Privacy-preserving Communication for VANETs with Conditionally Anonymous Ring Signature

Shengke Zeng, Yuan Huang, and Xingwei Liu
(Corresponding Author: Xingwei Liu)

School of Computer and Software Engineering, Xihua University
999 Jin Zhou Road, Jin Niu District, Chengdu, Sichuan Province 610039, P. R. China
(Email: lxw@mail.xhu.edu.cm)

Abstract

In this paper, we introduce an efficient communication protocol for vehicular ad hoc networks (VANETs) based on conditionally anonymous ring signature scheme to address the issue on anonymous authentication and efficient tracking in case of a dispute. It offers low storage requirements and fast message authentication. In addition, the proposed protocol does not require Road-side Units to aid to authenticate or track. Indeed, the obvious advantage is that our construction does not depend on any fully trusted authority during the tracing phase.

Keywords: Conditional privacy, conditionally anonymous ring signature, ring signature, VANETs

1 Introduction

To reduce traffic accidents and improve driving experience, extensive efforts have been made by industry and academia. And so, a self-organized vehicular ad hoc networks (VANETs) emerged. VANETs mainly consist of wireless communication devices On-board Units (OBUs) and Road-side Units (RSUs). Through inter-vehicle communication and vehicle to OBU communication, VANETs can collect traffic and road information and deliver them to all the users after integration.

At present, one of the key issues in design and deployment of VANETs is anonymous authentication. On the one hand, we expect that a message is authenticated by a credible vehicle (sender) instead of malicious or bogus vehicle. On the other hand, the sender is reluctant to leak its identity or location information during the authentication. Clearly, the goals of privacy presentation and accountability seem conflicting. Furthermore, the conditional privacy protection should be satisfied where an involved vehicle should be revoked by Transportation Regulation Center (TRC) just in a traffic dispute [4, 8].

To tackle this conditional privacy during the communication in VANETs, there existing kinds of proposals such as pseudonyms-based approaches, group-oriented signature-based approaches and RSU-based approaches. In 2005, Raya et al. introduced a large number of anonymous keys based protocol (LAB) [9] which is a kind of pseudonyms-based approach. Although LAB protocol satisfies the conditional privacy requirement, it is inefficient in terms of storage, tracing and revocation since it requires 43800 certificates for each vehicle to meet the privacy. Some approaches have been proposed to reduce the large number of pseudonyms which are preloaded on each vehicle, such as [1]. In addition, the group-oriented signature-based approaches can avoid the inefficiency existed in pseudonyms-based approaches. For example, the GSB protocol [5] introduced by Lin et al. does not need to store large number of keys and anonymous certificates. However, it requires each remaining vehicle to calculate a new private key and group public key if the number of revoked vehicles is larger than some threshold. To verify the message, the time increases linearly as the number of revoked vehicles in the revocation list grows. Xiong et al. proposed an anonymous authentication protocol based on proxy re-signature scheme [12]. This protocol depends on the RSUs to aid to authenticate the safety messages. It enables lower computation and communication overheads compared to LAB protocol and GSB protocol. However, this kind of RSU-aided authentication is over-reliance on RSUs. As we know, RSUs are vulnerable to attackers in the real world. Furthermore, there are some other schemes, for example, PPSCP [7] used the shared keys instead of pseudonyms or anonymous certificates to authenticate vehicle safety messages. Zhang et al. [15] proposed an improved authentication scheme which needs to produce a pseudonym before the vehicle sending a message each time. The potential problems in [7] and [15] are the same as [11], which is proposed by Xiong et al. This scheme [11] introduced an efficient authentication for VANETs based on revocable ring signature [6] (denoted as RRSB). It is clear except that it relies on the absolutely honest TRC. In the realization of tracing OBU, the TRC cannot show the evidence of the validation process. Actually, the authority can slander any vehicle arbitrary, and the framed vehicle has no way to prove its innocence.

