another to conclude the secret authentication vectors A and y of R_s, they combine all the authentication information of them and create the equation systems:

$$\begin{cases} Ax_1 = y \\ Ax_2 = y \\ \ldots \\ Ax_n = y \end{cases}$$

In these, matrix A is of $m \times n$ dimension, and y is m dimensional column vector. In the equation systems above, there are $m \times n + m$ unknown numbers, but only $m \times n$ equations, so there are infinitely many solutions of matrix A and vector y by solving with $m \times n$ equations. Consequently, despite that relevant systems of equations can be created to solve A and y, yet the accurate calculation is impossible due to infinitely many solutions. In this sense, this scheme can successfully resist collusion attack.

(4) Anonymity

The proposed scheme realizes the anonymity of the vehicle through the OT protocol. When R_s and V_p executed the OT protocol, V_p calculates $(r, g^l, C_1, \cdots C_t)$ and sends them to R_s . Then R_s calculates $y' = W - r$ and verifies $y' \overset{?}{=} \mathrm{y}$ to decide whether the authentication passes or not. Because of the randomness of r_j in $H_\mathrm{i}x + r_j$ and the solution theory of systems of linear equations, R_s can't get the real identity of V_p . So, the scheme doesn't leak any identity information about the requestor.

(5) Replay attack

If malicious vehicular node obtains the message sending to R_s by V_p, it will disguise itself as V_p to apply to R_s for authentication. However, During each authentication process, R_s will randomly generates new $(H_1, H_2 \cdots H_t)$, $t - k$ matrices of them are random, t is a secret random number, r_j in $H_\mathrm{i}x + r_j$ is random vector generated in the validation information generated process. So, the message $H_\mathrm{i}x + r_j$ which has been verified sent by malicious vehicle cannot fulfill the authentication requirement of R_s , thus is invalid. In this sense, the proposed scheme is able to prevent replay attack.

Comparison of security properties in the proposed scheme with that of other schemes is shown in Table 2:

Table 2. Comparison of security properties

	Ref.[8]	Ref.[11]	Ref.[20]	the proposed scheme
Anonymity	√	√	√	√
Privacy of V_p	√	√	√	√
Privacy of R_s			√	√
Collusion attack				√
Replay attack			√	√

5.2. **Efficiency analysis.** For the sake of qualitative analysis and comparison in analysis of computation complexity, we use T_{mul} to denote a multiplication operation, T_{exp} to denote a single exponentiation operation, T_{in} to denote a single inverse operation, T_{par} to denote a bilinear pairing operation, T_h to denote the a *hash* operation; n to denote the number of group members, N_{crl} to denote the number of CRL.

The computation cost of V_P is: $3tT_{mul} + 2tT_{\exp}$

The computation cost of R_s is: $4kT_{mul} + (4k - 2)T_{\exp} + kT_{in}$

The results of comparing the proposed scheme with the authentication schemes in reference [8][11][20] are shown in Table 3.

Table 3. Comparison of computation complexity

Scheme	Total computational cost
Ref.[8]	$3T_{\exp} + 2T_{par} + nT_{mul} + 9N_{crl}$
Ref.[11]	$20T_{\exp} + 13T_{par}$
Ref.[20]	$2N_{crl}T_{par} + 11T_{par} + 2T_h$
Our scheme	$(3t + 4k)\, T_{mul} + (2t + 4k - 2)\, T_{\exp} + kT_{in}$

As is shown in Table 3, all other typical schemes have bilinear pairing operations in public key cryptography. The computation time of bilinear pairings operation is much larger than the time required for other types of operations in the table. Although there are k and t (k represents the number of random matrices D_i ($i \in 1 \cdots k$), t indicating the number of messages) generated in step 1 of the authentication phase in the scheme, however our scheme still has a greater advantage compared to the scheme based on public key cryptography in the total overhead. As for the interactive frequency during authentication, the node only needs to conduct four times information interaction with vehicular nodes, which has advantage over the existing schemes. As a result, the efficiency of the scheme has improved significantly.

6. **Conclusion.** To prevent privacy leaking when vehicular information is transmitted on non-secure channel, this paper devises a secure and efficient anonymous authentication scheme for VANET based on secure multi-party computation. This scheme adopts solution theory of linear equations systems and concrete oblivious transfer protocol, so this scheme effectively avoids the traditional public key algorithms which have complex computation. By theoretical analyses and comparison, it is demonstrated that the scheme not only can fulfill multiple security requirements for authentication, anonymity, collusion attack and replay attack, etc, but also can improve authentication efficiency. Consequently, the proposed scheme has great theoretical significance and application value in limited computational performance environments such as the Internet of Things.

REFERENCES

[1] L. I. Jing-Lin, Z. H. Liu, F. C. Yang. Internet of Vehicles: The Framework and Key Technology. *Journal of Beijing University of Posts & Telecommunications*, vol. 37, no.6, pp: 95-100, 2014.

[2] F. J. Martinez, C. K. Toh, J. C. Cano, et al. Emergency Services in Future Intelligent Transportation Systems Based on Vehicular Communication Networks. *Intelligent Transportation Systems Magazine IEEE*, vol. 2, no.2, pp:6-20, 2010.

[3] M. Raya, J. P. Hubaux. Securing vehicular ad hoc networks. *Journal of Computer Security*, vol.15, no.1, pp:39-68. 2007.

[4] H. Lu, J. Li, M Guizani. A novel ID-based authentication framework with adaptive privacy preservation for VANETs Computing, *Communications and Applications Conference.* IEEE, pp:345-350, 2012.

[5] A. R. Beresford, F. Stajano. Location privacy in pervasive computing. *Pervasive Computing IEEE*, vol.2, no.1, pp:46-55, 2003.

[6] R. Lu, X. Lin, T. H. Luan, et al. Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs. *IEEE Transactions on Vehicular Technology*, vol.61, no.1, pp:86-96, 2012.

[7] M. S. Mathews, Y. BevishJinila. An effective strategy for pseudonym generation & changing scheme with privacy preservation for vanet. *International Conference on Electronics and Communication Systems.* IEEE, pp:1-6, 2014.

[8] S. Zeng, Y. Huang, X. LiuPrivacy-preserving communication for VANETs with conditionally anonymous ring signature *International Journal of Network Security(IJNS)*, vol.17, no.2, pp:135-141, 2015.

[9] H.Liu, H.Li, Z.Ma. Efficient and Secure Authentication Protocol for VANET. *International Conference on Computational Intelligence and Security.* IEEE Computer Society, pp:523-527, 2010.

[10] M. S. I .Mamun, A . Miyaji, H Takada. A Multi-purpose Group Signature for Vehicular Network Security. *International Conference on Network-Based Information Systems.* IEEE, pp:511-516, 2014.

[11] J . Shao, X. Lin, R. Lu, et al. A Threshold Anonymous Authentication Protocol for VANETs. *IEEE Transactions on Vehicular Technology*, vol.65, no.3, pp:1-1, 2016.

[12] C. D. Jung, C. Sur, Y. Park, et al. A robust and efficient anonymous authentication protocol in VANETs. *Journal of Communications & Networks*, vol.11, no.6, pp:607-614, 2009.

[13] Y. Hao, Y. Cheng, C. Zhou, et al. A Distributed Key Management Framework with Cooperative Message Authentication in VANETs. *IEEE Journal on Selected Areas in Communications*, vol.29, no.3, pp:616-629, 2011.

[14] X. Zhu, S. Jiang, L. Wang, et al. Privacy-preserving authentication based on group signature for VANETs. *GLOBECOM Workshops.* IEEE, pp:609-4614, 2013.

[15] B. K. Chaurasia, S. Verma, S. M. Bhasker. Message broadcast in VANETs using group signature. *International Conference on Wireless Communication and Sensor Networks.* IEEE, pp:131-136, 2008.

[16] X. Zhu, S. Jiang, L. Wang, et al. Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks. IEEE *Transactions on Vehicular Technology*, vol.63, no.2, pp:907-919, 2014.

[17] L. He, W. T. Zhu. Mitigating DoS attacks against signature-based authentication in VANETs. *IEEE International Conference on Computer Science and Automation Engineering.* IEEE, pp:261-265, 2012.

[18] C. I. Fan, W. Z. Sun, S. W. Huang, et al. Strongly Privacy-Preserving Communication Protocol for VANETs. *Asia Joint Conference on Information Security.* pp:119-126, 2014.

[19] M. S. I Mamun, A. Miyaji. Secure VANET applications with a refined group signature*Twelfth International Conference on Privacy, Security and Trust.* IEEE, pp:199-206, 2014.

[20] X. Lin, X. Sun, P. H. Ho, et al. GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications. *IEEE Transactions on Vehicular Technology*, vol.56, no.6, pp:3442-3456, 2007.

[21] K. Sampigethaya, M. Li, L. Huang, et al. AMOEBA: Robust Location Privacy Scheme for VANET. *IEEE Journal on Selected Areas in Communications*, vol.25, no.8, pp:1569-1589, 2007.

[22] R. H. Shi, H. Zhong, L. S. Huang. A novel anonymous authentication scheme without cryptography. *Transactions on Emerging Telecommunications Technologies*, vol.25, no.9, pp:875880, 2014.