In this paper, we focus on the construction of a communication protocol based on conditionally anonymous ring signature [13, 14] to tackle the conditional privacy presentation and authentication for VENETs, called CRSB. Different from [11], our protocol does not fully depend on the authority in tracing. In other words, TRC in our scheme cannot frame any vehicles during the anonymous authentication. The remainder of this paper is organized as follows. Section 2 introduces the preliminaries. Section 3 presents the system model and design goals. Section 4 proposes the privacy-preserving authentication protocol for VANETs and the security analysis and performance evaluation are shown in Section 5. The last section concludes this paper.

2 Preliminaries

In this section, we briefly introduce the mathematical tool and the underlying signature used in our protocol.

2.1 Mathematical Tool

Bilinear maps over an elliptic curve will be our mathematic tool. Let G_1 be an additive group over an elliptic curve and G_2 be a multiplicative cyclic group. Both of them have a same prime order q. P is a generator of G_1. Let $\hat{e} : G_1 \times G_1 \to G_2$ be a computable bilinear map with the following properties:

1) *Bilinearity.* $\forall P, Q \in G_1$, $\forall a, b \in \mathbb{Z}_q$, $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ holds.

2) $Non - degeneracy.$ $\hat{e}(P, P) \neq 1$.

3) *Computability.* All the group operations and the bilinear map must be efficiently computable.

2.2 Underlying Signature Algorithm

Ring signature algorithm was first introduced by Rivest et al. in 2001 [10]. It enables the signer to sign a message anonymously. The signer in the ring signature algorithm can randomly choose members (with their public keys) to form a group without these members' consent. Through a valid ring signature, the receiver can be convinced that the message coming from this group without knowing the actual sender. Thus, the anonymity of the signer is satisfied. Different from the group signature algorithm [2], the ring signature scheme does not need any group manager to join in. There is no setup algorithm in the ring signature scheme. Therefore, the ring signature scheme has a more flexible frame. However, the anonymity of the signer in the ring signature is unconditional. Even all the private keys of members in the group are revealed, it cannot be determined who is the actual signer.

Recently, Zeng et al. [13, 14] have introduced a conditionally anonymous ring signature with additional two algorithms: confirmation algorithm and disavowal algorithm. Compared to the revocable ring signature [6], this scheme does not require the third party to trace the actual signer. If the dispute arises, the malicious signer can be revoked through the disavowal protocol. The conditional anonymity without the third party is good for the privacy-preserving communication for VANETs. We adopt their scheme as the underlying signature algorithm. On the one hand, the conditional privacy can be satisfied. On the other hand, it is more fair for the vehicles even though TRC is not absolutely honest.

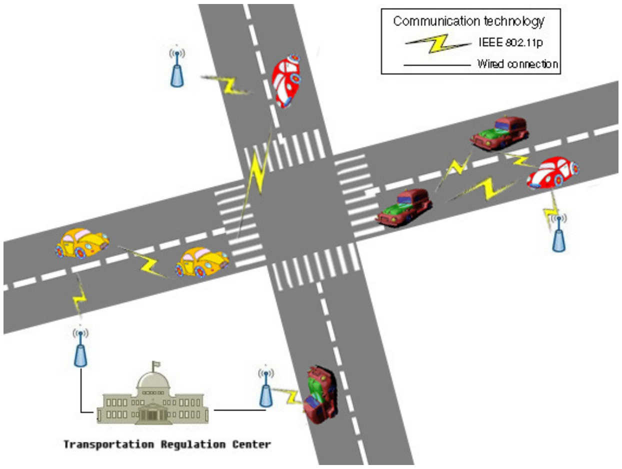

Figure 1: System model

3 System Model and Security Goals

In this section, we present the mainly entities in VANETs (Figure 1) in order to clear the later scheme. Further, we give the security requirements which should be satisfied during the secure and privacy-preserving communications in VANETs.

3.1 System Model

The common VANETs system with privacy protection mainly consists of three entities: the Transportation Regulation Center (TRC), the on-board units (OBUs) equipped on moving vehicles and the road-side units (RSUs). However, we do not employ RSUs in our system. Generally speaking, the moving vehicles in VANETS equipped with OBUs are registered with TRC which is in charge of revealing the real identity of the involved vehicle. Concretely,

- TRC. TRC in our scheme is an institution which is in charge of identity authentication, issuing and recycling certificate of each vehicle. Moreover, TRC can call out all of the vehicles in some ring to trace the target vehicle which involved in a traffic dispute. TRC has enough storage space and computational ability. However, unlike other related schemes, TRC is not required to be fully trusted in our protocol. In other words, TRC must show a valid proof while tracing the real identity of malicious vehicle.

- OBU. After initialization with the TRC, vehicles can join in the VANETs. Each vehicle is preloaded with public system parameters, certificate issued by TRC and the public-private key pair. As the vehicle moves most of the time, so does the OBU moves constantly. Each OBU should broadcast its routine safety messages when they are on the road, such as position, current time, direction, speed, acceleration or deceleration, traffic conditions and traffic events. Thereout, the communication between two vehicles or vehicle to RSU can assist drivers to get a better awareness of their environment and take action earlier.

3.2 Security Goals

We focus on the authentication and privacy during communications in VANETs, the following aspects should be addressed.

Authentication. The messages delivered in VANETs should be authenticated. To meet the security (e.g. against impersonation attack), the accepted messages should be generated by legitimate vehicles. Therefore, all the messages must be authenticated by the receiver no matter how they are sent by RSUs or OBUs.

Anonymity. From the perspective of the vehicles, they are disinclined to leak their personal information and be tracked during the messages authentication. It seems that the anonymity and authentication are contradictory.

Traceability. The vehicles may take the advantage of anonymity to misbehave, e.g., an insider can release selfish or malicious messages since it is not afraid to be tracked. In other words, a considerate communication protocol in VANETs should meet the conditional privacy. If the dispute occurs, the malicious vehicle must be revoked. Therefore, the authority (i.e. TRC) should reveal the vehicle's actual identity if necessary. Since TRC is not fully trusted, TRC must show the valid proof when it reveals the malicious vehicle's identity.

4 Efficient and Secure Privacy-preserving Vehicular Communication Scheme

We present our authentication protocol for VANETs based on conditionally anonymous ring signature scheme in detail in this section. Each vehicle can be obtained a set of public keys from other vehicles messages during its moving. The vehicle also would update this set of public keys if old ones are changed. When a vehicle (sender) wants to authenticate a message m, it randomly chooses n valid public keys from the set to form a ring R. Then the sender generates a ring signature σ with respect to (m, R) according to the underlying ring signature scheme. If σ is a valid signature w.r.t. (m, R), then the receiver is convinced that message m is sent by one member in ring R without knowing which one. In this way, the actual identity of the sender is protected. On the other side, if the sender is involved, TRC must track the sender out. Therefore, the underlying ring signature scheme cannot be unconditionally anonymous for the signer.

The proposed protocol includes four parts: system initialization and membership registration, OBU safety message generation, message verification and tracking algorithm. The notations used in the following scheme are listed in Table 1.

Table 1: Notation and description

Notation	Description
TRC	Transportation Regulation Center
OBU	On-board Unit
CRL	Certificate Revocation List
V_i	The i-th vehicle
RID_i	The real identity of V_i
$Cert_i$	The certificate of V_i
x_i	The private key of V_i
$y_i = x_i P$	The public key of V_i
m	The authenticated message
H_0, H_1	Hash functions
$Sig(\cdot)$	Digital signature algorithm
$m\|\|n$	Concatenation of strings m and n

A. System Initialization and Membership Registration

Given the security parameter γ, TRC generates the parameters $(G_1, G_2, P, q, \hat{e})$, where G_1 is an additive group and G_2 is a multiplicative cyclic group, both of them have the same prime order q. P is the generator of G_1. $\hat{e}$ is a computable bilinear map such that $\hat{e} : G_1 \times G_1 \rightarrow G_2$. TRC also selects a secure digital signature algorithm $Sig(\cdot)$ and two cryptographic hash functions:

$$H_0 : \{0,1\}^* \rightarrow G_1 \text{ and } H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q.$$

After that, TRC randomly selects $x_{TRC} \leftarrow \mathbb{Z}_q$ as its private key and computes $y_{TRC} = x_{TRC}P$ as its public key. Finally, TRC outputs system parameters $(G_1,G_2,P,q,\hat{e},H_0,H_1,y_{TRC},Sig(\cdot))$.

To achieve more comprehensive security, each vehicle V_i with its real identity RID_i generates its key pair by itself and obtains its certificate from TRC as follows.

- V_i randomly chooses $x_i \leftarrow \mathbb{Z}_q$ as its private key, and computes $y_i = x_i P$ as its public key.

- V_i randomly selects an integer $t_i \leftarrow \mathbb{Z}_q$ to compute the verification information $a_i = H_1(t_iP||RID_i)$ and $b_i = t_i + x_ia_i$. Then V_i sends (y_i, RID_i, a_i, b_i) to TRC for registration.

- After received this message, TRC checks whether the following equation holds or not:

$$a_i \stackrel{?}{=} H_1((b_iP - a_iy_i)||RID_i).$$

  If it meets, (y_i, RID_i) will be defined as valid public key and identity of V_i. After that, TRC stores (y_i, RID_i) and creates the certificate $Cert_i = Sig(y_i, RID_i; x_{TRC})$ for V_i with TRC's private key x_{TRC}. Finally, the tamper-proof device of each vehicle is preloaded with $(x_i, y_i, Cert_i, RID_i)$.

B. OBU Safety Message Generation

For each vehicle in VANETs, it should generate the signature on message m before sending it. In our scheme, we consider the common vehicles (excluding ambulance, police cars, military vehicles and so on) which need privacy protection. We take a common vehicle V_k for example. As mentioned before, when V_k moves on the road for some time, it has collected and stored many public keys of other vehicles. We suppose this set of public keys is $\mathcal{R}$ $=\{y_1, y_2, \cdots, y_n, y_{n+1}, \cdots\}$. When V_k needs to send and authenticate a message m, it randomly chooses n public keys from set $\mathcal{R}$ to form a group (e.g. ring) R. The signature generation algorithm is listed as follows:

1) V_k randomly selects $r_0 \leftarrow \{0,1\}^\gamma$, computes $\mu_0 = H_0(0, r_0, m, R)$ and $\mu_1 = H_0(1, r_0, m, R)$.

2) V_k computes $\rho = \hat{e}(\mu_1, \mu_0)^{x_k}$. After that, V_k generates verification information Π_1 to prove $\rho = \hat{e}(\mu_0, \mu_1)^{x_k}$ is consistent with some public key in R as follows:

   - Select $d, r_1 \leftarrow \mathbb{Z}_q$, compute $M = \hat{e}(P,P)^d$, $N = \hat{e}(\mu_1, \mu_0)^d$, $R_1 = \rho^{r_1}$.
   - For $1 \leq i \leq n$ but $i \neq k$, randomly choose $U_i \leftarrow G_1$, compute $h_i = H_1(m, M, N, R_1, \rho, U_i)$.
   - Compute U_k, h_k, and e as follows:

$$\begin{aligned} U_k &= r_1y_k - \sum_{i \neq k}(U_i + h_iy_i - h_iy_k), \\ h_k &= H_1(m, M, N, R_1, \rho, U_k), \\ e &= d - (\sum_{i=1}^{n} h_i + r_1)x_k. \end{aligned}$$

The signature with respect to (m, R) is $\sigma = (\rho, r_0, \Pi_1)$ where $\Pi_1 = (M, N, R_1, \{U_i\}_{i=1}^n, e)$. Finally, V_k broadcasts (m, R, σ).

C. Message Verification

Upon received (m, R, σ), the receiver, say V_l, checks whether these public keys y_i in ring R are contained in CRL or not. If all these public keys y_i are not in CRL, then, V_l checks σ as follows:

1) For $1 \leqslant i \leqslant n$, V_l computes $h_i = H_1(m, M, N, R_1, \rho, U_i)$.

2) V_l verifies whether the following conditions are true.

$$\begin{aligned} M &\stackrel{?}{=} \hat{e}(P,P)^e \cdot \hat{e}(P, \sum_{i=1}^{n}(U_i + h_iy_i)) \\ N &\stackrel{?}{=} \rho^{\sum_{i=1}^{n} h_i} \cdot R_1 \cdot \hat{e}(\mu_1, \mu_0)^e. \end{aligned}$$

If they hold, V_l will be convinced that message m is authenticated by one member in the ring R without knowing which one.

D. Tracking Algorithm

When comes a reward or dispute, there should be some mechanisms to reveal the real identity of the message authenticator. Consider the two scenarios. If the sender will be received a reward for his signing on one message, he is willing to admit his identity for his generation σ. In this case, our *confirmation algorithm* is helpful for him. On the other hand, if his malicious signing involves dispute, TRC must trace this member to take the responsibility for his fault. In this case, the malicious sender will not admit his signing of course. Then we should take our *disavowal algorithm* to help TRC to track the sender out.

confirmation algorithm. V_k and TRC conduct the confirmation algorithm as follows to convince TRC that he is the signer of given signature σ w.r.t. (m, R).

1) V_k randomly selects $d' \leftarrow \mathbb{Z}_q$, and computes $M' = \hat{e}(P,P)^{d'}$, $N' = \hat{e}(\mu_1, \mu_0)^{d'}$, $h'_k = H_1(M', N', \rho)$, $e' = d' - h'_k \cdot x_k$.

2) V_k computes $\Pi_2 = (e', M', N')$, then sends Π_2 to TRC.

After received Π_2, TRC performs as follows.

1) TRC computes $h'_k = H_1(M', N', \rho)$;

2) TRC verifies Π_2 by checking the following equations:

$$\begin{aligned} M' &\stackrel{?}{=} \hat{e}(P,P)^{e'} \cdot \hat{e}(P, y_k)^{h'_k} \\ N' &\stackrel{?}{=} \rho^{h'_k} \cdot \hat{e}(\mu_1, \mu_0)^{e'}. \end{aligned}$$

If they hold, TRC is convinced that σ is generated by V_k.

Disavowal Algorithm. When V_k involves the dispute for his signing σ and V_k does not admit his generation. Then TRC must depend on our disavowal algorithm to trace V_k. Our strategy is that, TRC calls out all the members in ring R to execute the disavowal algorithm with him. If the member V_i is not the sender, he must pass verification of the disavowal algorithm. In this way, only V_k (who is the actual signer of σ) cannot pass the verification. Therefore, TRC tracks the malicious sender out. The detail of disavowal algorithm is as follows.

1) V_i computes $\rho_i = \hat{e}(\mu_1, \mu_0)^{x_i}$.

2) V_i generates Π_3 as confirmation algorithm to prove that ρ_i is consistent with his public key y_i, and sends (ρ_i, Π_3) to TRC.

3) TRC checks Π_3's validation according to the verification equations in confirmation algorithm and checks that $\rho_i \neq \rho$. If they hold, TRC accepts the disavowal of V_i.

Remark 1. *Our communication protocol (CRSB) does not require each vehicle to store a large number of keys and anonymous certificates like LAB protocol. Each vehicle in CRSB only needs to store its key pair and CRL. The storage overhead of CRSB is lower than pseudonyms-based protocols. CRSB protocol does not require any RSUs to aid to authenticate messages or trace the vehicle. CRSB is based on ring signature scheme, compared to GSB protocol, CRSB does not require each remaining vehicle to update any public parameters if the number of revoked vehicles is larger than some threshold. CRSB meets the conditional privacy for the confirmation protocol and disavowal protocol. Indeed, any verifiers can obtain the proof transcript if one conducts the confirmation protocol or disavowal protocol with members in the ring R. Thus, CRSB does not rely on the absolutely honest TRC during the tracing phase. While RRSB [11] is based on revocable ring signature scheme, the actual member must be revoked by authority. Therefore, RRSB is secure only on the assumption that TRC is fully honest.*

5 Security Analysis and Performance Evaluation

In this section, we give the security analysis and performance evaluation of our construction.

5.1 Security Analysis

We analyze the security of CRSB protocol in terms of message authentication, user privacy preservation and traceability of the target vehicle.

- *Message Authentication*: In our scheme, σ w.r.t. (m, R) can be generated only by a registered vehicle in the ring R. Under the unforgeability of the underlying ring signature scheme, it is infeasible for an attacker which do not belong to ring R to forge a valid ring signature σ. Therefore, as long as σ fulfills the equation in the message verification phase in section 4, we can confirm that the message m must be authenticated by one member from the ring R.

- *User Privacy Preservation*: This property holds under the anonymity of the underlying ring signature scheme. It is proven in [13, 14] that the anonymity of this underlying ring signature is satisfied if Decisional Bilinear Diffie-Hellman assumption holds. Therefore, the privacy of the vehicle (authenticator) is protected in our protocol.

- *Traceability*: CRSB protocol provides the *confirmation protocol* and the *disavowal protocol* to revoke the actual signer. Specially, the traceability and the nonframeability of the underlying ring signature guarantee that the actual signer must be traced if a generated ring signature is valid and an innocent member cannot be framed if he does not generate one signature, respectively. Therefore, TRC can reveal the real identity of the vehicle by checking the list (y_i, RID_i).

5.2 Performance Evaluation

We evaluate the performance for CRSB protocol in terms of storage requirements and computational overhead, and compare CRSB to other related privacy-preserving protocols in VANETs.

A. Storage Requirements

We focus on the comparison between the RRSB protocol [11] and our protocol (CRSB) since both two protocols are based on ring signature algorithm. According to the analysis in [11], the total storage overhead of each vehicle in RRSB protocol is $m+1$ if there are m OBUs which are revoked and each key occupies one storage unit. Likewise, each vehicle stores one keypair registered in TRC and m revoked public keys in the CRL. Thus, the total storage unit of CRSB is also $m + 1$.

For the storage overhead, ring (group) signature-based protocols are better than LAB [9] since each vehicle in LAB protocol needs to store its own anonymous key pairs (almost up to 10^4 key pairs for the security) and m revoked public keys in the CRL. In other words, $(m + 1) \cdot 10^4$ is the total storage overhead for LAB protocol. However, RSU-based protocols such as [12] is the best for the storage overhead. For example, each OBU in [12] only needs to store one key pair and a short-time key pair together with its anonymous certificate issued by RSU. The storage overhead in such RSU-based protocols is only 2 since OBU does not need to store the CRL. Although the Roadside Unit-aided case is the most efficient in the storage, it requires Road-side Units to join in the communication authentication. However, in our scheme, we do not require any RSUs to aid to authenticate or trace.

B. Computation Overheads

In CRSB protocol, the vehicle authentication phase requires 1 pairing computation, 4 exponentiations and n point multiplications, $n + 2$ hashing operations where n is the size of the ring (the number of vehicles involved in ring R). The vehicle verification phase requires 2 pairing computations, 3 exponentiations, n point multiplications and $n + 2$ hashing operations. Thus, the total computation overhead during communication for our construction requires 3 pairing computations, 7 exponentiations,

$2n$ point multiplications and $2n+4$ hashing operations. While the RRSB protocol during the vehicle authentication phase requires 1 pairing computation, 2 exponentiations, $2n$ point multiplications and 2 hashing operations. Their vehicle verification phase also requires 1 pairing computation, 2 exponentiations, $2n$ point multiplications and 1 hashing operations. Then the total computation overhead during communication for RRSB protocol requires 2 pairing computation, 4 exponentiations, $4n$ point multiplications and 3 hashing operations.

Under the same security parameter, the time consuming for the pairing computation, exponentiation, point multiplication and the map to point hashing operation are 47.4ms, 3.13ms, 6.83ms and 3.00ms respectively with the subgroup of order prime 160-bit q in a super-singular elliptic curve $E(\mathbb{F}_p)$ with the embedding degree 2, where p is 512-bit prime [3]. This implementation of these primitives are executed on Pentium IV 2.26GHz with 256M RAM.

The total computation overhead comparison between CRSB protocol and RRSB protocol is listed in Table 2. We can find that the computation overheads of the two schemes are increasing with the growth of the number of vehicles n. In addition, with the increase of n, the computation of RRSB has a faster growth than CRSB.

Table 2: Comparison between CRSB and RRSB

	Descriptions	Execution Time
T_{CRSB}	The total execution time for CRSB protocol	$(176.11 + 19.66n)$ms
T_{RRSB}	The total execution time for RRSB protocol	$(116.32 + 27.32n)$ms

6 Conclusion

We introduce an efficient authentication protocol based on conditionally anonymous ring signature (CRSB) for privacy-preserving VANETs. Our protocol satisfies efficient authentication and conditional privacy preservation. Moreover, our protocol does not require any RSUs to participate in the authentication. Meanwhile, we also does not require any fully trusted authority during the tracing phase.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (NOs. 61402376, U1433130), the Key Technology Research and Development Program of Sichuan Province and Chengdu Municipality (NOs. 2013GZX0140, 12DXYB127JH).

References

[1] M. Burmester, E. Magkos, V. Chrissikopoulos, "Strengthening privacy protection in VANETs," in *IEEE International Conference on Networking and Communications, 2008 (WIMOB '08)*, pp. 508-513, 2008.

[2] D. Chaum and van E. Hevst, "Group signature," in *Eurocrypt'91*, pp. 257-265, Brighton, UK, 1991.

[3] S. Cui, P. Duan, C. W. Chan, "An efficient identity-based signature scheme and its applications," *International Journal of Network Security*, vol. 5, no. 1, pp. 89-98, 2007.

[4] C. T. Li, M. S. Hwang, Y. P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular Ad hoc networks," *Computer Communications*, vol. 31, no. 12, pp. 2803-2814, 2008.

[5] X. Lin, X. Sun, P. H. Ho, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442-3456, 2007.

[6] D. Y. W. Liu, J. K. Liu, Y. Mu, "Revocable ring signature," *Journal of Computer Science Technology*, vol. 22, no. 6, pp. 785-794, 2007.

[7] M. Mikki, Y. M. Mansour, "Privacy preserving secure communication protocol for vehicular Ad hoc networks," in *2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pp. 189-195, 2013.

[8] H. H. Ou, M. S. Hwang, J. K. Jan, "The UMTS-AKA protocols for intelligent transportation systems," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, pp. 1–12, 2009.

[9] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks", *Journal of Computer Security*, Special Issue on Security of Ad Hoc and Sensor Networks, pp. 39-68, 2007.

[10] R. L. Rivest, A. Shamir and Y. Tauman, "How to leak a secret," in *Asiacrypt'01*, pp. 552-565, Gold Coast, Australia, 2001.

[11] H. Xiong, K. Beznosov, Z. Qin, "Efficient and spontaneous privacy-preserving protocol for secure vehicular communication," in *International Communications Conference (ICC'10)*, pp. 1-6, Cape Town, South Africa, 2010.

[12] H. Xiong, Z. Chen and F. Li, "Efficient privacy-preserving authentication protocol for vehicular communications with trustworthy," *Security and Communication Networks*, vol. 12, no. 5, pp. 1441-1451, 2012.

[13] S. Zeng, S. Jiang and Z. Qin, "A new conditionally anonymous ring signature," in *17th International Computing and Combinatorics Conference (COCOON'11)*, pp. 479-491, Dallas, USA, 2011.

[14] S. Zeng, S. Jiang and Z. Qin, "An efficient conditionally anonymous ring signature in the random oracle model," *Theoretical Computer Science*, vol. 461, pp. 106-114, 2012.

[15] J. Zhang, M. Xu, "On the security of a secure batch verification with group testing for VANET", *International Journal of Network Security*, vol. 16, no. 5, pp. 355-362, 2014.

Shengke Zeng is a Lecturer at the School of Mathematics and Computer Engineering, Xihua University. She received her Ph.D. degree from University of Electronic Science and Technology of China (UESTC) in 2013. Her research interests include: Cryptography and Network Security.

Yuan Huang is a Master Candidate at the School of Mathematics and Computer Engineering, Xihua University. Her research interest is Network Security.

Xingwei Liu is a Professor at the School of Mathematics and Computer Engineering, Xihua University since 2002 and is also the director of the Laboratory for Wireless and Mobile Networks. He received his Ph.D. degree from Sichuan University in 2001. He has been a visiting professor at the Key Laboratory of Information Coding and Transmission in the Southwest Jiaotong University, Chengdu, China. His current research includes: Wireless and Mobile Networks.